IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 12, Issue 4, April 2023

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2023 ||

| DOI:10.15680/IJIRSET.2023.1204160 |

Medical Image Forgery Detection Using Smart Healthcare

Mrs. Jyoti Bagate[1], Vinaya Nair[2], Akshay Jain[3], Girish Gopalakrishnan[4], Yukta Talagana[5]

Assistant Professor, Department of EXTC, University of Mumbai, VESIT, Mumbai, India[1]

Student, Department of EXTC, University of Mumbai, VESIT, Mumbai, India [2]

Student, Department of EXTC, University of Mumbai, VESIT, Mumbai, India [3]

Student, Department of EXTC, University of Mumbai, VESIT, Mumbai, India [4]

Student, Department of EXTC, University of Mumbai, VESIT, Mumbai, India [5]

ABSTRACT: Nowadays, in the world of advanced digital computers, tampering, and implication of digital images can be easily performed with a number of accessible advanced image processing software like Adobe Photo shop, Corel Draw, etc. Therefore, it becomes very challenging for end users to distinguish whether the image is novel or forged. In the fields such as forensics, medical imaging, e-commerce, and industrial photography, the legitimacy and integrity of digital images are crucial. This motivates the need for detection tools that are transparent to tampering and can reveal whether an image has been counterfeit. Recently, many new methods are presented with improved performances of detection. However, there is still a place to improve this performance further. Some of the proposed state-of-the-art image tamper detection techniques have been selected for the proposal. The methodology to detect forgery is discussed thoroughly as well as the steps taken to implement the above-mentioned techniques are mentioned in detail.

KEYWORDS: Tampering, intrusion, extrusion, watermark, signatures, segmentation, template matching

I. INTRODUCTION

Need for Forgery Detection in Healthcare system:
With the increased importance of digital images in various applications, where authenticity is of prime importance, it is necessary to verify the integrity and authenticity of digital images. But the usage of digital images has become more frequent throughout society; the creation of digitally forged images has increased. Because of the easy availability of image editing software such as Photoshop, making forgeries in digital images has become an easy task without leaving obvious evidence that cannot be recognized by human eyes. So, image authentication came forth as an important problem. In the healthcare domain, image forgery can be serious. If a mammogram is hacked and the intruder uses the copy-move forgery, to enlarge the area of cancer, the diagnosis will be wrong and the patient will be in life-threatening trouble. If there is an image forgery detection, system in a healthcare framework, it can detect the forgery before starting the diagnostic process.

Different Method Of forgery detection:
Digital image authentication technique broadly has two types:

Intrusive method: Intrusive method is concerned with data hiding where some code is embedded into the image at the time of generation. Verifying this code authenticates the originality of the image. Active authentication methods are further classified into two types:
Digital Watermarking: Digital watermarks are embedded into the images at the time of image acquisition.
Digital Signatures: Digital signatures: Digital signatures are embedded giving secondary information, usually extracted from the image at the acquisition end into the image.

Non-intrusive (Extrusive): Extrusive method or passive authentication also called image forensic is the process of authenticating images with no requirement of prior information but it's done with just the image itself. Passive techniques are based on the assumption that even though tampering may not leave any visual trace but they are likely to alter the underline statistics. It is these inconsistencies that are used to detect tampering. The passive technique has the

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2023 ||

| DOI:10.15680/IJIRSET.2023.1204160 |

advantage that they do not require prior information about the image. They just need the tampered image that requires to be verified for authenticity. Images are usually manipulated in ways such as Image slicing and region duplication through copy- move forgery. In image slicing, regions from multiple images are used to create the forged images. However, in the copy-move forgery image, regions are copied and pasted onto the same image. To conceal or increase some important content in the pictured image. As copied regions are apparently identical with compatible components (colour, noise) it becomes challenging to differentiate the tampered region from the authentic region. Furthermore, a counter filter applies various post-processing operations such as blurring, edge smoothing, and noise to remove the visual traces of image forgery. Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), Principal Component Analysis (PCA), Singular Value Decomposition (SVD), and Scale Invariant Feature Transformation (SIFT) are the different techniques that help to detect forgery.

