Medical Image Forgery Detection using Cnn

K. Premkumar, J. Preethi, J. Sandhya, Inti Satyapriya Harshini

Abstract: ***With the improvement of the computer technology, image processing techniques have become important in a wide variety of medical applications. Numerous new features have been added to satisfy people. People consult doctors online, without even visiting them. As health is a critical issue, we should take care with full attention and security. This paper proposes a medical image forgery detection system for the identifying whether the image is altered or not. The forgery done on the medical images can lead to various issues that can shake the medical industry this also promotes wrong diagnosis, organ trafficking etc. Hence a group of different forgery detection algorithms is described and by using the Convolution neural networks we can detect and the forged images. This paper also gives a brief outline about the advantages and disadvantages of the existing systems in forgery detection.***

Keywords: Convolution neural network, Copy-move attack, Forgery detection, Medical imaging.

I. INTRODUCTION

The popularization of digital cameras and the internet have become easy for anybody to capture and send pictures. As there are various image editing software tools such as Adobe Photoshop that allows anyone to create or alter images for malicious purposes. The term ‘image forgery' is commonly known in the world of powerful image editing tools. Recently, the healthcare sector has adopted various new techniques and drastic improvement has been done in terms of facilities. Since the medical sector is emerging many things should be taken into account in order to provide a safe and secure healthcare facility for people. For example, if medical data is altered or leaked, the patient may face serious problems such as social embarrassment. Therefore, we have implemented a system that can check if the medical images are altered during transmission via online by anybody like intruders or hackers. Detection of forged image from the original image is very hard. It is difficult to identify the tampered region from the forged image with naked eye.

Revised Manuscript Received on April 30, 2020.
* Correspondence Author

Mr.K. PremKumar*, Computer Science and Engineering, Sri Manakula Vinayagar Engineering College, Puducherry, India. Email: hodcse@smvec.ac.in.

J. Preethi, Computer Science and Engineering, Sri Manakula Vinayagar Engineering College, Puducherry, India. Email: preethijanakiraman06@gmail.com

J. Sandhya, Computer Science and Engineering, Sri Manakula Vinayagar Engineering College, Puducherry, India. Email: sandhyajeeva30@gmail.com

Inti Satyapriya Harshini, Computer Science and Engineering, Sri Manakula Vinayagar Engineering College, Puducherry, India. Email: intiharshini@gmail.com

Copy move image forgery is common among the various image forgery techniques, here a specific part of image is copied and pasted in the same image to cover some important information. The main focus of Copy -move forgery is to either make an object “hidden” or create an additional copy of an object in a specified location.

A. Copy-Move Attack:

The copy move forgery is famous because it is one of the most frequently used among the different kind of image tampering technique. In this method, a part of the image is covered in order to add or remove any information. A part of the same image is copied In Copy-Move Image manipulation technique. Then the copied part of the image is pasted into another part of that image itself. The intention of the copy-move attack is to hide something from the original image with the help of some other part of the same image.

B. Medical Imaging:

Medical imaging is the process of creating visual representation of the body as interior view for medical analysis. Medical imaging technique helps to treat various diseases that reveals the internal structures of organs. A database of normal anatomy and physiology has been established by medical imaging to make it possible to identify abnormalities.

II. RELATED WORKS

***Ahmed Ghoneim, Ghulam Muhammad, Syed Umar Amin, and Brij Gupta, “Medical Image Forgery Detection for Smart Healthcare”, April 2018*.**

This paper proposed an image forgery detection system to the healthcare frameworks. There are several components, such as noise-pattern extraction, the realization of a multi-resolution regression filter, and two classifiers. The color image will be decomposed. Each component of the color image is applied with a Weiner-filter. The resultant image will be noise free. To get an approximate noise pattern of the image, the noise free image is subtracted from original image. If any forgery is done, this fingerprint is distorted.This technique works locally in an image. There are also other noise reduction techniques but they have used this because there should not be any loss of information in medical images. It consists of three components, one is for the patients and the doctors, another is edge computing and the last component is the cloud computing. The patients can consult the doctors from remote areas itself. It is not necessary to go to hospital for basic checkups. Face to face interaction is not required. Nowadays they have facilities to interact via mobile phones, web apps etc.

