

## IMAGE SPLICING DETECTION SCHEME USING SURF AND MEAN-LBP BASED MORPHOLOGICAL OPERATIONS

Nashat Salih Abdulkarim Alsandi <sup>a</sup>

<sup>a</sup> Information Technology, Duhok Private Technical Institute, Duhok Kurdistan Region, Iraq-(Nashat.alsandi@dhk-pti.com)

Received: Sept., 2021 / Accepted: Dec., 2021 / Published: Dec., 2021

<https://doi.org/10.25271/sjuoz.2021.9.4.866>

### ABSTRACT:

Tampering with images and changing them without giving any evidence has become very popular because of the presence of an enormous degree of intense altering device. The image forensics technique has grown popular for deciding whether a picture has been changed with a copy-move, splicing, or different forgery techniques. This paper presents a novel passive image splicing forgery detection technique which includes three steps. Firstly, extracting an interest region (ROI) by using SURF descriptor (Speed up Robust Transform) Points is concerned based on the morphological procedure. Secondly, the Extraction of Mean-LBP (Mean Local Binary Pattern) Highlights on ROI is carried out. Lastly, a Classification of Mean-LBP characteristics is done with the SVM classifier. This novel method has shown the best outcome as SVM is used for classification. As well as it has shown a higher accuracy on the standard three datasets CASIA TIDE V1.0, CASIA TIDE V2.0, and Columbia University, revealed that current method has achieved higher accuracy of 97.9%, 98.2%, and 98.9% respectively. Finally, in terms of accuracy, the proposed SFD scheme outperformed the best recent works in this area.

**KEYWORDS:** Splicing Forgery detection, Texture features, Support Vector Machine, SURF, MEAN-LBP

### 1. INTRODUCTION

Image forgery is defined as an artistic technique adopted in photography that spans across centuries. The earlier photography years identified new avenues utilized in the designing and development of portraits. Photographers have resorted to effective techniques in enhancing quality of image through retouching it which pleases a customer and raises the due income of such work [1,2].

Because of the convenience and simplicity of operation, this is the most well-known and often used technique for modifying a picture [3]. It entails mixing multiple components of two original images to create a new image. Because the merged component is from the same image, the dynamic color and range stay in compatibility mode with the rest of the image. The lack of essential and sufficient verification methods has resulted in a deterioration in the feasibility of automated content due to the lack of picture verification processes. Furthermore, the growth of automated algorithms effects the possible amount of manipulation, which restricts the level of human inspection, resulting in increasing image manipulation owing to a lack of the essential verification methods. [4]. When the image splicing procedure is done, the statistics of the image get disarranged. Nevertheless, these statistical modifications may not be obvious to the visual system of the human. These statistic disarrangements of an image cannot be decreased, even when expert criminal performs blending [5] and cover [6] works on the forged image as a post-processing operation.

The rest of this paper is organized as follows. Section 3 describes the proposed method. Experimental results and analysis are given in section 4. Concluding remarks are made in Section 5.

### 2. RELATED WORK

The completely automated spliced picture would include variations in different sections of the photos. The segment borders of the two areas may be discovered to be either authentic or spliced by estimating the camera response function (CRF) using geometric invariants from locally planar irradiance positions (LPIPs) [7]. On a forensic basis, the human visual model proposed by [8] may also be utilized to identify fraudulent images utilizing an automated detection framework based on visual saliency and fixation. While this is a practical approach for demonstrating spliced photos, there is a learning curve involved in completing this activity correctly.

In [9] proposes that manipulated photos may be shown using modeling edge information. The chroma of the picture around the photograph's edge is regarded a finite-state Markov chain that necessitates the extraction of low-dimensional feature vectors originating from stationary distributions that may be utilized for tamper detection. The Markov in Quaternion discrete cosine transform (QDCT) algorithm proposed by [9] used for the of detection image splicing.