II. LITERATURE SURVEY

Medicalimage forgery detection using Smart healthcare.
Nameoftheauthor: GhoneimAhmed,Muhammad Ghulam,AminSyed Umar,andGuptaBrij
Yearofpublication:2019
Name of the journal: IEEE, vol. III
Abstract and methodology:

The methodology of this project was as follows: It used the latest technologies like edge computing,IoT, and cloud computing were used. A multi-resolution regression filter is applied to the noise map tofind an inter-relationship between a pixel and a neighboring pixel. The output is fed into an ELM(Extreme Learning Machines) and SVM (Support Vector Machines) classifier. The system was testedusingthreedifferentdatabases.Theresultobtainedfromthismethodologywasthatitachievedaccuracies over 98% for natural images and 84.3% for medical images. The system performs best whencombined the scores of two classifiers.
The drawbacks were that this system cannot detect intrusive methods because it needs extra bandwidthand causes delays in transmission.

DoubleJPEGCompressiondetectionbyexploringthecorrelationsinDCTDomain.
Nameoftheauthor: PengpungYoung
Yearofpublication:2019
Name of the journal: IEEE, vol. III
Abstract and methodology:
Themethodologyofthisprojectwasasfollows:Itworksontheproposedtechniqueontheprinciplethat properties like periodic zeros and the double peak is available if a JPEG image is changed. Theresult was that a detection method of double JPEG squashed image with DCT and SVM was developed.The drawbacks were that the modulation of high false positives to natural images resulted in no perfecthistogram.

Revealingimageforgerythroughimagemanipulationdetection.
Name of the author: Ms. Jayshree Charpre, and Ms. Antara Bhattacharya.
Yearofpublication:2019
Name of the journal: IEEE, vol. IV
Abstract and methodology:

The active approach includes intrusive methods like watermarking and digital signature. The majordrawback of the watermarking approach is that watermarks need to be embedded in the image beforedistribution. In the market, most cameras nowadays are not equipped with the function of embeddingwatermarks. Also, the use of these methods deteriorates image quality. To verify the image authenticityusing the passive approach, no information needs to be embedded in images for distribution. Thesemethods are also known as blind as the presence of the original image is not required to verify theauthenticity. So, these methods also have applications in the field of image forensics. Since the problemof image forensics is very broad, this paper focuses on forgery detection in digital images. This paperpresents efficient and reliable techniques for detecting global and applied contrast enhancement andcopy-pasteforgery in digital images.
The methodology of this project was as follows: In this system for detecting copy paste the algorithmused is DCTfor extracting features.For the detection of the global contrast, enhancement is done with the help of the calculation of

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2023 ||

| DOI:10.15680/IJIRSET.2023.1204160 |

thehistogramimage.Theresultswerethatthealgorithmcanefficientlydetectthelargeblockthatwentupto 64 X 64.
Thedrawbackswerethatthis system was not efficient for compressed images. On the other hand,somealgorithms likehistogram, andcontrast stretchinghave avery hightime complexity.

Pixel-basedimageforgerydetection.
Nameoftheauthor: Mohd.DilshadAnsari,S.P.GhreraandVipinTyagi
Yearofpublication:2018
Name of the journal: IEEE, vol.V
Abstract and methodology:

The methodology of this project was as follows: In this project, they used different forgery detectionAlgorithmslikecloning,resampling,andsplicingunderpixel-baseddetection.TheresultswerePixel-based image forgery detection that aimed to verify the authenticity of digital images without anyprior knowledge of the original image.
Thus, it only used image processing techniques. The drawbacks were that in this system pixel-basedalgorithms are unable to detect forgery effectively, they are having high time complexity, and the modelneedsto develop an efficient andaccurate image forgery detection algorithm.

