DOI: 10.15439/2023R29
ISSN 2300-5963 ACSIS, Vol. 38

# Detection of Copy-Move Image Forgery Using Local Binary Pattern from Detailed Wavelet Coefficient

Daljeet Kaur
Department of Computer
Science & Engg
Gyan Ganga College of Technology
Jabalpur, India
daljeetkaur@ggct.co.in

Ajay Lala
Department of Computer
Science & Engg
Gyan Ganga College of Technology
Jabalpur, India
ajaylala@ggits.org

Kamaljeet Singh Kalsi
Department of Computer
Science & Engg
Gyan Ganga College of Technology
Jabalpur, India
kamaljeetsingh@ggct.co.in

***Abstract*—One of the most prevalent types of image forgery is copy-move forgery. A portion of the image is being copied and further pasted to a different location inside the identical image during the copy-move approach in order to hide a significant portion of the image. Finding duplicate portions in the image is the purpose of the copy-move based forgery detection technique. In this paper, we suggest a system which tends to detects forged portion in a forgery image. The DILBP (Detailed image local binary pattern) approach is used in this work to extract features, which includes extraction of feature, matching of feature, duplicate valued block detection. Several experiments have been initiated on a forged image to detect copy-move forged part. The experimental conclusions highlight that the suggested system is efficient for quality with respect to accuracy and speed.**

***Index Terms*—Image Forgery, DILBP (Detailed image local binary pattern), local binary patterns (LBP), set difference, Wavelet Decomposition.**

## I. Introduction

This Digital picture forgery is one of the often emerging difficulties in the realm of crime. There are currently no precise approaches available to automatically determine the authenticity and integrity of digital photographs. Typically, pictures have been used to verify the reality of an event. In the processing of image, the veracity of a digital picture can serve as crucial evidence. The detection of fraud in digital photographs is a developing study area for assuring the validity of the images. The availability of less expensive software and hardware tools makes it convenient to produce, edit and change digital photographs without leaving any visible signs that these activities have taken place. Regular newspapers, television, magazines, and the Internet disseminate a massive number of sophisticated archives that are produced by a variety of devices on a regular basis. In addition, by enhancing the capacity of image processing tools, modifying these pictures becomes quite easy. Pictures are crucial to communication across all of these channels.

Image forging is the process of making a false image by altering the actual image's content and passing it off as the original image for illegal purposes. The existence of digital picture authentication has received a significant deal of attention recently since digital media is now often employed in many security organizations as well as applications, making image fraud an important problem. Therefore, methods for identifying manipulated photos are now being researched. Different methods for manipulating images were created within a few years after photography was invented. Combination prints, which were produced by using darkrooms to print several portions of an image on a single sheet of photographic related paper, are one of the techniques that helped in the production of pictures. The Two Ways of Life by Oscar G. Rheinlander, which required up to 30 distinct negatives and it takes approx six weeks to create, contains the first well-known combination prints.

Humans may now readily obtain engaging multimedia from the internet and alter or modify it as they see fit, thanks to advancements in technology and the ease of use of the internet. There are two common methods of manipulating images: region duplication by copy-move forgeries and image splicing. During image splicing, portions of different photographs are combined to produce a manipulated image. On the other hand, image sections are copied and pasted onto the same image in copy-move forgery in order to increase or hide some significant content in the image.

It becomes difficult to distinguish between tempered and legitimate sections when copied regions appear to be identical with compatible components (such as color and noise). In addition, a counterfeiter employs several post-processing techniques like noise reduction, edge smoothing, and blurring to eliminate any visible indications of image manipulation. One unique form of forgery is called "copy-move forgery imaging," in which portions of a picture are copied and then pasted back into the original. Because of this, picture forensics and copy-move forgery detection have grown in significance in our networked culture.

The proposed work aim to design a detection system which detect forged image of copy-move forgery type. In the proposed system, digital image is divided into overlapped blocks. After that, the feature extraction approach has been applied on the forged image to extract the particular features from particular image block. Further duplicate blocks have been detected, which indicated the forged portion of an image. Some the sample forged image and original images have been shown in “Fig. 1-a”and “Fig. 1-b”.

