IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

FORENSIC VERIFICATION TO DIFFERENTIATE BETWEEN REAL AND FAKE IMAGES

[1]Swapnil S. Pawar, [2]Kushal R. Dogra, [3]Prof. Dr. S. M. Kamalapur, [4]Pranav A. Varpe, [5]Shubham R. Dhanwat
[1,2,4,5] Students, Department of Computer Engineering
[3]Professor, Department of Computer Engineering
K. K. Wagh Institute of Engineering Education & Research, Nashik(SPPU), Maharashtra, India

Abstract: Multimedia security is one of the most significant issues all are currently facing because of the reliance society is on multimedia information, that is increasing each day. Every normal user of a smart phone or computer today has access to affordable image editing software that enables users to modify the information present in images and videos in a particular manner. The authenticity of the images must be verified by the detection of image tampering.To restore the public's faith in visual media, forgery detection in digital images is vital. Hence, forensic verification of digital images is an essential area of research to distinguish between authentic and altered images, notably in the caseof copy-move and splicing forgeries. Copy-move detection seeks to locate areas of an image that have been copied andpasted elsewhere, whereas splicing detection seeks to locate areas of other images that have been combined to producea fake image. This paper addresses a system that consists of two methodologies for copy-move detection: CFA Artifacts and the DBSCAN clustering algorithm, a methodology for splicing detection: ELA (Error Level Analysis) as well as a method for double compression detection. These methodologies can be used to accurately identify copy-move and splicing forgeries in digital images, which is useful in a variety of sectors such as law enforcement, multimedia, and digital forensics.

Index Terms - Forensic Verification, Copy-Move Forgery, Splicing Forgery, CFA Artifacts, Clustering Algorithms, Error Level Analysis (ELA), Deep Learning

1. Introduction

Forensic verification of images is becoming increasingly important due to the rise of digital manipulation and image editing software. In recent years, the proliferation of fake images on social media platforms and online news sources has seriously harmed both people and organizations. This has brought attention to the necessity for trustworthy and precise techniques to distinguish between real and fake images. Today, everyone with a smart phone or computer has access to reasonably priced image editing software, which enables users to change the data contained in images and movies in someway. The detection of image manipulation is necessary to confirm the reliability of the images.

Copy-move and splicing forgeries are two of the most popular types of image forgeries. Splicing forgeries combine portions from multiple images to generate a fake image, whereas copy-move forgeries use copying and pasting specific sections of an image to make a replica within the same image. Detecting these forgeries is crucial in maintaining the integrity of digital images. Forensic experts face significant challenges in detecting these forgeries and verifying the authenticity of images.

For detecting these forgeries, several methodologies have been put forward, including CFA Artifacts and the DBSCAN clustering algorithm for copy-move detection, and ELA (Error Level Analysis) and CNN for splicing detection. The CFA Artifacts method use statistical analysis to spot irregularities in color filter array patterns brought on by copy-move manipulation. The DBSCAN clustering algorithm, on the other hand, groups comparable image regions to identify copy- move forgeries. For splicing detection, ELA uses differences in compression quality to identify regions of an image that have been spliced together, while CNN is used to build a model able to classify the image as real or fake depending on ELA of splicing image.

In this paper, these methodologies are explored in depth and presented an overview of their efficiency in detecting copy-move and splicing forgeries. The paper also addresses the significance of forensic image verification and the implications of image tampering in many sectors. In the end, this research hopes to support the creation of dependable andefficient methods for detecting fake images and ensuring the trustworthiness and authenticity of digital evidence.

The contents of this work are organized as follows: Section 2 reviews related work. Section 3 describes our methodologies in detail with corresponding algorithms and block diagrams. Section 4 presents our experimental results and relevant performance analysis. Finally, Section 5 presents our conclusions.

2. Literature Survey

Image forgery detection is an area of research that has gained considerable attention in recent years due to the increasing prevalence of digital image manipulation and the potential misuse of such manipulations. Image forgery can bedefined as the deliberate alteration of an image with the intention to deceive viewers. With the rise of digital media and theavailability of image editing software, image forgery has become more prevalent, making it necessary to develop techniques to detect and prevent such manipulations.

On a target image, an attacker is able to make one or a series of subsequent alterations, either to the entire image or just to a tampered area, such as a semantic alteration, e.g., object duplication, JPEG compression, geometric transformations, up-sampling, filtering, and so on. Antiforensics is employed when an attacker uses this series of modifications to mask the initial forgery. A. Dixit reviewing some of the studies discussing image forgery [7] this researchsummarizes some methods of image forgery and its application which are discussed below in brief.