Arotationallyinvarianttexturedescriptortodetectthecopy-moveforgeryinmedicalimages.
Nameoftheauthor: Mrs.SurbhiSharma,UmeshGhanekar.
Yearofpublication:2018
Name of the journal: IEEE, vol. IV
Abstract and methodology:
Copy- moveimageforgerydetection using localbinarypatternandneighborhood.
Name of the author: Al Sawadi and Muhammad G Hussain

Yearofpublication:2017
Name of the journal: IEEE, vol. III
Abstract and methodology:
The sixth paper that was studied was titled “Copy move image forgery detection using local binarypattern and neighborhood”. The authors were. The year of publication was 2013. The methodology ofthis project was as follows: The image is first converted into grayscale. The block pairs with minimumdistance are taken based on the calculation of histogram distance with blocks. The proposed method shows significant improvement in reducing the false positive rates over some recent related methods. The results were that an efficient detection method of copy-move image forgery is proposed. Theproposedmethodutilizesthreecolor components and LBP (Local Binary Patterns) to find texture patterns.

The methodology of this project was as follows: This project presents an efficient method to detectcopymoveforgerydetectioninmedicalimagesusingacentersymmetricallocalbinarypattern(CSLBP) which is able to detect the forgery size up to 12 X 12. The proposed CSLBP block-based methodisrobust against geometric distortion, Gaussian blurring, JPEG compression, and AdditiveWhite Gaussian Noise.
Thedrawbackswerethatthissystemperformedwellwith32X32regionsinthepresenceofAWGNbut still was not able to detect 16 X 16 tampered regions.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2023 ||

| DOI:10.15680/IJIRSET.2023.1204160 |

III. METHODOLOGY

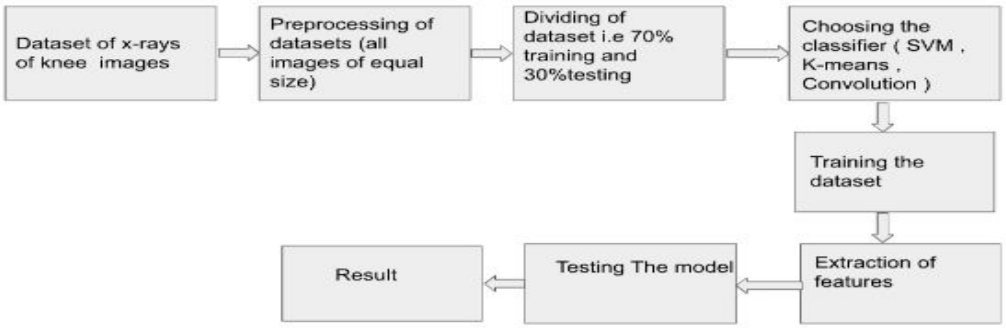

Fig 3.1 Block diagram of proposed project

The following steps denote the flow of our project:
1. The input will be JPEG images (Joint Photographic Experts Group).
2. We use JPEG images because compressed images will be preferable for pre-processing the image.
3. In preprocessing process, we will apply thresholding and brightness control operations to the image.
4. After preprocessing, we will do the segmentation process.
5. Image segmentation is a method of dividing a digital image into subgroups called image segments, reducing the complexity of the image and enabling further processing or analysis of each image segment.
6. We would also perform a histogram process in the image if it is needed. An image histogram acts as a graphical representation of the tonal distribution in a digital image. It plots the number of pixels for each tonal value. By looking at the histogram for a specific image a viewer will be able to judge the entire tonal distribution at a glance
7. At last, we will do Template matching. It is a process of moving the template over the entire image and calculating the similarity between the training image present in the sets of images and the input image.
8. After features matching we will get the image that matches the most with the features of the input image and set of images present in the dataset.
9. Finally, we have will have the result.
10. This can be done by using any of the algorithms in artificial neural networks. We have used SVM (Support Vector Machine), K-means and convolution.
11. The result obtained from SVM had an accuracy over 85.71 percent. The accuracy of images obtained from K-means was about 70.90 percent whereas the accuracy obtained from convolution was 68.784 percent.
12. Out of these techniques, we can conclude that SVM provided the highest accuracy and thus can be considered to be an efficient algorithm among all the three mentioned algorithm.
13. The reason to provide preproccesing is to filter out the image and to verify the results manually whether these algorithms are providing effective results.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2023 ||

