JSRT JOURNAL

PAGES: 1-11
09/03/24

JOURNAL OF SCIENTIFIC RESEARCH AND TECHNOLOGY VOLUME-2 ISSUE-9 SEPTEMBER

High Resolution Image Forgery Identification And Detection Using Machine Learning

Pallavi Kulakarni[1], Bharati S. Pochal[2]

[1]Department of Computer Science and Engineering (MCA) VTU CPGS Kalaburagi-585105, Karnataka, India. pallavikulakarni4@gmail.com https://orcid.org/0009-0007-5581-1010

[2]Assistant Professor, Department of Computer Science and Engineering (MCA), Visvesvaraya Technological University Kalaburagi, Karnataka, India. bharatipochal@gmail.com

ORCID ID: https://orcid.org/0000-0001-9562-8420

ABSTRACT

Now a days we are blindly trusting the authenticity of digital imagery so image forgery is expanding with High frequency. By manipulating the technology to conceal some important or critical information about the image, digital image fraud might be done. The detection of forgery in the image is required to maintain the integrity and authenticity of the image. Utilizing digital images has become simpler with the aid of picture editing software as a result of acclimating to modern life and technological advancements in photographic equipment. Consequently, it is essential to spot these image forging techniques in the photos. On the basis of object removal, object addition, and unexpected size adjustments in the image, the fake of an image can be detected.

Keywords: Discrete Wavelet Transform(DWT), Discrete Cosine Transform(DCT), CMFD Algorithm

1. INTRODUCTION

The growing concern over altered or faked visual content is being addressed by an emerging field called forgery detection for high-resolution digital photographs. picture manipulation and alteration have been easier because to developments in digital imaging technology, which has increased picture forging and transmission of incorrect or misleading information. High- resolution digital images' integrity will be recognized and verified through the use of counterfeit detection tools. These technologies evaluate the picture data using sophisticated algorithms and computational tools to look for indications of alteration or tampering. It enables consumers to base their judgments on real visual information, reduces the propagation of false information, and increases the credibility of digital material. The arms race between forgery detection and forgery tactics, nevertheless, is still going strong, and both fields have made gains. [1] Esteban Alejandro, Armas Vega, and others. Method for digital picture authentication based on DWT, DCT, and local binary patterns. Digital images of written papers, scans of important certificates, circuit schematics, design concepts, and signed checks are all included in this multimedia material. Designing effective solutions to the issue is crucial since there is a pressing need to protect the authenticity and integrity of digital photographs from different manipulation efforts.[2] Vialatte, Jean-Charles, Vincent Gripon, and Gilles Coppin. Learning local receptive fields and their weight sharing scheme on graphs. 2017 GlobalSIP, an IEEE conference on signal and information processing. IEEE, 2017, The NSF-funded and Signal Processing Society-supported Signal Processing Information Base (SPIB) initiative is a first attempt to make data, articles, software, and material broadly accessible in a timely, efficient manner. It would appear simple to disseminate information over computer networks and search through information using software. However, contemporary publications now include tables, graphics, graphs, and several types of data displays—images—in addition to text, which exacerbates the representation issue. [3] Musaed Alhussein. Using a local texture descriptor and an extreme learning machine, identify image manipulation. The 18th International UKSim-AMSS Conference on Computer Modeling and Simulation was held in 2016. The field of computer simulation modeling is becoming more and more popular in both government and business. Complex system design, development, and assessment can be aided by computer simulation modeling. Computer simulation modeling is used by designers, program managers, analysts, and engineers to comprehend and assess "what if" case situations. It may simulate a real or hypothetical system using computer software and is helpful when alterations to the real system are challenging to make, expensive, or impractical. The majority of us are aware with certain applications of computer simulation modeling, such as weather forecasting, pilot training simulators, and vehicle crash modeling.