Copy-move forgery is one of the most common types of image forgery techniques. D. Chauhan in the paper [16] mentions different sections of an image are duplicated and transferred to different positions inside the same picture in copy-move forgery. In terms of characteristics, different regions of a picture are tightly connected. To calculate abrupt features,divide a picture into overlapping or disjoint chunks, or compute local key points for the whole image. These features playa key role in copy-move forgery detection [15]. Operations such as cropping, conversion of an RGB image to grayscale, DCT or DWT transformation are all managed by Pre-processing in order to improve the classification performance [14] Jeronymo DC uses Feature Matching to compare the selected features of every block to the other to find any similarity [13]. By highlighting the corresponding blocks in an image, forgery can be discovered.

The most prominent kind of image Forgery is image splicing. In the world of images, numerous techniques for detecting image splicing have been presented. Khalid M. Hosny mentions that splicing detection can often be divided intotwo kinds. Extract the features using support vector machines (SVM) and the orthogonal moments.[4] Traditional approachesfor extracting features include Markov features in discrete cosine transform (DCT) and discrete wavelet transform (DWT).The second strategy uses a variety of deep learning techniques to detect image splicing forgeries (ISFD).

A forensic technique called error level analysis (ELA) uses various degrees of compression to analyze images. Luo, W presented error level analysis (ELA) for the identification of image piracy [24]. Dua introduced a technique based on JPEG compression in paper on Robust copy-move forgery detection [22]. A block of an image that has been divided into non-overlapping blocks of size 8x8 pixels is evaluated separately for each block's discrete DCT coefficients. When a JPEGcompressed image falters, the statistical characteristics of the AC components of the block DCT coefficients change. The recovered feature vector is utilized to categorize genuine and fake images using the SVM. Ehret presented a method for forgery detection in [23] that uses SIFT and gives sparse key points with scale, rotation, and illumination invariant descriptors. Using an effective and reliable strategy, Mohammad F.H. evaluated accuracy, recall, and false positive rate while combining undecimated wavelet transform with scale invariant feature transform [5] One method for identifying altered images is error level analysis, which involves storing images at a specific quality level and comparing the differenceto the compression level [12].

Popescu A. discuss the procedure for detecting CFA artefacts in [9]. The Fourier transform (FT) of the picture is determined and calculate the probability map of the presence/absence of CFA artefacts. The presence of CFA artefacts in the image is shown by spikes in the Fourier domain, which are proof of the map's periodicity. Similar to this, Gallagher Ain [8] suggested a method for identifying the nature of pictures (whether the pictures were captured with a digital device or intentionally made), based on the fact that CFA artefacts have a periodic structure. This approach is likewise based on FT analysis. A CFA filter was not utilized in the registering device if there are no CFA artifacts in a certain picture region,which suggests that the area has been manipulated.

The research [20] presents a novel way to enhance copy-move forgery detection based on neural networks and deep learning, focusing on the convolutional neural network architectural approach. The recommended solution makes use of aCNN architecture with pre-processing phases to provide good results. In order to identify copy-move forgeries, the study
[21] employs a fusion processing approach that combines a deep convolutional model and an adversarial model. In this experiment 4 datasets were used. The findings reveal that the forgery detectors for deep learning CNN and discriminator have an 85% detection rate. The network is constructed using a fusion module and a two-branch configuration. The two branches are utilized to find and recognize copy-move forgery areas with CNN and GAN.

According to Chen's [1] study, a tailored Convolutional Neural Network (CNN) may be used to detect median filteringusing JPEG post-processing. After median filtering, the forensic task became more challenging since JPEG compression may partially conceal the forensic evidence of medial filtering. The Median Filtering Residual (MFR) rather than the raw
pixel data was given to the first layer of the modified CNN. The MFR is the difference between a picture and its median filtered representation. In terms of forensic categorization, the network performed better. More recently, Tang [2] proposedto upscale the input with closest neighbor interpolation in an effort to increase the difference between altered and originalpatches.

Data mining and machine learning frequently employ the clustering technique known as Density-Based Spatial Clustering of Applications with Noise (DBSCAN). It has also been used in picture forgery detection in recent years. A Hegazi used DBSCAN for image forgery detection is that it can identify clusters of pixels that have similar color or textureproperties in an image. By clustering these pixels, it can help detect regions of an image that may have been tampered withor manipulated.