| DOI:10.15680/IJIRSET.2023.1204160 |

V. EXPERIMENTAL RESULTS

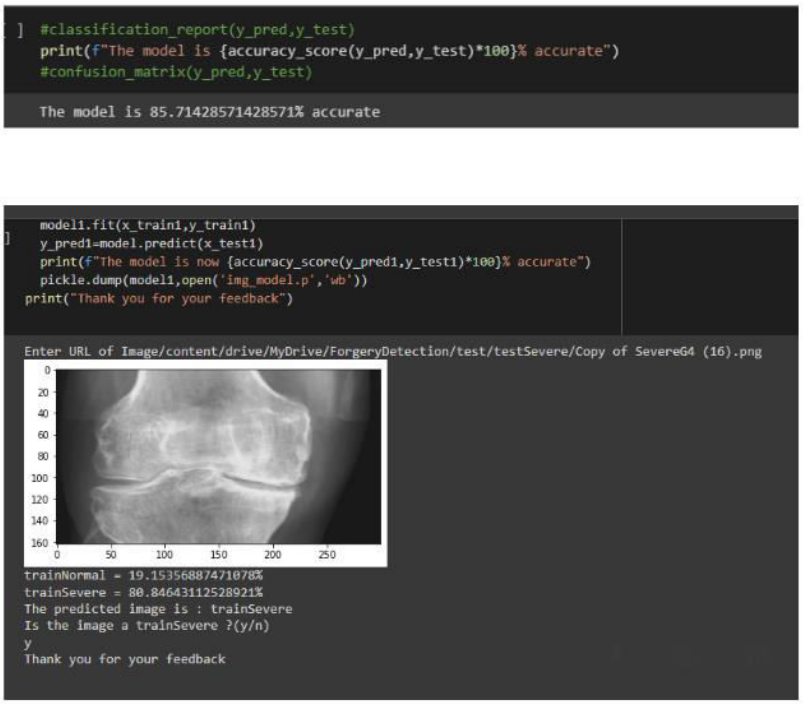

Fig 4.1 Accuracy obtained by SVM algorithm.