The SVM is utilized to categorize the photos in line with the suggested technique, which uses color information inside the images to achieve high classification accuracy. In order to calculate image splicing employed by [10], class dependences based on three sequential classes and transition probabilities may be considered. Transition probabilities can be computed by progressing from the current class to the following two classes while looking for discriminative characteristics. Conditional co-occurrence probabilities are examined as a group (CCPM) using a matrix that is supplied into the SVM for accurate classification. Kakar suggested in [11] that motion blur estimation based on image gradients can also be used to detect possible irregularities in an image based upon the possible spliced region. The motion blur may be assessed by segmenting a conflicting region in photos with a modest level of blur. Suggestions method by [12]

that the detection be done by determining specific artifact based on Markov features which were acquired using DCT domain and DWT with the best features selected by SVM-RFE can be used to compute LBP for each pixel. In [13] Utilizing a multi-resolution WLD to extract chrominance components, a support vector machine can assist in determining picture fraud using an image database holding image forgery information. An improved Markov state selection method introduced in [14] was represented by decreasing the number of characteristics, this process analyzes the expected coefficients for development area and maps infinite coefficients with limited expresses that have coefficients in light of different suggested work patterns. A method to derive the features form the spliced image based on deep learning is proposed in [15] where the features are derived from CNN then PCA is used to reduction the dimension of features.

In (A) (Abraham et al., 2020), a new descriptor called Adaptive Threshold Mean Ternary Pattern (ATMTP) was developed based on the strength and weaknesses of both Local Binary Pattern (LBP) and Local Ternary Pattern (LTP). The ATMTP extraction feature is normally achieved by using proposed mean-based thresholding and adaptive ternary thresholding, and the ATMTP color features extracted from R, G, and B channels have revealed that the present method achieved higher accuracy on standard datasets than CASIA V2.0, out of 99.03%, Sensitivity 99.6%, and specificity 98.1%. multiple image splicing forgery detection using Mask R-CNN, with a backbone as a MobileNet V1 proposed by(B) (Kadam et al., 2021). which calculates the percentage score of a forged region of multiple spliced images. The proposed model is trained and tested using the MISD (Multiple Image Splicing dataset), and achieves an average precision of 82% on Multiple Image Splicing Dataset, 74% on CASIA 1.0, 81% on WildWeb, and 86% on Columbia Gray. The F1-Score of the proposed method on MISD was 67%, 64% on CASIA 1.0 68% on WildWeb, and 61% on Columbia Gray, outperforming ResNet variants

### 3. PROPOSED METHOD

Concept of image Splicing forgery detection and implemented contributions lead to achieve robust image Splicing forgery detection scheme. Main goal of proposed method is improving existing image SFD scheme, research framework therefore should be proposed to control all method processes in order to verify this goal. Figure 1 illustrates the proposed structure method. It deals with all the fundamental features of digital image processing spliced image detection included.

#### 3.1. Pre-processing

Among numerous existing techniques of image pre-processing, the color conversion process is considered to be the most common one. Generally, the major objective of the source image representation is to facilitate the task of subsequent steps and to improve the next stages performance [18] in this paper the weighted average method selected as show in equation (1).

$$Y = 0.299R + 0.587G + 0.114B \quad (1)$$

Where Y represented the luminance of the R, G, and B channels of the RGB image.

#### 3.2. Speed Up Robust Feature (SURF) extraction based on morphological operation

The Speeded-up robust feature (SURF) locator pointed a ‘fast-hessian’ locator. It is based on the basic likeness of the Hessian matrix which depends on indispensably pictures to diminish the time of computing. as well because it has extraordinary computation time and accuracy [19]. SURF represents to the dissemination of intrigued point neighborhoods and 64 measurements are given. SURF steps: 1) Utilize the Hessian matrix to discover the images' points of interest. 2) Utilize non-maximal concealment to discover the most intrigued focuses in scale-space 3) To discover feature direction to produce rotationally invariant features 4)