3. Methodologies

This section illustrates the details of the methodologies used. The two most significant forgeries, Copy-Move Forgeryand Splicing Forgery, are detected using the suggested techniques.

3.1. Copy-Move Forgery

Copy-move forgery is the technique of copying and pasting an image's portion into another portion of the same imageto create a new image. It is possible to move the piece that was copied and pasted anywhere inside the same image or intoa different image. The goal of copy-move forgeries is often to persuade onlookers that the image is real and unaltered. Copy-move forgery is a fairly straightforward process that can be carried out with the aid of easy-to-use picture editing software like Adobe Photoshop. The forger chooses a portion of the original image to copy, and they then paste it into another region of the same image. To decrease the sight of the forged, the pasted section can then be blended with the surrounding pixels using the clone stamp tool or other editing tools.

One of the most common methods for identifying copy- move forgeries is based on the idea that when a piece of a picture is copied and pasted, there will be sections that are the same or very similar to the original. This can be discoveredusing algorithms that search for regions of a picture with similar pixel values or texture patterns. Other strategies to identifycopy-move forgeries include looking at the image's metadata, inspecting the image for imperfections in lighting and perspective, and looking for signs of cloning or other editing techniques. To summarize, copy-move forgery is the practiceof copying and pasting an element of an original image to create a new one. It is a common sort of digital image fraud. It has many applications and is occasionally difficult to notice with the unaided eye. Digital forensic techniques can be usedto identify copy-move forgeries and determine whether a picture has been manipulated.

For the purpose of detecting copy-move forgeries, DBSCAN Clustering Algorithm and CFA Artifacts Detection methodologies have been used.

3.1.1. DBSCAN Clustering Algorithm

The DBSCAN clustering method detects copy-move forgeries by combining the Scale-Invariant Feature Transform (SIFT) feature descriptor and the Density-Based Spatial Clustering of Applications with Noise (DBSCAN) algorithm.

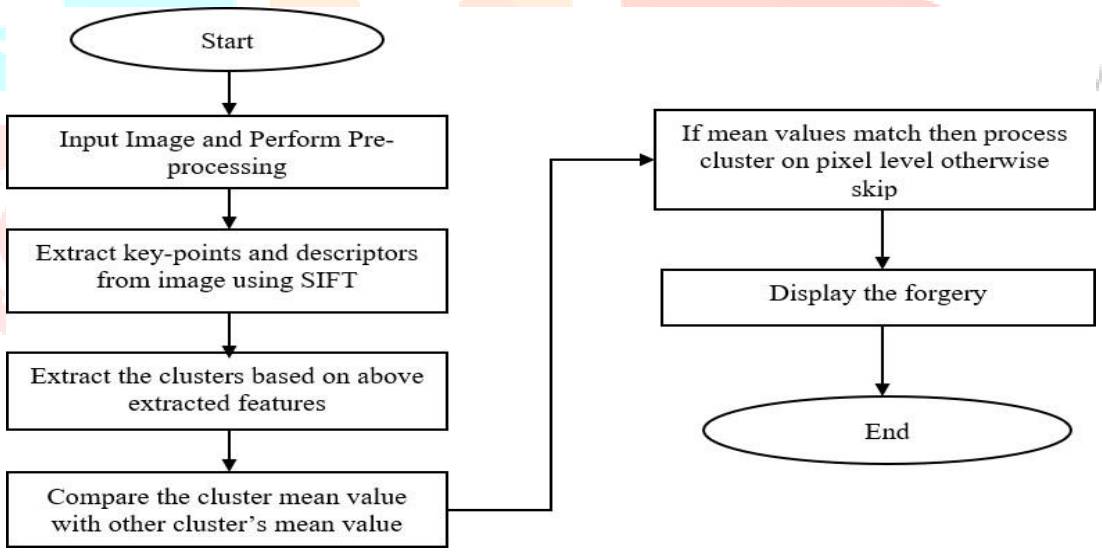

Figure 1: Flow Chart

The **algorithm** is as follows:

1. Read the input image, first.
2. Use the SIFT create function to extract SIFT key-points and descriptors from the input image.
3. Use (eps, min_samples) as input parameters in DBSCAN clustering on SIFT descriptors to define the maximum distance between points in the same cluster and the minimum number of points required to form a dense region that can be considered as a cluster.
4. Group key-points according to the SIFT descriptors. Each group is a collection of key-points with related characteristics.
5. On a duplicate of the input image, locate clusters that include many key-points and draw green lines connecting them.
6. Send back the updated image with the green lines. In the absence of forgery detection, return None.