The primary information carriers in the modern digital environment are digital photos and movies. However, the validity and integrity of the digital images are a major cause for concern because these information sources are easily manipulated using widely available software. Furthermore, the most common method of altering digital photographs is copy-move image forging. A specific kind of image manipulation known as "copy-move forgery" involves copying and

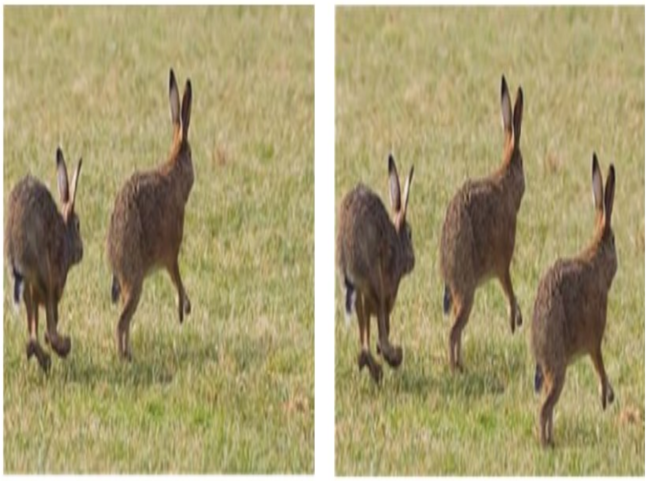

Fig. 1-a Actual image/ Corresponding Copy- move forged image.

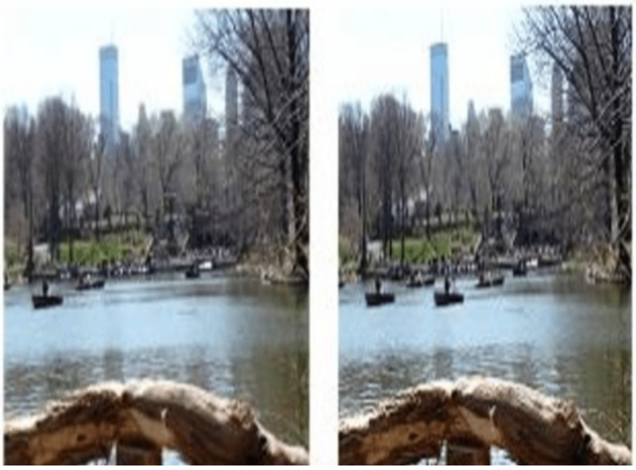

Fig. 1-b Actual image/ Corresponding Copy- move forged image.

pasting an image portion in a different location with the goal of hiding a significant aspect of the original image. Therefore, finding identical or strikingly similar image regions is the aim in the detection of copy-move forgeries.

The following are further enumerated in the paper. A review of the relevant studies is provided in Section 2. Section 3 describes the suggested image forgery detection method. Section 4 presents the outcomes of the experiments, and Section 5 wraps up the work. Beginning with the extraction of a section of the input image or a model of 3D object, image forgeries are created. Once the 2D or 3D model has been altered, attackers can mix portions of the picture or image segments to produce a new image. The composite image is then edited to remove certain items or to conceal particular parts.

## II. Related Work

Guiwei Fu et al. [1] suggest an image copy-move forgery detection method based on fused features and density clustering. Tahaoglu, et al. proposed digital image copy move forgery based detection system which need to be implemented in the environment of real time[2].They suggested a strategy that starts by removing the input image's textural form. A Ciratefi-based method is used to localize the faked pixel. A novel technique was suggested by R. H. et al.[3] to detect the copy-move forgery, which is the most common type of forgery attack. The detection and localization of forgeries is a notable issue that has drawn and continues to draw the attention of academics working in the area of digital based forensics, according to Pranshav Gajjar et al. [4]. To enable accurate localization of the tampered area, Mauro Barni and colleagues [5] devised a technique to determine the copy-move forgery's source and target locations. Agarwal R et al.[6] In order for our system to identify the tampered region, the suggested technique initializes the tampered image as the input. When using SIFT characteristics, Fontani et al.'s J-linkage approach and copy-move detection idea were proposed [7] in 2013. A classification-based attack (CLBA) technique is suggested by Muhammad et al.[8] in 2012 for the identification of tempered pictures. Sunil et al.[9] determines the state of One post-processing action that the attacker might use to get around image forgery detection techniques is changing the intensity of the copied portion. The introduction to the bibliography on the blind picture forgery detection technique is provided by Mahdian et al[10]. A block-based technique was proposed by Edoardo [11] in which texture is taken from the block and used as a feature.