2. RELATED WORK

[4] Ojeniyi, Joseph A.et al. 10(4)(2018), 22. this survey basically about detecting copy-move attack using Hybridized approach. International Journal of Image, Graphics, and Signal Processing The availability of several sophisticated and potent picture altering programs has increased as the world has significantly undergone substantial technology improvement over the years. There has been an increase in the authenticity of digital photos as a result of how simple it is to obtain these image altering tools over the internet and how easily newcomers to the field may now modify images without leaving any evident evidence. [5] Giuseppe Mazzola, Alessandro Bruno, and Edoardo Ardizzone. Detecting fake copies of moves. 10(10)(2015), 2084–2094. The majority of detection techniques either employ point- based approaches, where pertinent keypoints are extracted and matched to one another to locate comparable regions, or block-matching techniques, which divide the picture into overlapping blocks and then extract and compare characteristics to find similar ones. We describe a highly innovative hybrid technique in this research that compares triangles rather than blocks or single points.[6] by Juliana C. Gomes and others. An electrical impedance tomography image is recreated utilizing back some powerful learning tools Biomedical Engineering Research, 2020, 1–12. The main advantages of EIT are its portability, cost. [7] Evaluation of feature-based approaches for automatic network orientation. F. I. Apollonio et al. The 45th issue of the International Archives of Photogrammetry, Remote Sensing, and Spatial Information Sciences was published in 2014. The study, we analyze a number of feature-based methods that automatically extract the tie points needed for calibration and orientation operation in order to better understand their capabilities for 3D reconstruction tasks.[8] Bappy and Jawadul focused on locating and detecting picture frauds.Here, a pre-filtering procedure called copy-move detection is utilized. The findings demonstrate that when the copy- move method is coupled with different resampling detection techniques, the detection rate consistently rises by 8% to 10%. [9] In his study, Chauhan Devanshi developed methods for detecting fake images using keypoints.Additionally, they focused on methods already in use for identifying fake pictures in photographs as well as for detecting copy-move films. Here, GLSM clustering and optical method were employed.[10] Marra, Francesco,Diego Gragnaniello, and Luisa Verdoliva investigated how deep learning for camera model recognition is vulnerable to adversarial assaults. To identify false photos, this system employs deep learning algorithms.

2.1 HARDWARE AND SOFTWARE REQUIREMENTS

2.1.1 Hardware Requirement

Table 1 : Hardware Requirement

Processor	Pentium coreI5 and higher
RAM	4GB or more
Hard Disk	500GB or more
Monitor	15 inch color monitor
Mouse	Optical Mouse
Keyboard	102/104 keys