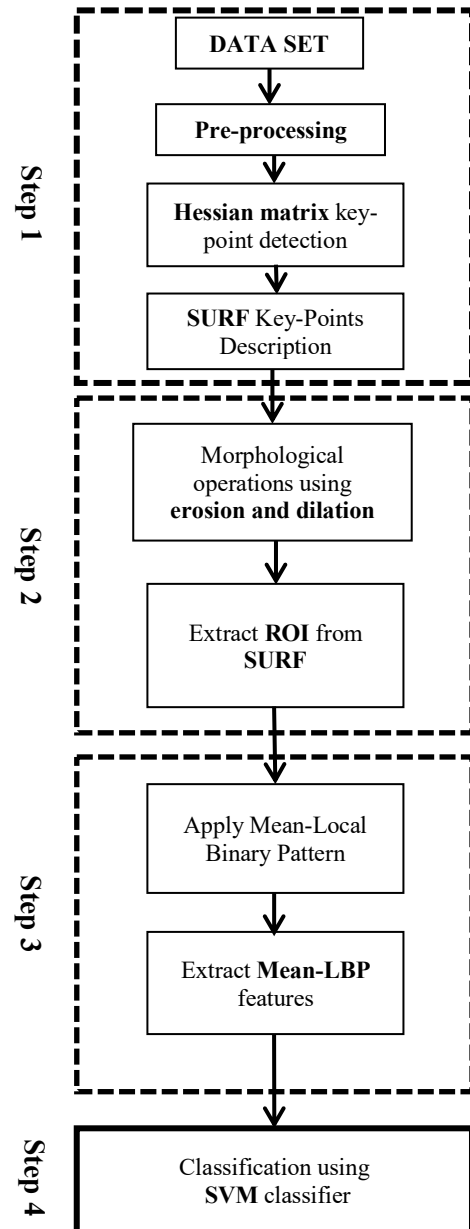


Figure 1. The suggested algorithm Block diagram

Create the vector feature. Different areas are utilized to choose the interest points such as blobs, corners, and T-junctions. An appropriate pointer ought to be rehashed where it can where recognize the comparable include highlights in different sees. overseeing the intrigued focuses can be done by orchestrating the edge and selecting the major highlights. Sudden change with the orientation of the frame and border on the object generates

interest points. As well as intersection among segmented edges yields interest points in an image.

Harris corner detector is one of the most famous corner-detector, nonetheless, it is not balanced invariant [19]. This problem was solved by T. Lindeberg [20] with the use of the Hessian matrix for automated system selection. Therefore, Hessian matrix approximation is used in SURF for detecting the image's interest points in both scale and rotation invariant. As well, to decrease the computational time. This technique helps the derivation of SURF to approximate Gaussian second-order but at a low computational time [21].

The whole picture of an image I is a medium representation, indicated by a point. It is computed by the summation of intensities between the point and the origin as in (1). to calculate the sum of the rectangular area that is used by the whole image we need four memory aperture and three additions.

$$I_{(x,y)} = \sum_{i=0}^{i \leq x} \sum_{j=0}^{j \leq y} I(i,j) \quad (2)$$

For the discovery of Interest Points, SURF uses the Hessian detector. The Hessian matrix relies on images integrations to lessen the time of computing and to obtain the main interest points in the scale space through the use of the non-maximal suppression.

An image with a point, the Hessian matrix of can be defined as the following:

$$H(x, \sigma) = \begin{pmatrix} L_{xx}(X, \sigma) & L_{xy}(X, \sigma) \\ L_{xy}(X, \sigma) & L_{yy}(X, \sigma) \end{pmatrix} \quad (3)$$

Where  $L_{xx}(X, \sigma)$ ,  $L_{xy}(x, \sigma)$ ,  $L_{xy}(X, \sigma)$ , and represents  $L_{yy}(X, \sigma)$  the convolution of the Gaussian at point P at the image I is the second-order derivative. By measuring the image's pixels and values we can determine the interest points, this is done by the Hessian method. [22]. determine points of the ( $Stji$ ) of every  $i^{th}$  image of  $j^{th}$  class, and passes it to step 2 for the get Region of Interest ( $ROI_i^j$ ).

### 3.3. Morphological Operations

Morphological filtering of an image includes transforming the image into a different image by applying a function or set, recognized as the structuring element. For the processing and analysis of binary and grayscale images Mathematical morphology is used f [23, 24, 25].