Copy-move forgery detection methods in digital photos, databases, and evaluation metrics are surveyed and compared by Sami Gazzah et al[12]. The study attempts to shed light on the relative efficacy of several techniques for identifying copy-move frauds. Several popular detection strategies are included in the study, such as deep learning, GAN, hybrid, transform domain, block-based, keypoint-based, and hybrid approaches. K. Latha et al.[13] successfully identify whether a picture has been edited and prevent users from trying to submit modified photographs by using a machine learning algorithm (SVM). The integrity and authenticity of digital photographs are now questioned, undermining consumer confidence in them due to recent advancements in image altering software.

Using deep learning to train a Convolutional neural network (CNN) on a dataset of real and fake photos, Devarshi Patrikar et al.[14] conduct an extensive investigation of image forgery techniques. GAN stands for generative adversarial network. They conclude that deep learning has demonstrated encouraging results for image forgery detection and is an active field of research despite a number of obstacles. By using a hybrid Deep Learning (DL) architecture, D Prabakar et al.[15] create a very powerful and efficient detection approach for this kind of image counterfeiting. To begin with, MICCF2000 is the source of the sample images. Secondly, the photos are resized, and any noise that may have existed in the original image is removed using a filtering approach. Ultimately, we construct a hybrid deep learning model by fusing support vector machines (SVM) and convolutional neural networks (CNN). The created hybrid deep learning model is verified using metrics like precision, F1-score, True Positive Rate (TPR) and Negative Rate (TNR), False Positive Rate (FPR) and Negative Rate (FNR), and accuracy.

With an emphasis on frequently occurring copy-move and splicing attacks, Zanardelli et al.[16] explore some of the most recent image fraud detection algorithms built specifically upon Deep Learning (DL) techniques. Insofar as DeepFake-generated content is applied to photographs, it is also addressed, producing an effect akin to splicing. Given that deep learning-powered techniques yield the best overall outcomes on the benchmark datasets that are currently available, this survey is very pertinent.

A technique proposed by Dipanshu Narayan et al.[17] to identify copy-move forgeries is based on breaking down blocks into features and then extracting those features from the transforms of the blocks. An additional instrument for identifying forgeries is a Convolutional Neural Network (CNN). To extract features, convolution and pooling layer pairings in serial fashion are used.

## III. Proposed System

The primary goal of this forgery region work is to highlight related regions in image that may vary in size and form. A difficult task is the approach of pixel to pixel comparison in order to locate the identical areas. In order to create a forgery detection system that is both effective and efficient, a logical window has been constructed. This sliding window shifts in accordance with size of window across the entire picture to obtain the photographs' feature vector. The regions have been regarded as a single block that is protected by sliding windows. The repositioning of the window has therefore resulted in the creation of one additional block.

For each potential block, values of feature in matrix format, which reflect the potential block values, have been retrieved by the system. With the aid of a sliding window, the input picture is split into small blocks of the similar size at the beginning. The feature extraction approach has been used on every potential block. DILBP (Detailed image local binary pattern), which combines the local binary pattern approach and detailed coefficients based wavelet transformation, is the suggested feature extraction strategy for each of the blocks as shown in “Fig- 2”.

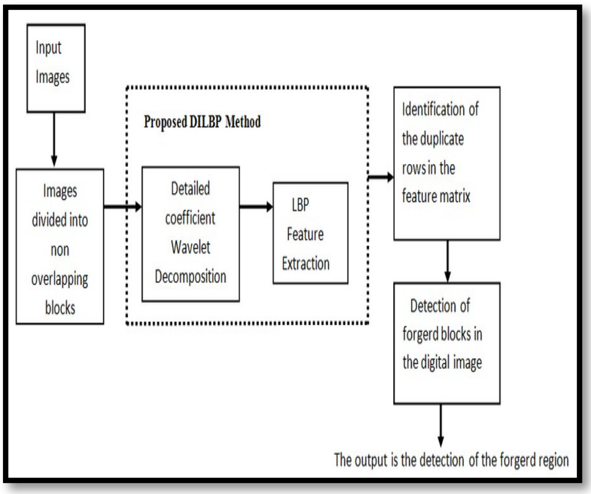
Input Images
Images divided into non overlapping blocks
Proposed DILBP Method
Detailed coefficient Wavelet Decomposition
LBP Feature Extraction
Identification of the duplicate rows in the feature matrix
Detection of forgerd blocks in the digital image
The output is the detection of the forgerd region

Fig-2. Work flow of the proposed system

### A. Proposed algorithm

#### 1) Overlapped Blocks Creation

With this method, the fake picture is first split into overlapping sections. Here, the fundamental technique is to find interconnected blocks that have been duplicated or relocated. There are several overlapping blocks in the forged area. Extraction of features from these blocks would come next.