The above algorithm finds groups of key-points with related characteristics and so identifies copy-move forgeries.Based on how similar their SIFT descriptors are, key-points are grouped using the DBSCAN clustering algorithm. Green lines are drawn between the cluster's key-points to emphasize the forgery regions, which are clusters containing more thanone key-point. The modified input image from the algorithm has green lines drawn between the key-points in the forged regions. The result is None if no forgery is found.

Note that the DBSCAN clustering algorithm requires two input parameters, eps and min_samples. These parameters regulate how the algorithm clusters data. The min_samples option defines the least number of points necessaryto construct a cluster, while the eps parameter determines the maximum distance between two points within the same cluster. Depending on the properties of the input image and the anticipated forgery patterns, the eps and min_samples values can be changed.

3.1.2. CFA Artifact Detection

CFA (Color Filter Array) artifacts are visible defects in digital images caused by the demosaicing process. Digitalcameras use the demosaicing technique to transform the sensor's raw data for images into a full-color image. In this process,a color filter array is used to filter light into red, green, and blue channels. The result of interpolating these channels is a full-color image. In digital cameras, the demosaicing process introduces CFA artifacts. These camera-specific artifacts canbe used as a signature to determine whether or not an image has been altered. The process of extracting the CFA pattern from an image and examining it to find pattern irregularities brought about by copying and pasting of picture portions is known as copy-move forgery detection using CFA artifacts. It is feasible to identify portions that have been duplicated orshifted within the image by contrasting the CFA patterns of various regions of the image. Particularly when other conventional methods, including pixel-level analysis, fall short due to image processing techniques like smoothing and filtering, this method is quite effective at detecting copy-move forgery.

Algorithm:

1. Load the image and convert it to grayscale
2. Divide the image into non-overlapping blocks of the specified size.
3. For each block, create a vector of pixel values.
4. Sort the vectors according to their lexicographic order.
5. Group similar block vectors into clusters. Vectors are considered similar if their absolute difference is less than or equal to `opt.blsim`, and their mean and deviation are such that the deviation divided by the mean is greater than or equal to `opt.blcoldev`.
6. Clusters that are close to each other (as determined by the Hausdorff distance) are merged.
   Hausdorff Distance = H(A, B) = max(max(d(a, b)), max(d(b, a))) (1)where,
   "d(a, b)" is the distance between point "a" in set A and point "b" in set B The sets A and B would be the vectors of pixel values for two blocks being compared
7. Clusters that are smaller than a certain size (`opt.minptssize`) are merged with the closest larger cluster.
8. If a cluster contains more than one block, it is considered a candidate for copy-move forgery.
9. If no clusters are found, the image is considered authentic.
10. If clusters are found, further analysis can be conducted to identify the forged region(s).
11. The average color of each cluster is computed, and each block within the cluster is set to this color.
12. The block vectors are converted back to images.
13. Output the result of the analysis, whether the image is authentic or contains copy-move forgery, and the location ofthe forged region(s).

`opt` refers to a set of parameters that can be adjusted based on the specific use case and requirements.

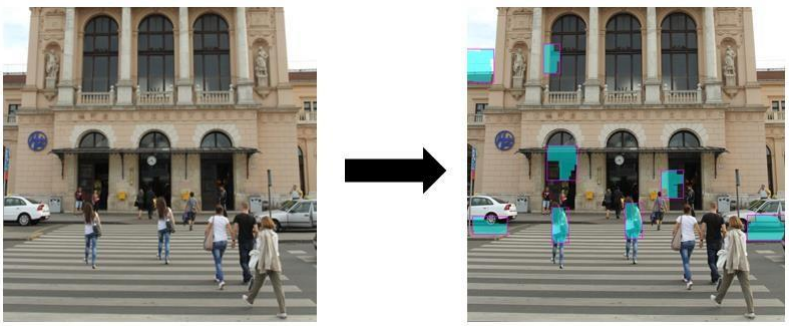

Figure 2: CFA Artifact Detection

3.2. Splicing Forgery

Splicing is a type of digital image forgery where different components from multiple images are blended to create a new image. This can be done by physically pasting pieces of printed images together, scanning or photographing the finished output, or physically cutting and pasting images using image editing software. Splicing can be done for a numberof reasons, including fabricating images for propaganda or personal advantage. Splicing might be challenging to spot withthe unaided eye, but it can be found using a variety of digital forensic techniques.