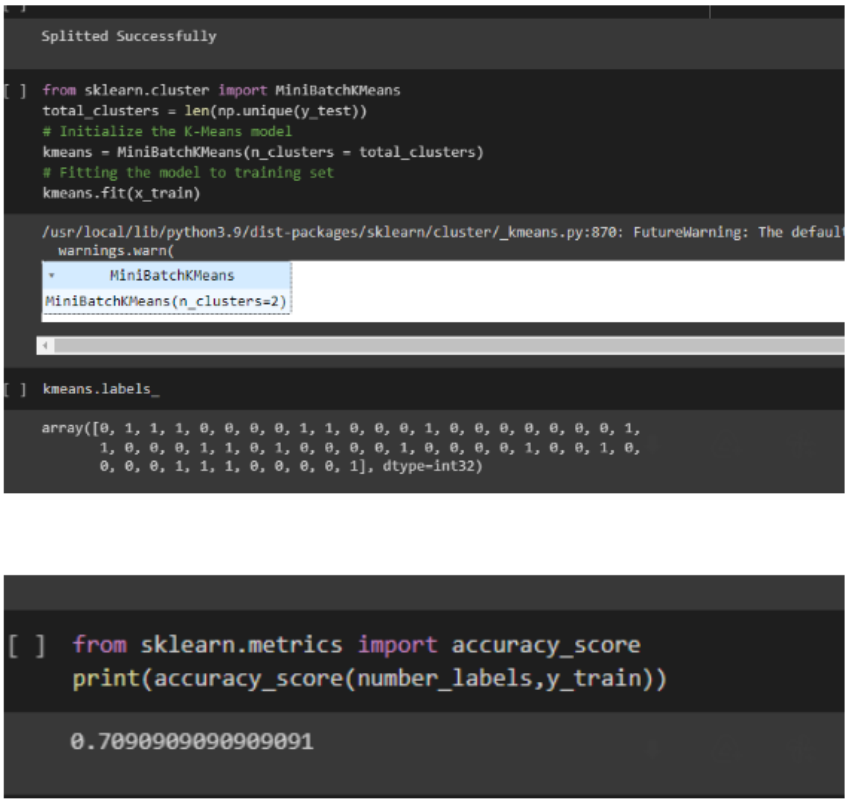

Fig 4.2 Accuracy obtained by K-means algorithm.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2023 ||

| DOI:10.15680/IJIRSET.2023.1204160 |

```
Epoch 1/5
2/2 [==============================] - 12s 6s/step - loss: 1.6005 - acc: 0.5469
Epoch 2/5
2/2 [==============================] - 7s 2s/step - loss: 1.3224 - acc: 0.7188
Epoch 3/5
2/2 [==============================] - 7s 3s/step - loss: 1.1543 - acc: 0.7031
Epoch 4/5
2/2 [==============================] - 3s 654ms/step - loss: 1.0069 - acc: 0.7027
Epoch 5/5
2/2 [==============================] - 3s 2s/step - loss: 0.8570 - acc: 0.7027
```

```
2/2 [==============================] - 5s 4s/step - loss: 0.9005 - acc: 0.6078
test_loss, test accuracy [0.9005222916603088, 0.6078431606292725]
```

Fig 4.3 Accuracy obtained by Convolution algorithm.

VI. CONCLUSION

Thus, we have been to able to detect the forgery of a single image out of the results from a dataset. The area of medical image forgery detection needs more attention to gain the trust of patients and avoid their embarrassment. Our current project detects the x-ray images of knees successfully. For the copy move images, we have obtained the accuracy of above 85 percent using SVM algorithm.

REFERENCES

[1] Ahmed Ghoneim, Ghulam Muhammad, Syed Umar Amin, and Brij. Gupta, quot;Medical Image Forgery Detection,quot; IEEE, vol. III, no. 12, pp. 60-82, JULY 2021.
[2] Pengpung Young, quot; Double JPEG COMPRESSION DETECTION BY EXPLORING THE CORRELATIONS IN DCT, quot; IEEE, vol. III, no. 13, pp. 40-62, January2019.
[3] Ms. Jayshri Charpre and Ms. Antara Bhattacharya, quot; Revealing Image Forgerythrough Image Manipulation Detection,quot; IEEE, vol. IV, no. 11, pp. 50-62, February2019.
[4] S. P. Ghrera and Vipin Tyagi Mohd. Dilshad Ansari1, quot; Pixel-Based ImageForgery Detection,quot; IEEE, vol. V, no. 10, pp. 40-52, JULY 2018.
[5] Mrs. Surbhi Sharma and Umesh Ghanekar, quot; A rotationally invariant texturedescriptor to detect copy move forgery in medical images,quot; IEEE, vol. IV, no. 11,pp. 70-92, AUGUST 2018.
[6] Muhammad. G Hussai, Al sawadi, quot; Copy-move image forgery detection usinglocal binary pattern and neighborhood,quot; IEEE, vol. III, no. 12, pp. 50-62, January2017.
[7] Rithin Krishna, India. Medical Image Forgery Detection. (Apr. 11, 2022). Accessed: Feb. 18, 2023. [Online Video]. Available: https://www.youtube.com/watch?v=AEZaySorOLst=90s.
[8] OKOKPROJECTS, India. Medical Image Forgery Detection for Smart Healthcare. (Sept. 24, 2021). Accessed: Feb. 18, 2023. [Online Video]. Available: https://www.youtube.com/watch?v=AEZaySorOLst=90s.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.423

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details