Region of Interest ROI extracted by performing the morphological operations using dilation and obtain the gradient masking of the image samples. Let M be a Euclidian space and I deals with the binarization of the image in E. The erosion of the image sample equals to the

$$A \ominus B = \{z \in M \mid B_z \leq E\} \quad (4)$$

where Z is the integer grid and B is the translation vector Pixels outside the image edge are assigned, the supreme value using the type of data. These pixels are set to 1 for binary type images.

Then dilation of the sample is performance which is obtained by:

$$A \oplus B = \{z \in M \mid (B_s)z \cap X_d \neq \emptyset\} \quad (5)$$

Where  $X_d$  is a shift-invariant operator on which it is performed?

Obtain the region of interests using (6) and evaluate the focus range among the nearest and farthest neighbors to find out the photometric attacks which has impact on both technical and aesthetic measure of the image samples.

$$F = (M_2 - M_1)^2 + (N_2 - N_1)^2 \quad (6)$$

### 3.4. Mean-LBP features of ROI

LBP is a limited operator that separates various types of textures. The primary LBP operator [10] portrays the images of each pixel classifications (LBP code). To calculate the LBP code, a comparison of 3x3 neighborhood pixel value against the threshold value is done. If the threshold value appears to be higher than that of neighboring pixel, then a binary digit 0 is held, otherwise 1 is held. Concatenation of the neighbor's binary digits is done for the purposes of creating a binary code. The decimal value for that particular's binary code is equal to the LBP. A perfect exemplar of the computation procedure of LBP code is portrayed in figure 4.

The LBP operator is represented by LBP\_ (P, R) and is defined in equation (7):

$$LBP_{p,r} = \sum_{i=1}^{p-1} S(P_i - P_c) 2^i \quad (7)$$

From the above equation, P is equal to the total pixels present in neighborhood, while R is the radius, and  $P_c$  is the value of central pixel, hence the threshold formula being defined in the following criterion:

$$S(P_i - P_c) = \begin{cases} 1 & P_i - P_c \geq 0 \\ 0 & P_i - P_c < 0 \end{cases} \quad (8)$$

The process of LBP computation commences by a perfect definition of T, the local 3x3 Cb image's neighborhood as the dual distribution of the 9 image pixels' grey levels, as it's shown in equation (9).

$$T = P\{g_0, g_1, g_2, g_3, g_4, g_5, g_6, g_7, g_8\} \quad (9)$$

Where  $g_i$  ( $i=0, \dots, 8$ ) and match up to the 3x3 neighborhood's grey scale values respective of spatial layout portrayed in figure 2. The neighbors' pattern is identified as the 'window', which slides the complete image pixel by pixel from left to right to the final column and the window reverts to the initial column via a top-to-down downward movement.

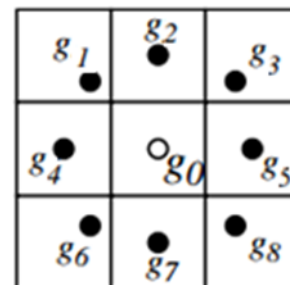


Figure 2. The circularly symmetric neighbor set of eight pixels in a 3x3 neighborhood

Mean LBP features computed on ROI constructed, same to the standard LBP computation just using mean value instead of center pixel, a comparison of 3x3 ( $g_p$ ) neighborhood pixel value against the threshold value ( $g_{mean}$ ) is done. If the threshold value appears to be higher than that of neighboring pixel, then a

binary digit 0 is held, otherwise 1 is held. The process is illustrated in Figure 3.

$$\text{mean}_{LBP} = \sum_{p=0}^{p-1} s(g_p - g_{\text{mean}})2^p, \quad s = \begin{cases} 1, & g_p \geq g_{\text{mean}} \\ 0, & \text{otherwise} \end{cases} \quad (10)$$

The computed on to extract the Mean-LBP features, is a neighboring pixel of the center pixel; represents the mean gray value of the cell.