One of the most popular techniques for splicing detection is based on the idea that, depending on the camera or scanningdevice used to acquire them, various areas of an image may have varying amounts of noise or grain. Algorithms that compare the noise patterns of various areas of the image to see if they match can be used to analyze this. Inconsistencies in lighting and perspective, metadata analysis, and a careful examination of the image for evidence of cloning or other editing techniques are other ways to spot splicing. Splicing, as mentioned earlier, is a form of digital image fraud that entails fusing bits and pieces from many images to produce a new one. It can be used for a number of things and is sometimes challenging to see with the naked eye. To spot splicing and verify whether a picture has been altered, there area few digital forensic techniques that can be used.

For the purpose of detecting splicing forgeries, Error Level Analysis (ELA) in combination with Neural Network (CNN)method have been proposed.

3.2.1. Error Level Analysis

The Error Level Analysis (ELA) method examines variations in the compression level of various portions of an image to identify digital image forgeries. The fundamental tenet of ELA is that distinct digitally altered portions of an image may have varying levels of compression, which can be identified by examining the pixel values in the image.

The original image is first compressed using a certain compression method, such JPEG, before being subjected toELA. As a result, the image has a "baseline" level of compression. Using image editing software, the image is then digitallyaltered, and the edited version is compressed using the same compression process. ELA can be used to visualize the variation in compression level between the original and altered copies of the image.

An ELA image will display various colors in portions of the image that have been compressed more or less than the baseline level. The ELA image shows sections of the image that have been altered or processed as bright white or yellow regions because they often have a higher compression level than the surrounding areas.

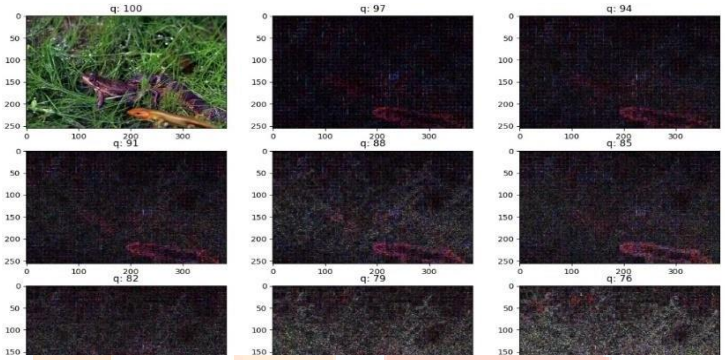

Figure 3: ELA Compression Levels of an Image

ELA can be helpful for identifying a number of digital picture modifications, such as splicing forgery. Other formsof image alteration, like resizing, rotation, and blurring, can also be discovered using this method. A drawback of ELA is that if the source image was already highly compressed, it may result in false positives. ELA can also be less successful atspotting specific kinds of image modification, like those that entail altering an image's color or brightness.

Error Level Analysis, which examines changes in compression levels between various portions of a picture, is a valuable method for spotting digital image fraud. Despite its drawbacks, it can be a useful tool for detecting specific kindsof image modification and can be used with other forensic methods for results that are more precise.