2.1.2 Software Requirement

Table 2 : Software Requirement

Operating System	Windows 10 or above
Frontend	Python
Backend	SQlite3

3. PROPOSED SYSTEM

3.1 Workflow Model

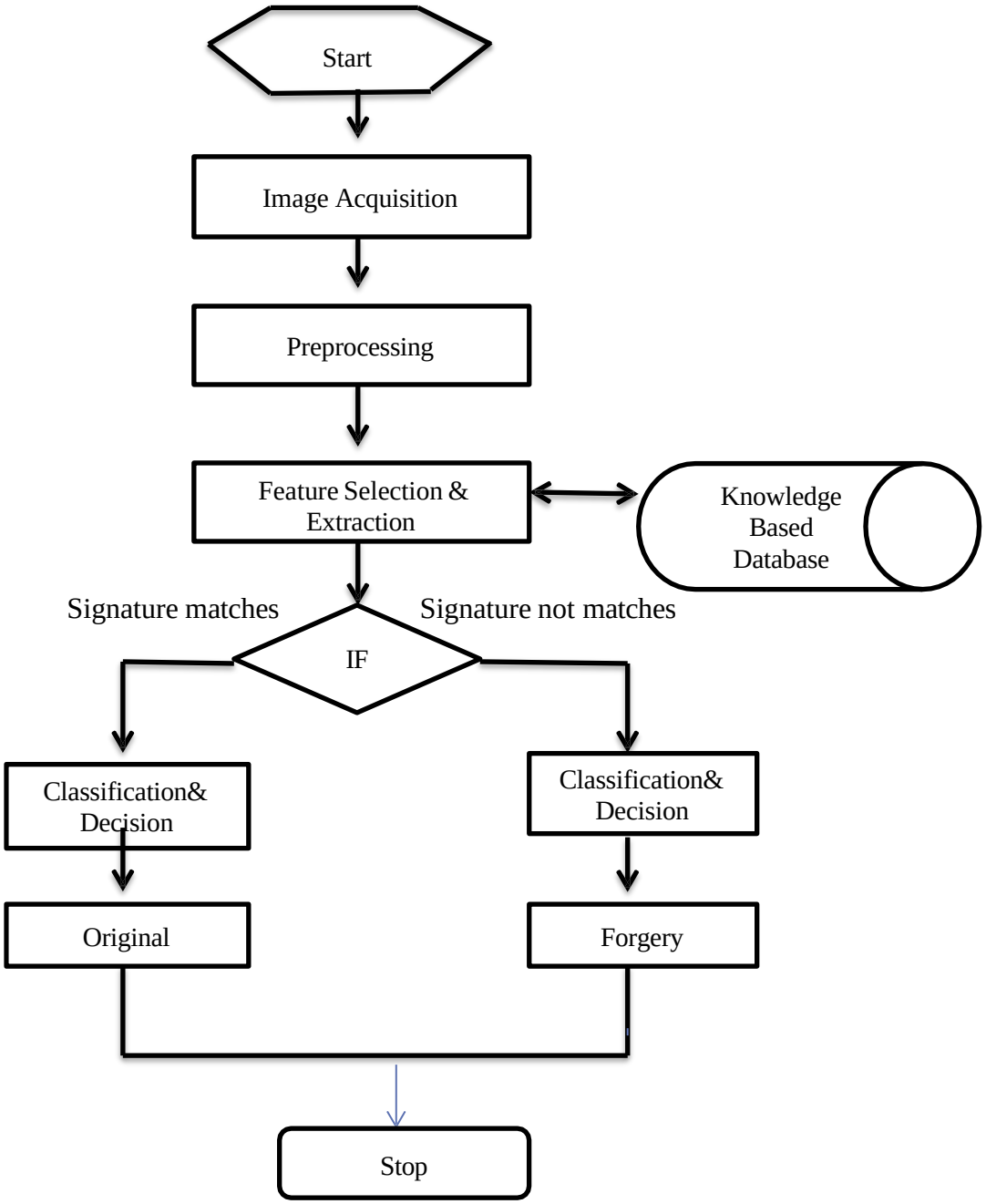

Figure 1. Workflow Diagram

3.2 Methodology

3.2.1 System Perspective

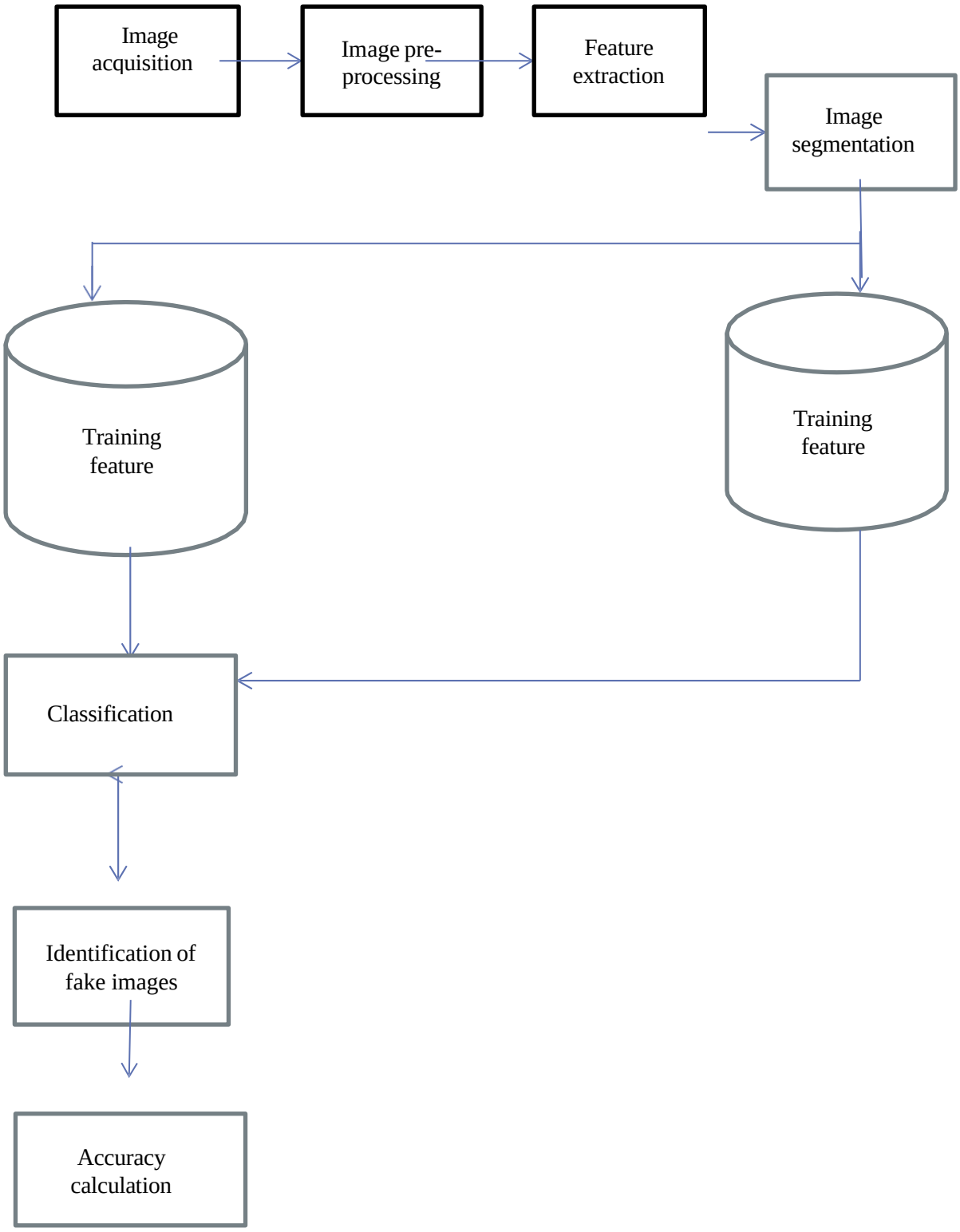

Figure 2. System Perspective Diagram

A System Perspective diagram for image forgery detection would typically consist of following components:

1. **Image input:** This displays the input photographs that must be evaluated for possible forgery.

2. **preprocessing**: module: Images may be preprocessed before analysis, such as scaling, normalization, noise reduction, and so on, to prepare them for subsequent processing.

3. **Feature extraction:** This module extracts relevent feature from the preprocessed images.

4. **Segmentation:** In ,segementation image is divided into some parts. After the image is segmen.ted, feature matching is performed concerning the segmentation image.

5. **Training Data:** This is the dataset that was used to train the forgery detection model.It would include both actual and fake images from which to learn.

Later, it categorizes and selects.The final output indicates the forgery detection process's outcome, showing whether the input image is genuine or tampered with.

3.2.2 Proposed Methodology

Algorithm 1. Proposed CMFD Scheme.

Variable Declaration: I: test image

Di : extracted descriptors, i = A − KAZE, SURF

Pj : positions of detected points, j = A − KAZE, SURF

Pk : positions of matched points with g2NN test, k = A1 , A2, S1 , S2, 1, 2 T: estimated affine transformation matrix

Pinliners: matched points with RANSAC Mmap: correlation coefficient map

Mmask: final binary image with demarcated duplicated regions Proposed CMFD Scheme:

1. Read Image I←tested image Mmask←image whose pixel values are 0

2. Feature Extraction [DA−KAZE,PA−KAZE] ← A − KAZE(I) [DSURF,PSURF] ← SURF(I)

3. Feature Matching

[PA1 ,PA2] ← g2NN(DA−KAZE,PA−KAZE) [PS1 ,PS2] ← g2NN(DSURF,PSURF)