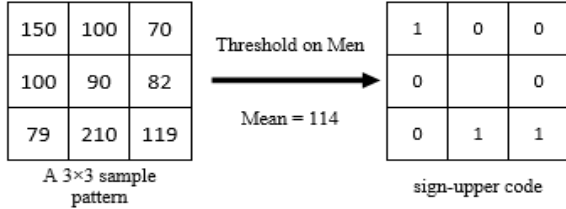


Figure 3. Calculation of sign-upper code using the (mean) threshold

Following the above theoretical explanation, an example is given below in figure 4 to show how the Mean -LBP is computed After completion, the next operation is to feed extracted features to SVM classifier.

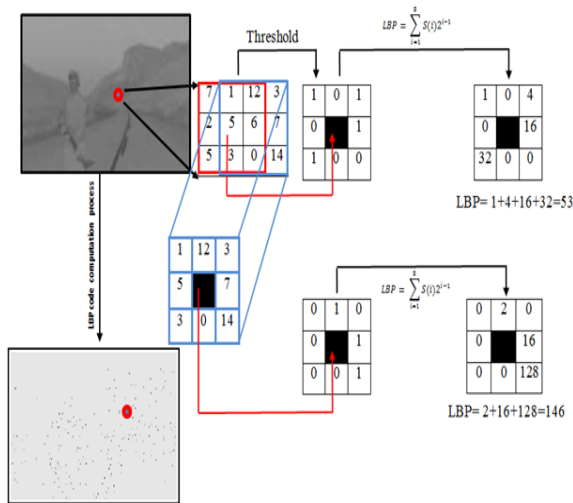


Figure 4. Mean-LBPed image generation

### 3.5. Classification

In the domain of pattern recognition, the Support Vector Machine application is widely used [7]. In our study, the SVM is trained to produce the image classifications, if it was authentic or tampered with. In general, SVM classifies the high-dimensional space by creating a hyperplane. As the interspace between the data of training-set of any of the classes and the hyperplane is the most comprehensive, it is set as the perfect separation. Given labelled samples of a training set:

$$K = (M_i, n_i) | m_i \in \{-1, 1\}_i^p = 1 \quad (11)$$

To separate the samples that have the most insignificant errors, SVM attempts to obtain a hyperplane.

$$wm - b = 0 \quad (12)$$

The input vector is represented by  $m_i$ , to achieve the classification process the distance from  $m_i$  to hyperplane is evaluated. one-against-rest strategy is used to perform the

multi-class classification desped of SVM being a binary classifier.

## 4. EXPERIMENT RESULT

### 4.1. Performance Evaluation

For assessing the execution of any procedure, a standard evaluation measure is needed to determine the scheme of pattern recognition or a classifier. Overall classification accuracy is used to measure the accuracy rate, this refers to the balance of successfully recorded test samples to the total number of tested samples. After evaluating the proposed method on the tampered Image Detection Evaluation CASIA V1.0, V2.0 and Columbia University even if there is no forgery detection the classification outcomes show an error in terms of forgery failure identification or successful discovery of the forgery.

There are several terms that are commonly used along with the description of sensitivity, specificity, and accuracy. They are true positive (TP), true negative (TN), false negative (FN), and false positive (FP). If a disease is proven present in a patient, and the given diagnostic test also indicates the presence of the disease, the result of the diagnostic test is considered true positive. Similarly, if a disease is proven absent in a patient, and the diagnostic test suggests the disease is absent as well, the test result is true negative (TN). Both true positive and true negative suggest a consistent result between the diagnostic test and the proven condition (also called the standard of truth). However, no medical test is perfect. If the diagnostic test indicates the presence of disease in a patient who actually has no such disease, the test result is false positive (FP). Similarly, if the result of the diagnosis test suggests that the disease is absent for a patient with a disease for sure, the test result is false negative (FN). Both false positive and false negative indicate that the test results are opposite to the actual condition.