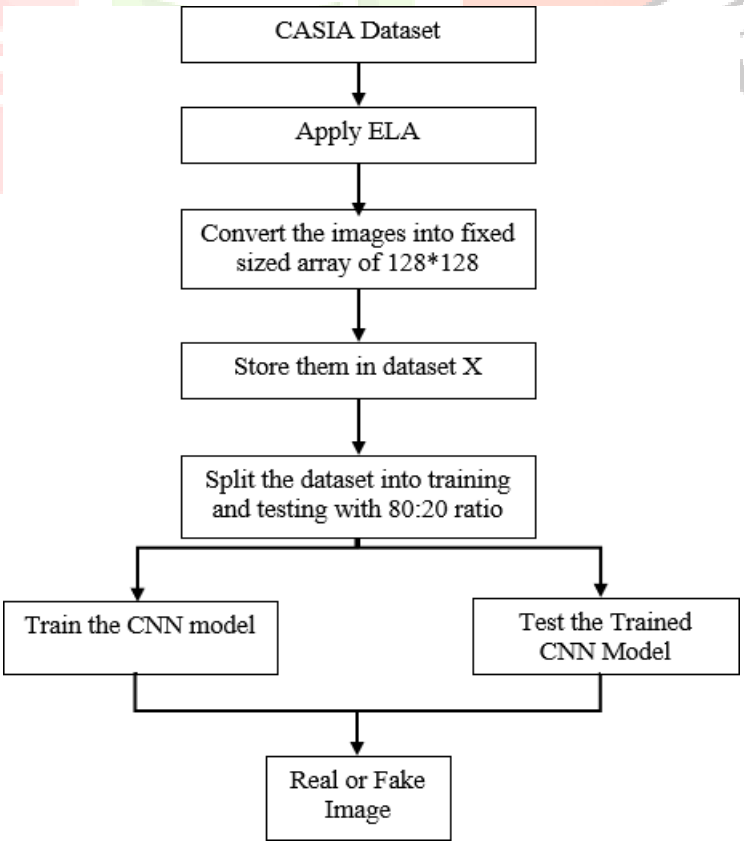

Figure 4: Block Diagram (Splicing Detection using ELA)

Here is a method to identify image splicing on the CASIA dataset using error level analysis (ELA) and convolutional neural network (CNN):

1. Load the CASIA dataset after importing the required libraries.
2. Preprocess the dataset by scaling the images to a predetermined size and making them grayscale.
3. Generate an ELA image for each image in the dataset. The following steps can be used to accomplish this:
    a. Make a high-quality copy of the original image.
    b. Resave the image with a lower quality to add artifacts from compression.
    c. Determine how much the original and compressed images differ.
    d. Adjust the final image's normalisation to a 0-255 range.
4. Split the training and testing sets with 80:20 ratio from the dataset.
5. Use a binary classification technique to train a CNN on the ELA images in the training set, determining whether ornot each image has been spliced.
6. Test the trained CNN on the testing set's ELA images to determine the accuracy with which it detects spliced images.
7. If the CNN's accuracy exceeds a predetermined threshold, proceed to the next stage. If not, change the CNN's hyperparameters and retrain the model until the desired accuracy is attained.
8. Carry out additional analysis to identify the spliced region(s) for each testing set image that the CNN identified asbeing spliced. Techniques like edge detection or texture analysis can be used for this.
9. Output the analysis results, indicating whether each image is real or spliced, as well as the location of any spliced region(s).

ELA of Real Image ELA of Fake Image

Figure 5: ELA Image Conversion

The CASIA dataset is described in the following ways:

1. CASIA is a dataset of digital images that was developed for the purpose of digital forensics research.
2. It includes over 10,000 digital images, including both authentic and tampered images.
3. Different devices, such as digital cameras, smartphones, etc. were used to gather the images for the dataset.
4. A number of picture types, including JPEG, BMP, and PNG, are included in the dataset.
5. A number of techniques, including copy-paste, splicing, and retouching, were used to manipulate the images.
6. The dataset also contains ground-truth data that identifies which images have been altered and the method usedto alter them.
7. CASIA is frequently used as a benchmark dataset for studies in the fields of digital image forensics and relatedones.
8. It has been extensively used in research projects and has helped with the creation of new algorithms and methodsfor identifying picture manipulation and associated problems.
9. The dataset is freely downloadable from multiple web sources and is available for research purposes.

3.3. Double Compression Detection

Double compression includes determining, using lossy compression techniques, if a picture has been saved or compressed more than once. This can be achieved by looking at the compression artifacts and the image's information.

Inconsistencies in the image's information, such as variations in the file format, compression methodology, or compression ratio, are a frequent way to spot double compression. An image may have been double compressed, for instance, if it appears to have been saved as a JPEG file twice but the quality or compression ratios are different.

Analyzing the visual distortions or artifacts caused by the compression process, sometimes known as the image's compression artifacts, is another strategy. Double compression can make these artifacts more obvious or pronounced, which may give the impression that the image is artificial or manufactured. These artefacts can be recognized and measured by forensic professionals using a variety of image analysis techniques, such as Fourier analysis or wavelet analysis.

Overall, applying double compression to identify image forgeries is a crucial tool in the struggle against digital manipulation and deception. Forensic experts can establish whether a picture has been altered or changed by identifying and examining the compression artefacts and metadata of the image, and they can also produce evidence that can be utilizedin legal processes or investigations.

Double compression detection algorithm using Discrete Cosine Transform (DCT) and Fourier Transform:

1. The first stage is to define the algorithm's parameters, such as the threshold value, the DCT quantization environments,and the DCT block size.