[P1 ,P2] ← pos_combination(PA1 ,PA2 ,PS1 ,PS2)

4. Eliminating False Matches with

RANSAC [T,Pinliers] ← RANSAC(P1 ,P2)

5. Calculate Correlation Coefficient

Map Mmap ← corr_map(I, T)

6.Filtering and Mathematical Morphology Operation Mmask ← post_processing(Mmap)

7.Judgment

if Mmask is black

I is an authentic image

else

I is a tampered image

end if

Evaluation Metric

i. Precision = $\frac{TP}{TP+FP}$

ii. Recall = $\frac{TP}{PN+TP}$

iii. F1-measure = $\frac{2*Precision*Recall}{Precision+Recall}$

Here,

TP = True Positive (Correctly predicted as positive).

TN = True Negative (Correctly predicted as negative).

FP = False Positive (Incorrectly predicted as positive). FN = False Negative (Incorrectly predicted as negative).

4. RESULTS AND DISCUSSION

SCREEN SHOTS

Figure 3. Input Image

The given figure 6 is input image. In the context of forgery detection, an input picture is often the digital image that must be evaluated to identify whether it contains any counterfeit or modified parts.

Figure 4.Grayscale

Figure 5.Threshod image

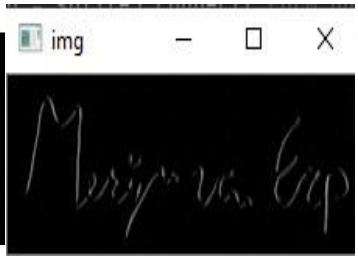

Figure 6. Feature extracted

After receiving the input picture, it changes it to grayscale image since grayscale images simplify processing and minimize the amount of data required to describe the image. Image thresholding is a method of converting a grayscale image to a binary image.

4.1 TEST CASES

Test Number	Form	Description	Expected Result	Actual Result
1	Input	Provide a high resolution digital image without forgery	The system should classify image as real	Pass(image correctly classified As real)
2	Input	Provide a high resolution digital image with a known forgery	The system Should classify Image as fake	Pass(Forgery correctly detected and classified)
3	Accuracy	Test the System with a diverse dataset of high-resolution digital images	The system Should achieve An accuracy of Atleast 90%	Pass(Accuracy of 92%)

4.1.2 TEST RESULTS

Test Case Id: 1

Figure 7. Input Image

Result

The given Figure 7 image is real image. so the message “Real” is displayed .

Test Case Id: 2

Figure 8. input image

Result

The given figure 8 image is forged image so the error message “Fake” is displayed

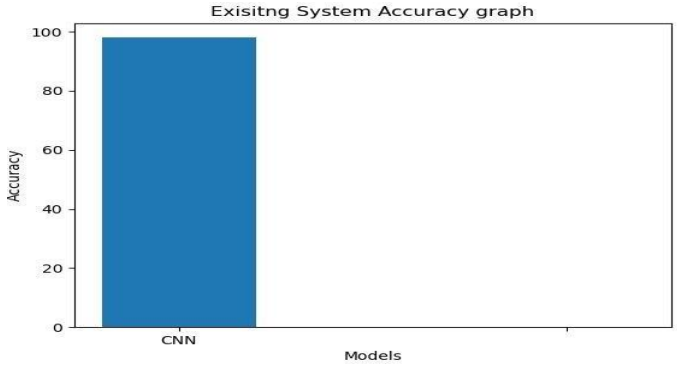

Figure 9. Accuracy Graph for Existing System

Figure 9 shows Existing System Accuracy Graph which has accuracy of about 90%.