Accuracy, Sensitivity and specificity are described in terms of TP, TN, FN and FP.

$$\text{Accuracy} = \frac{TN + TP}{TN + TP + FN + FP} \quad (13)$$

$$\text{Sensitivity} = \frac{TP}{TP + FN} \quad (14)$$

$$\text{Specificity} = \frac{TN}{TN + FP} \quad (15)$$

It can be recognized from Figure 5 that proposed method achieved the best detection performance on Columbia dataset with significant differences compared to CASIA TIDE V1.0 and CASIA TIDE V2.0. These outcomes support that the suggested method improves the detection rate of image forgeries due to its ability to capture the trace of tampering hat are not obvious visually that are affected by single or double photometric attacks, The performance of SURF and Mean-LBP further improves the results.

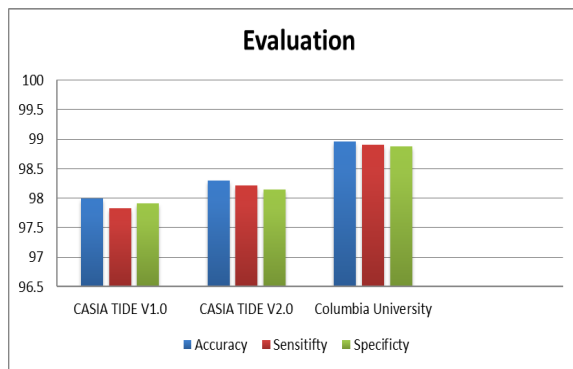


Figure 5. Experimental results from tampered images detection CASIA TIDE V 1.0,V 2.0 and Columbia University

The ROC curve shows the execution of the algorithm by charting rates of true and false positives in which deemed as varied discrimination threshold as show in figure 6. Likewise, in process of designating performance of proposed algorithm where this paper avoids specifying loss which it incurs when a false positive versus a false negative occurred. The results show that proposed method guides to a high level of efficiency.

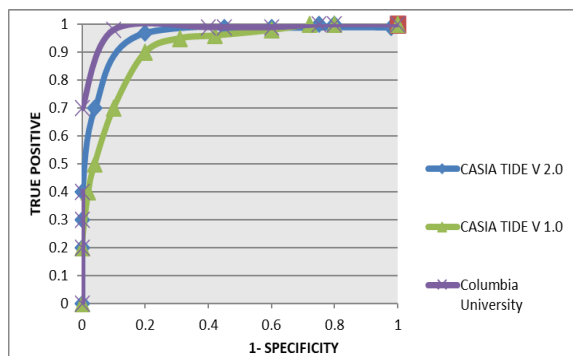


Figure 6. illustrate the ROC curve for the proposed system

Table 1. illustrate the Area under the curve for each feature.

CASIA TIDE V 1.0	CASIA TIDE V 2.0	Columbia University
0.979	0.982	0.989

A backpropagation of a 2-layer neural network is used in our structure, the training of the network was with 70%, testing 20% and validation with 10%. Figure 7 shows the best validation performance. It can be observed that the proposed SFD scheme outperformed the best recent works in this area.

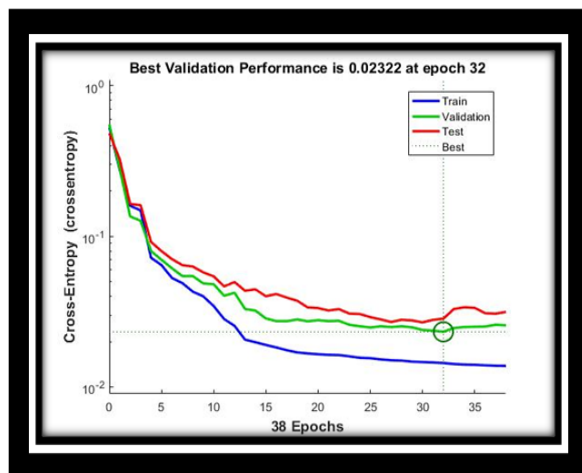


Figure 7. Training, validation and testing performance at epoch 32 shows the high validation performance (0.02322)

Table 2. Illustrates outcomes of comparison between method proposed by this study and other methods.