2. The OpenCV library is used to read the input image, and the image's dimensions are obtained.
3. The dimensions of the image are adjusted to ensure that they are divisible by 8 as DCT is performed on 8x8 blocks.
4. The image's Y channel, which holds the most data and is frequently utilized in image compression, is extracted in theYCrCb color space.
5. To extract the frequency coefficients, the Y channel is divided into 8x8 blocks, and DCT is applied to each block.
6. The mean value of each block is subtracted to normalize the acquired DCT coefficients.
7. A histogram is then used to display each block's 64 DCT coefficients.
8. The spectrum that results from applying the Fourier Transform to the histogram is moved so that the zero frequencyis located in the middle.
9. The indices of the peaks are calculated, and the slope of the spectrum is determined.
10. To assess whether the image has been doubly compressed or not, the number of peaks above the threshold value istallied and compared to a threshold count.
11. If the number of peaks exceeds the threshold count, the image is categorized as double compressed and the functionreturns True; otherwise, it returns False.

4. Result and Discussion

The performance of the classification models for a specific collection of test data is evaluated using a matrix called the confusion matrix. Important predictive metrics like recall, specificity, accuracy, and precision are visualized using it. Because they provide clear comparisons of values like True Positives, False Positives, True Negatives, and False Negatives, confusion matrices are helpful.

1. Accuracy - Accuracy is the most intuitive performance measure, and it is simply a ratio of correctly predicted observations to the total observations.

$$\text{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN} \quad (2)$$

2. Precision - Precision is the ratio of correctly predicted positive observations to the total predicted positiveobservations.

$$\text{Precision} = \frac{TP}{TP+FP} \quad (3)$$

3. Recall - Recall is the ratio of correctly predicted positive observations to all observations in the actual class.

$$\text{Recall} = \frac{TP}{TP+FN} \quad (4)$$

4. F1-score - f1-score is the weighted average of Precision and Recall. Therefore, this score takes both false positivesand false negatives into account.

Table 1: Performance Metrics

Forgery	Methodologies	Accuracy	Precision	Recall	F1-Score
Copy-Move	**DBSCAN Algorithm**	94.3	92.77	96.01	94.36
	CFA Artifact	91.08	89.02	93.59	91.25
Splicing	**ELA + CNN**	93.04	94.84	91.25	93.01
Double Compression	**DCT + Fourier Transform**	95.33	93.3	97.5	95.35

According to the experimental results, the methodologies for copy-move detection—CFA Artifacts and the DBSCAN clustering algorithm—perform more accurately and robustly against image modifications than current methods. Even in the presence of compression artifacts, the suggested method for splicing detection, ELA with the use of CNN, achieves good accuracy in detecting image manipulation. These results demonstrate the effectiveness of the suggested techniques work at detecting different types of image tampering, which is helpful for forensic applications like detecting image forgeries.

The system is capable of extracting and detecting Double JPEG Compression Detection, Copy-Move Detection usingthe DBSCAN clustering technique, CFA Artefact Detection, Splicing Detection using Error Level Analysis (ELA) in addition with CNN from input images. The system offers the user the option to select any approach and generate results using pop-up windows, output windows on the user interface, or image output.

5. Conclusion

The review of prior research work conducted on forensic verification to detect real and fake images is discussed in thispaper. Four distinct image forgery detection principles are mentioned in the proposed system, which can primarily detect Copy-Move and Splicing Forgery. The system has the ability to accept input images and produce results that are appropriate for overcoming the problem of forged images. The overall discussion leads to the conclusion that using the suggested system can more accurately

identify various counterfeiting. The study has successfully distinguished images based on their authenticity through forensic verification. Therefore, it can be concluded that the system is capable of detecting several types of forgeries and can significantly enhance the accuracy level of detecting a fake image.

References:

[1] Chen J., Kang X., Liu Y., "Median filtering forensics based on convolutional neural networks," IEEE Signal Processing Letters, vol. 22, no. 11, 2015.