#### 2) Technique For Feature Extraction

The forged image was subjected to the feature extraction technique in order to extract specific features from a block of the image after the overlapped blocks were generated. In order to extract features from the block region, the detailed image local binary pattern features method is used in this activity.

### B. DILBP (Detailed image Local Binary Pattern)

Face photos have been converted into detailed images using a bi-level wavelet decomposition technique. Local binary patterns (LBP) have then been used to extract local aspects of the fake images from detailed coefficients-based deconstructed images. The accurate and efficient DILBP approach combines the long-running LBP method with comprehensive coefficient-based wavelets decomposition. Detailed coefficients based wavelet decomposition.

### C. Detailed coefficients based wavelet decomposition

This decomposition technique makes use of signal and temporal analysis. It can be applied to deconstruct a bogus image into multiple sub-band images with different directional attributes, spatial resolution, and frequency characteristics. In this method, the forged image is broken down into up to two layers in order to calculate the approximation and details coefficients. Details coefficients do not contain the highest frequency component of a picture, in contrast to details coefficients, which do. In this investigation, only the detailed coefficient has been used further during the complete process.

The forgery's high frequency region is the only component of the picture that is altered by the small scale obstruction and expression modifications. For forged images, any additional decomposition processes cause information loss and are thus not included in this study.

### D. Principles of local binary pattern

The output of the wavelet has been used to local binary pattern (LBP), where the original picture has been divided into tiny sections from which the local binary patterns or histograms have been extracted. As seen in figures. 3 and 4, distinct LBP histograms were derived, which depict circular neighbor-sets for three distinct values of R and P. The display of the fake picture is created by concatenating all of the blocks of the fake image into a single feature histogram.

As illustrated in "Fig-3," the feature vector of the image can be generated [18] after the evaluation of the local binary pattern (LBP) for every individual pixel.

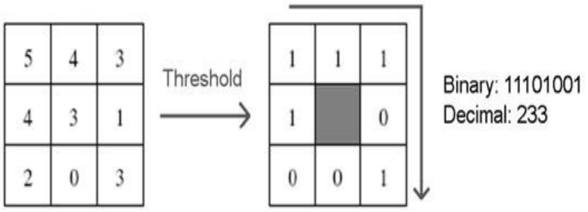

Fig-3. The actual LBP Operator (source of image: [18])

The threshold value is used as the centre pixel's value by the basic LBP operator, which operates on the values of the eight neighbors' pixels. If the grey value of a neighboring pixel is equal to or greater than that of the centre pixel, then

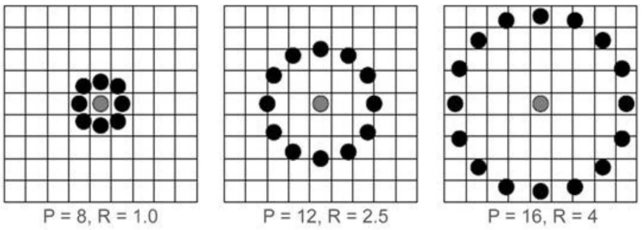

Fig-4. Neighbor-sets for three distinct P and R (source of image: [18])

one is assigned to specific pixel; else, zero is assigned to it. The LBP code is then created for the centre pixel value by concatenating 8 zeros or ones to create a binary code [18], as seen in “Fig-4”.

The LBP based operator's borders have expanded further to employ various sizes relevant to the neighborhood. A circle with radius R has been drawn starting from the centre pixel. The values of the centre pixels and the hypothetical P sampling sites on the circumference of the particular circle are compared. (Dual) interpolation is required to extract the numerical values of every neighborhood sample point for any number of pixels and radius. Figure 4 illustrates the notation (P, R) that has been used for the particular neighborhood.

### 1) *Duplicate Rows identification in a feature matrix*

Each row in the feature matrix represents a certain block. To find the duplicate rows, the system first counts how many rows in the feature matrix are being compared to the filtered out rows that remain duplicates. Consequently, the blocks with repeated entries in the feature matrix are the outcome of this comparison.