Methods	Columbia	CASIA v1.0	CASIA v2.0
Ref. [29](Manu and Mehtre, 2017)	98.08%	97.5 %	n/a
Ref[28](Li et al., 2017)	n/a	95.21%	92.38%
Ref.[27](Alahmadi et al., 2017)	97.77%	97%	97.5%
Ref.[26](Agarwal and Chand, 2018)	92.31%	96.8%	n/a
Our Method	98.9 %	97.9%	98.2%

## 5. CONCLUSION

The aim of this paper is to represent a novel image splicing forgery detection system that can handle the above-mentioned splicing tactics with improved accuracy rate. Thus, a new texture feature - based image splicing forgery detection is proposed to detect spliced image. The suggested technique uses SURF and Mean - LBP for image splicing detection. As well as SURF is used for the extraction Region of Interest (ROI) in an image based on morphological operations and Mean - LBP is used for feature extraction. The Mean - LBP Features obtained are then fed to SVM classifier to classify spliced image from authentic. In this paper, three standard datasets such as CASIA V1.0, CASIA V2.0 and Columbia, that contain all kinds of splicing tactics such as (blurring shallow depth, additive noise, edge smoothing, homogeneous region, and combined attacks et cetera) have been used to reconcile the copied area with full image in order to gauge the execution of proposed technique. It evident that, image-level of image splicing detection, the present method outperformed the best of the latest works in this area with accuracy rate of 97.9% CASIA TIDE V1.0, 98.2% CASIA TIDE 2.0, and 98.9% Columbia.

## REFERENCES

- [1] Fakery, P. (1999) 'The History and Techniques of Photographic Deception and Manipulation', Dino Brugioni. Brassey's.
- [2] Farid, H. (2009) 'Exposing digital forgeries from JPEG ghosts', IEEE transactions on information forensics and security. IEEE, 4(1), pp. 154–160.
- [3] Ardizzone, E., Bruno, A. and Mazzola, G. (2010) 'Copy-move forgery detection via texture description', Proceedings of the 2nd ACM workshop on Multimedia in forensics, security and intelligence - MiFor '10, p. 59. doi: 10.1145/1877972.1877990.
- [4] Sridevi, M., Mala, C. and Sanyam, S. (2012) 'Comparative study of image forgery and copy-move techniques', Advances in Intelligent and Soft Computing, 166 AISC(VOL. 1), pp. 715–723. doi: 10.1007/978-3-642-30157-5\_71.
- [5] Yatziv, L., & Sapiro, G. (2006). Fast image and video colorization using chrominance blending. IEEE transactions on image processing, 15(5), 1120-1129.
- [6] Tai, Y. H., Chuang, L., & Chen, C. H. (2001). U.S. Patent Application No. 09/444,141.
- [7] Hsu, J. C., Lee, H. L., & Chang, W. J. (2007). Flexural vibration frequency of atomic force microscope cantilevers using the Timoshenko beam model. Nanotechnology, 18(28), 285503.
- [8] Qu, Z., Qiu, G. and Huang, J. (2009) 'Detect Digital Image Splicing with Visual Cues.', Information Hiding, 5806, pp. 247–261. Available at: <http://dblp.uni-trier.de/db/conf/ih/ih2009.html#QuQH09>.
- [9] Kong, H. and Box, P. O. (2010) 'Proceedings of 2010 IEEE 17th International Conference on Image Processing IMAGE TAMPERING DETECTION BASED ON STATIONARY DISTRIBUTION OF MARKOV CHAIN National Laboratory of Pattern Recognition , Institute of Automation , Chinese Academy of Sciences ', pp. 2101–2104.
- [10] Zhao, T., Zhang, Z. N., Westenskow, P. D., Todorova, D., Hu, Z., Lin, T., ... & Clegg, D. O. (2015). Humanized mice reveal