[2] Tang H., Ni R., Zhao Y., Li X., "Median filtering detection of small-size image based on CNN," Journal Visual Communication and Image Represent, 2018. Crossref, https://doi.org/10.1016/j.jvcir.2018.01.011

[3] Lin M., Chen Q., Yan S., "Network in network," arXiv 2013, arXiv:1312.4400. Crossref,

[4] Youseph SN, Cherian RR, "Pixel and Edge Based Illuminant Color Estimation for Image Forgery Detection," Procedia Computer Science, 2015.Crossref, https://doi.org/10.1016/j.procs.2015.02.099

[5] Hashmi MF, Anand V, Keskar AG, "Copy-move Image Forgery Detection Using an Efficient and Robust Method Combining Un-Decimated Wavelet Transform and Scale Invariant Feature Transform," AASRI Procedia, 2014. Crossref, https://doi.org/10.1016/j.aasri.2014.09.015

[6] Zhao J, Guo J., "Passive forensics for copy-move image forgery using a method based on DCT and SVD," Forensic Science International, 2013. Crossref, https://doi.org/10.1016/j.forsciint.2013.09.013

[7] A. Dixit and R. K. Gupta, "Copy-Move Image Forgery Detection a Review International Journal of Image," Graphicsand Signal Processing 8(6):29-40 DOI:10.5815/ijigsp.2016.06.04

[8] Gallagher A and Chen T, 2008, "Image authentication by detecting traces of demosaicing," IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops 1-8. DOI: 10.1109/CVPRW.2008.4562984

[9] Popescu A and Farid H, 2005, "Exposing Digital Forgeries in Color Filter Array Interpolated Images," IEEE Transactions on Signal Processing, 53(10) 3948-3959.

[10] Malviya AV, Ladhake SA., "Pixel Based Image Forensic Technique for Copy-move Forgery Detection Using Auto Color Correlogram," Procedia Computer Science, 2016.

[11] Oommen RS, Jayamohan M, Sruthy S., "Using Fractal Dimension and Singular Values for Image Forgery Detection and Localization," Procedia Technology. 2016.

[12] Jeronymo DC, Borges YCC, Coelho L dos S, "Image forgery detection by semi-automatic wavelet soft-Thresholdingwith error level analysis," Expert Systems with Applications, 2017.

[13] O.M. Al. Qershi and B. E. Khoo, "Comparison of Matching Methods for Copy-Move Image Forgery Detection," Proc. Springer 9th International Conference on Robotic, Vision, Signal Processing and Power Applications, pp. 209â€“218, 2017.

[14] K. G. Birajdar and V. H. Mankar, "Digital image forgery detection using passive techniques: A survey," Digital Investigation, vol. 10.

[15] O.M. Al. Qershi and B. E. Khoo, "Passive detection of copy-move forgery in digital images: State-of-the art," Forensic Science International, vol. 231, pp. 284â€ “295, 2013.

[16] D. Chauhan, D. Kasat, S. Jain and V. Thakare, "Survey on Keypoint Based Copy-move Forgery Detection Methods on Image," Procedia Computer Science, vol. 85, pp. 206â€ “212, 2016.

[17] Popescu A C, Farid H., "Statistical tools for digital forensics," International Workshop on Information Hiding, (Springer, Berlin Heidelberg 2004), pp. 128-47.

[18] J LukÃ¡Å¡, J Fridrich, "Estimation of primary quantization matrix in double compressed JPEG images," in Proc. Digital Forensic Research Workshop, 2003, pp. 5â€ “8.

[19] Z Lin, J He, X Tang, CK Tang, "Fast, automatic and fine-grained tampered JPEG image detection via DCT coefficientanalysis," Pattern Recognition 42(11), 2492â€ “2501 (2009).

[20] R. Thakur, R. Rohilla, "Copy-Move forgery detection using residuals and convolutional neural network framework: a novel approach," 2019 international conference on robotics and automation in industry (ICRAI) (2019).

[21] Y. Abdalla 1, M.T. Iqbal, M. Shehata, "Convolutional Neural Network for copy-move forgery detection," conference:computer vision and pattern recognition Doi: 10.11.19/ICPR (Nov 2019).

[22] Y. Abdalla 1, M.T. Iqbal, M. Shehata, "Copy-Move forgery detection and localization using a generative adversarialnetwork and convolutional neural network," article - department of computer science, math, physics, and statistics, university of British

Columbia, Kelowna, BC v6t 1z4, Canada (2019).

[23] Dua S., Singh J., Parthasarathy H., "Image forgery detection based on statistical features of block DCT coefficients," Procedia Computer Science, 2020, 171, 369â€ “378.

[24] Ehret T., "Robust copy-move forgery detection by false alarms control," arXiv 2019, arXiv:1906.00649.

[25] Luo, W.; Huang, J.; Qiu, G. "JPEG Error Analysis and Its Applications to Digital Image Forensics," IEEE Trans. Inf.Forensics Secur, 2010, 5, 480â€ “491.