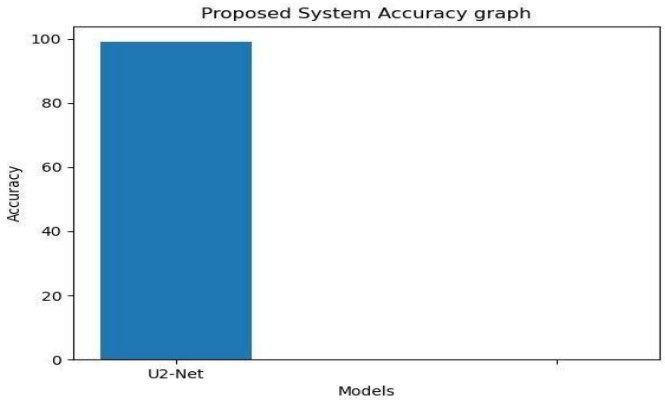

Figure 10. Accuracy Graph for proposed system

Figure 10 shows proposed system accuracy graph ,which has an accuracy of about 92%.

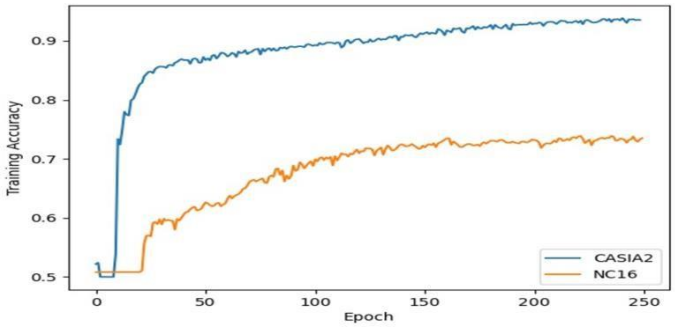

Figure 11.Training Accuracy Graph

Figure 11 shows Training Accuracy Graph.