- differential immunogenicity of cells derived from autologous induced pluripotent stem cells. *Cell stem cell*, 17(3), 353-359.
- [11] Kakar, P., Sudha, N. and Ser, W. (2011) 'Exposing digital image forgeries by detecting discrepancies in motion blur', *IEEE Transactions on Multimedia*, 13(3), pp. 443-452. doi: 10.1109/TMM.2011.2121056.
- [12] He, Z. et al. (2012) 'Digital image splicing detection based on Markov features in DCT and DWT domain', *Pattern recognition*. Elsevier, 45(12), pp. 4292-4299.
- [13] Hussain, M. et al. (2013) 'Image forgery detection using multi-resolution Weber local descriptors', *Eurocon 2013*, (July), pp. 1570-1577. doi: 10.1109/EUROCON.2013.6625186.
- [14] Su, B. et al. (2014) 'Enhanced state selection Markov model for image splicing detection', *EURASIP Journal on wireless communications and networking*. Springer, 2014(1), p. 7.
- [15] El-Latif, A. et al. (2019) 'A Passive Approach for Detecting Image Splicing using Deep Learning and Haar Wavelet Transform.', *International Journal of Computer Network & Information Security*, 11(5).
- [6] Abraham, A. R., Rahim, M. S. M., & Sami, A. S. (2020). Image Splicing Forgery Detection Scheme Using New Local Binary Pattern Variant. *Academic Journal of Nawroz University*, 9(3), 208-215.
- [17] Kadam, K., Ahirrao, S., Kotecha, K., & Sahu, S. (2021). Detection and Localization of Multiple Image Splicing using MobileNet V1. *IEEE Access*. <https://doi.org/10.1109/ACCESS.2021.3130342>
- [18] Zandi, M., Mahmoudi-Aznaveh, A. and Mansouri, A. (2014) 'Adaptive matching for copy-move Forgery detection', in *Information Forensics and Security (WIFS)*, 2014 IEEE International Workshop on, pp. 119-124.
- [19] Bay, H., Tuytelaars, T., & Van Gool, L. (2006, May). Surf: Speeded up robust features. In *European conference on computer vision* (pp. 404-417). Springer, Berlin, Heidelberg.
- [20] Lindeberg, T. (1998). Feature detection with automatic scale selection. *International journal of computer vision*, 30(2), 79-116.
- [21] Shivakumar, B. L., & Baboo, S. S. (2011). Detection of region duplication forgery in digital images using SURF. *International Journal of Computer Science Issues (IJCSI)*, 8(4), 199.
- [22] Mikolajczyk, K. and Schmid, C. (2001) 'Indexing based on scale invariant interest points', in *Proceedings Eighth IEEE International Conference on Computer Vision. ICCV 2001*, pp. 525-531.
- [23] Serra, J. (1982). Morphology for Grey-Tone Functions. *Image analysis and mathematical morphology*, 424-478.
- [24] Haralick, R. M., Sternberg, S. R., & Zhuang, X. (1987). Image analysis using mathematical morphology. *IEEE transactions on pattern analysis and machine intelligence*, (4), 532-550.
- [25] Maragos, P., & Schafer, R. W. (1987). Morphological filters--Part II: Their relations to median, order-statistic, and stack filters. *IEEE Transactions on acoustics, speech, and signal processing*, 35(8), 1170-1184.
- [26] Agarwal, S. and Chand, S. (2018) 'Image forgery detection using co-occurrence-based texture operator in frequency domain', *Advances in Intelligent Systems and Computing*, pp. 117-122. doi: 10.1007/978-981-10-3373-5\_10.
- [27] Alahmadi, A. et al. (2017) 'Passive detection of image forgery using DCT and local binary pattern', *Signal, Image and Video Processing*. Springer, 11(1), pp. 81-88.
- [28] Li, C. et al. (2017) 'Image splicing detection based on Markov features in QDCT domain', *Neurocomputing*. Elsevier, 228, pp. 29-36.
- [29] Manu, V. T. and Mehtre, B. M. (2017) 'Blind technique using blocking artifacts and entropy of histograms for image tampering detection', in *Second International Workshop on Pattern Recognition*, p. 104430T.
- [30] Zhao, X. et al. (2011) 'Passive detection of image splicing using conditional co-occurrence probability matrix', *APSIPA ASC 2011 - Asia-Pacific Signal and Information Processing Association Annual Summit and Conference 2011*.