### 2) *Forged region Detection*

The next stage is to expose the identical blocks of digital image, which also serves as a warning sign for counterfeit areas, after identifying blocks that behave identically. Thus, the machine finally finds a fake area in the digital image. The system is highlighting the specific forged locations.

When using the DILBP technique for extraction of feature, the computing time of the entire process is lowered when the LBP approach is combined with wavelets. This increases the system's efficiency and tends to enhance the effectiveness of forgery detection system.

## IV. Result of Experimental Analysis

An Intel (R) Core (TM) i3-3120M CPU running at 2.50 GHz with 4GB of random access memory has been used to test the proposed system. All activities connected to simulations are carried out using the MATLAB platform. As seen in Table I, which shows the sizes of two images—one is titled "River and Tree Image" and the other is titled "House and Chimney Image"—the performance is evaluated by looking for forged portions in the digital image. An additional column in the Table I. shows specific blocks size which are represented by each row in the feature matrix. Execution Time indicates the time taken to detect the forged part. Last entry in the Table I. show the no of forged blocks detect by the proposed system.

Adobe Photoshop 7.0 was used to create the equivalent set of forged pictures, which were then saved in the 275 * 275 , 300 * 300 png format. A sliding window with a size of 26 by 26 is being placed on each individual pixel. To get the results of the experiment on picture forgery, the suggested DILBP approach is being used to the faked photos. Following the application of the suggested detection of image forgery method, we obtain a forged part in the forged images and corresponding forged areas are emphasized by the block-based system that are exactly similar to one another from every angle, as shown in “Fig-5.1” and “Fig-5.2”, which effectively indicates the forged image.

Table I. Performance Table

| Sr No | Image Size | Block Size | Execution Time | No of duplicate blocks identified |
|---|---|---|---|---|
| 1. | River and Tree image<br>275 ×275 | 23 × 23 | 0.32 sec | 1 |
| 2. | House and Chimney Image<br>300 × 300 | 34 × 34 | 0.50 sec | 1 |

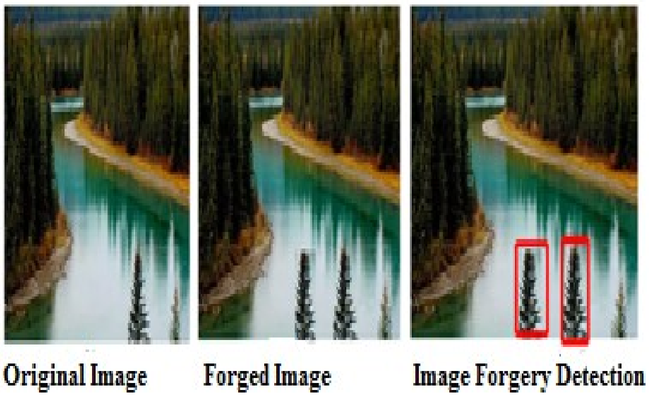

Fig-5.1. Detection of Forged part Results I

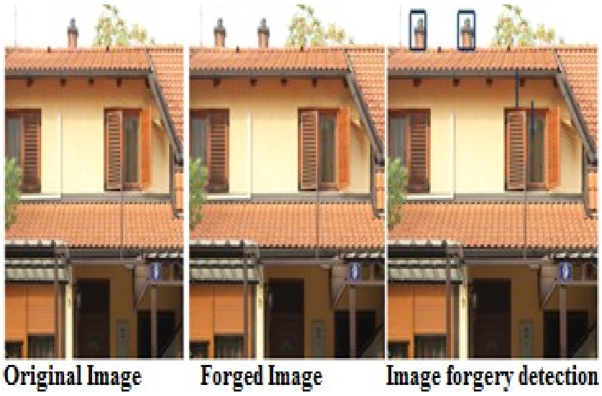

Fig-5.2. Detection of Forged part Results II

## V. Conclusion

This proposed study use the DILBP approach, which incorporates the wavelet decomposition's detailed coefficient characteristics, to recognize the copy-move forged picture. The research covered in this paper yields a good outcome for detecting fabricated regions. The improvement of time complexity to detect the forged region will be the next step in the future. Also, the proposed system as the proposed approach aims to detect forged portion in still forged images only, in future next step will be to detect forged portion in video also.

## References

[1] Image Copy-Move Forgery Detection Based on Fused Features and Density Clustering, Guiwei Fu, Yujin Zhang, Yongqi Wang, et al., Appl. Sci. 2023, 13, 7528. This link points to 10.3390/app13137528.