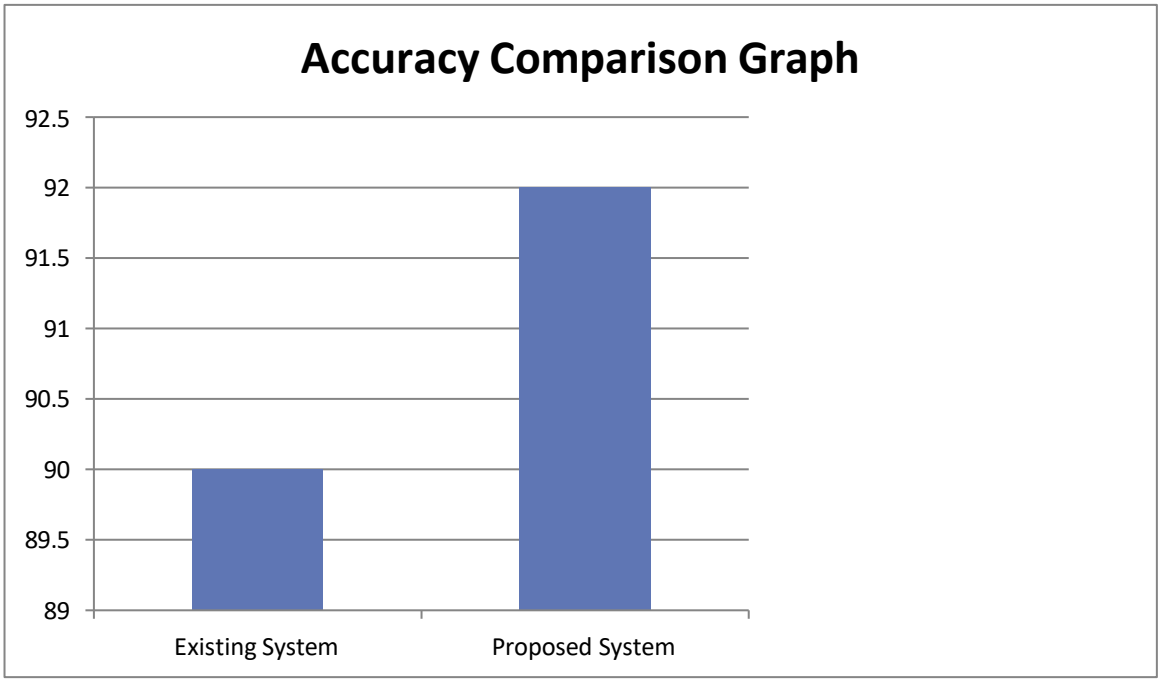

Figure 12.Accuracy Comparison Graph

CONCLUSION

In conclusion, forgery detection for high-resolution digital images is a critical area of research and development in today's digital age. The ability to accurately identify and authenticate manipulated or tampered visual content is crucial for maintaining the integrity, credibility, and trustworthiness of digital media. By addressing challenges such as subtle manipulations, computational complexity, scalability, and evolving forgery techniques, forgery detection can benefit media organizations, law enforcement, forensic experts, content creators, researchers, and the general public. It plays a vital role in combating misinformation, protecting digital assets, ensuring the authenticity of evidence, and promoting media literacy.Continued collaboration among researchers, industry experts, and practitioners, along with the establishment of standardized evaluation metrics and benchmark datasets, will drive further advancements in forgery detection. These advancements will contribute to a more secure and trustworthy digital landscape, where high-resolution digital images can be verified and authenticated with confidence.The future enhancements of forgery detection for high-resolution digital images hold several possibilities for advancing the field and improving the accuracy and effectiveness of forgery detection techniques. Further advancements in deep learning algorithms and artificial intelligence can improve forgery detection by training models on larger and more diverse datasets. This can enhance the ability to detect subtle manipulations and adapt to evolving forgery techniques. Developing forgery detection techniques that are specifically designed to detect and counter adversarial attacks can provide more robust and resilient detection capabilities. Developing techniques that can explain the decision-making process of forgery detection models can provide transparency and build user trust in the detection results. Future enhancements should focus on developing real-time and scalable forgery detection solutions to handle large volumes of high-resolution digital images efficiently. This is particularly important in domains like social media platforms, where quick detection and prevention of the spread of manipulated images are crucial.

REFERENCES

[1] Armas Vega, Esteban Alejandro, et al. Digital images authentication technique based on DWT, DCT and local binary patterns. Sensors. 18(10)(2018), 3372.

[2] Vialatte, Jean-Charles, Vincent Gripon, and Gilles Coppin. Learning local receptive fields and their weight sharing scheme on graphs. 2017 IEEE Global Conference on Signal and Information Processing (GlobalSIP). IEEE, 2017.

[3] Alhussein, Musaed. Image tampering detection based on local texture descriptor and extreme learning machine. 2016 UKSim-AMSS 18th International Conference on Computer Modelling and Simulation (UKSim). IEEE, 2016.

[4] Ojeniyi, Joseph A., et al. Hybridized Technique for CopyMove Forgery Detection. International Journal of Image, Graphics and Signal Processing. 10(4)(2018), 22.

[5] Ardizzone, Edoardo, Alessandro Bruno, and Giuseppe Mazzola. Copy–move forgery detection by matching triangles of keypoints.10(10)(2015), 2084-2094.

[6] Gomes, Juliana C., et al. Electrical impedance tomography image reconstruction based on back projection and extreme learning machines. Research on Biomedical Engineering, (2020), 1- 12.

[7] Apollonio, F. I., et al. Evaluation of feature-based methods for automated network orientation. International Archives of the Photogrammetry, Remote Sensing & Spatial Information Sciences. 45(2014).

[8] Bappy, Jawadul, et al. Detection and Localization of Image Forgeries Using Resampling Features and Deep Learning. Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops. 2017.

[9] Chauhan, Devanshi, et al. Survey on keypoint based copymove forgery detection methods on image. Procedia Computer Science. 85(2016), 206-212.

[10] Marra, Francesco, Diego Gragnaniello, and Luisa Verdoliva. On the vulnerability of deep learning to adversarial attacks for camera model identification. Signal Processing: Image Communication. 65(2018), 240-248.

Authors' Profiles

Ms. Bharati S. Pochal Assistant Professor, Department of Computer Science & Engineering, VTU CPGS, Kalaburagi- 585105, Karnataka, India.
Major interests: Wireless sensor networks, Internet of things, Cloud Computing, Machine Learning, Image Processing.

Pallavi Kulakarni Department of Computer Science & Engineering (MCA), VTU CPGS, Kalaburagi-585105, Karnataka, India.