[2] Tahaoglu, G., Ulutas, G., Ustubioglu, B., et al. Digital picture copy move forgery detection using a Ciratefi approach. 81, 22867–22902 (2022) Multimed Tools Appl. This link points to 10.1007/s11042-021-11503-w.

[3] R. H. Jaafar, Z. H. Rasool and A. H. H. Alasadi, "New Copy-Move Forgery Detection Algorithm," 2019 International Russian Automation Conference (RusAutoCon), Sochi, Russia, 2019, pp. 1-5, doi: 10.1109/RUSAUTOCON.2019.8867813.

[4] Pranshav Gajjar et al 2022, "Copy Move Forgery Detection: The Current Implications and Contemporary Practices", in International Conference on Electronic Circuits and Signalling Technologies", doi:10.1088/1742-6596/2325/1/012050.

[5] Phan QT, Tondi B, Barni M (2021) Transfer source-target disambiguation via multiple branch CNNs in a copy manner. 16:1825–1840 IEEE Trans Inf Forensics Secur.

[6] Verma O, Agarwal R (2020) An effective deep learning feature extraction and matching technique for copy move forgery detection, Multimedia Tools and Applications, number 79, pages 7355–7376 (2020).

[7] A Framework for Decision Fusion in Image Forensics Based on Dempster-Shafer Theory of Evidence, Marco Fontani, Tiziano Bianchi, Alessia De Rosa, Alessandro Piva, and Mauro Barni, IEEE Transactions on Information Forensics and Security, Vol. 8, no. 4, April 2013.

[8] Gandhim Muhammad, Hussain, and George Bebis, "Undecimated dyadic wavelet transform for passive copy move image forgery detection," Elsevier, 2012.

[9] Kumar Sunil, Desai Jagan, Mukherjee Shaktidev, "DCT-PCA Based Method for Copy-Move Forgery Detection", ICT and Critical Infrastructure: Proceedings of the 48th Annual Convention of Computer Society of India- Vol II, 2014, Volume 249

[10] Mahdian B, Saic S. A bibliography of techniques for detecting image forgeries without sight. 2010;25(6):389–399. Signal Processing: Image Communication.

[11] Giuseppe Mazzola, Alessandro Bruno, and Eduardo Ardizzone, "Copy-Move Forgery Detection via Texture Description," Proceedings of the 2nd ACM symposium on Multimedia in forensics, security, and intelligence, 2010, pp. 59-64.

[12] Sami Gazzah; Lamia Rzouga Haddada et al. "Digital Image Forgery Detection with Focus on a Copy-Move Forgery Detection: A Survey" in 2023 International Conference on Cyberworlds (CW), DOI: 10.1109/CW58918.2023.00042.

[13] K. Latha; D. Kavitha; S. Hemavathi et al. "Image Forgery Detection Using Machine Learning" in 2022 International Conference on Power, Energy, Control and Transmission Systems (ICPECTS), DOI: 10.1109/ICPECTS56089.2022.10046422.

[14] Devarshi Patrikar; Usha Kosarkar; Anupam Chaube "Comprehensive study on image forgery techniques using deep learning" in 2023 11th International Conference on Emerging Trends in Engineering & Technology - Signal and Information Processing (ICETET - SIP), DOI: 10.1109/ICETET-SIP58143.2023.10151540.

[15] D Prabakar; R. Ganesan; D. Leela Rani; Praveen Neti et. al. "Hybrid Deep Learning Model for Copy Move Image Forgery Detection" in 2022 Sixth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC) , DOI: 10.1109/I-SMAC55078.2022.9987319

[16] Zanardelli, M., Guerrini, F., Leonardi, R. *et al.* Image forgery detection: a survey of recent deep-learning approaches. *Multimed Tools Appl* **82**, 17521–17566 (2023). https://doi.org/10.1007/s11042-022-13797-w

[17] Dipanshu Narayan; Himanshu; Rishabh Kamal "Image Forgery Detection" in 2023 International Conference on Disruptive Technologies (ICDT), **DOI:** 10.1109/ICDT57929.2023.10151341

[18] Md. Shafiul Azam, Tanzillah Wahid, Md. Abdur Rahim, and Md. Najmul Hossain, "Face Recognition using Local Binary Patterns (LBP)" in Global Journal of Computer Science and Technology Graphics & Vision, Volume 13 Issue 4 Version 1.0, (2013).