The mobile app or the web app can be used by the patients to capture and upload the medical images. While uploading there may be devices that can embed the images with watermarks. Some work has to be done in the edge computing component to support real time transmission to the core cloud. The second component, edge computing is designed for low-latency and real-time transmission of data with limited computing resources. There are two management system are used in order to interact with the core cloud. They are: an edge computing platform applications management system and an edge computing hosting infrastructure management system. The communication applications, the wireless network, and the radio access network are managed by the edge computing management system. It can also interact with the application management system and the infrastructure as a service (IaaS). The edge computing hosting infrastructure management has a virtualization layer and hardware resources. The edge computing hosting infrastructure management system manages these two components. The application management system actually interacts with both the edge computing and the cloud computing. The data processing, feature extraction, classification, record keeping and processing can be done by the virtual machines of the system. The core cloud component consists of storage devices, virtual machines (servers), a registration and verification unit, and a distribution manager. The first time users are registered and verified using the registration and verification unit. The doctors/caregiver have to send the data and decisions to the patients. The load on the servers are minimized by the distribution manager. The distribution manager helps in distributing the works. The edge computing component and the cloud computing components helps in providing low latency and real time output. The cloud component contains the image forgery detection part. It makes use of two servers. One server is used for feature extraction. Another server is used for classification. The feature extraction part consists of many parallel units based on the image. If the image is monochrome, there is no need for parallel units. [1]

Yuan Rao1, Jiangqun Ni2 "A Deep Learning Approach to Detection of Splicing and Copy-Move Forgeries in Images", 2016

In this paper, deep learning technique was used for the new image forgery detection method. They used the convolution neural network (CNN) algorithm to represent the hierarchical representation of input colour image. The CNN algorithm is used here for image splicing and copy- move types of images. The first layer is the network layer which consists of weights. It is initialized with the basic high pass filter. The high pass filter is used for calculating residual maps in spatial rich model. The contents of the image is suppressed and captures the artifacts using the spatial rich model. To extract the key features from the test images the pre trained CNN is used as a patch descriptor. Then the most key feature is extracted for SVM classification using the feature fusion technique. The results of several dataset reveals that the proposed system performs better than the state of art methods. The proposed CNN has unique designs that overcomes the disadvantages of the existing detection applications. The first network layer is initialized with 30 basic high pass filter which helps in suppressing the complexity of the image and accelerates the convergence of the first layer. The CNN model here serves as a patch descriptor locally. The labeled patch samples issued for training the model. It is then used to extract the most important features from the test images and feature fusion technique is used. [2]

R.F. Olanrewaju, Othman. O. Khalifa, Aisha- Hassan Hashim, Akram M. Zeki and A.A. Aburas, "Forgery Detection in Medical Images Using Complex Valued Neural Network (CVNN)" , July 2015.

The medical images should be protected to keep the patient's documents against any act of tampering by unauthorized persons. The main aim is to develop some standard solution to preserve the authenticity and integrity of the content of medical images. Digital watermarking is used to enhance the security of medical images by adding special information, known as hidden data or watermark. Watermark information are inserted in a binary format to the pixel value of the host image. This factor has hindered proper detection and treatment. A new technique for embedding and detecting watermarked image using CVNN has been developed. The results obtained is the embedder using PSNR, IFM and SSIM shows that the watermarked images are minute and indistinguishable from the host images for a properly trained network. The tamper detector response will show that if the watermarked image is slightly manipulated even if one bit error occurred in the watermark message, it leads to a total different authentication it happens because of the embedding procedure. With this, it is easy to verify if the image is tampered. The results of the experiment confirmed that it is easy to correctly detect the watermark keys without using host image.[3]

Cao Y, Gao T, Fan L,Yang Q," A robust detection algorithm for copy-move image forgery of digital images", August 2012

The copy-move forgery done on digital image here a robust detection algorithm is used. DCT is used for finding DC coefficient. Each block is represented by circle block. Then the feature is extracted from each circle block. Forgery region is found by searching similar block pairs. There are many editing software and digital cameras by which region duplication can be done in image manipulation. This is possible by pasting part of an image into another location to conceal objects. Initially, the original input image is divided into fixed and equal sized blocks. Then a block is applied with discrete cosine transform. Hence, the DCT coefficients represent each block. Then, each cosine transformed block is represented by a circle block. As a result, nearly four features are extracted to reduce the dimension of each block. Finally, the feature vectors are sorted. A preset threshold value is maintained to which the duplicated image blocks are compared. In order to make the algorithm more robust, some parameters are proposed to remove similar blocks that are not correct.

Experiment results show that the proposed scheme is robust with low computational complexity.[4]

Hwei-Jen Lin, Chun-Wei Wang and Yang-Takao, "Fast copy-move forgery detection", May 2009

In order to detect forgery PCA are used to find features vectors and dimension reduction. After that application of radix sort is done to the feature vectors. It works well in noisy and compressed images. This algorithm is efficient. The input image is divided into equal sized overlapping blocks. And then feature for each block is extracted and represented as a vector. Using the radix sort all the extracted feature are sorted. Then the computation of difference of the positions of every pair of adjacent feature vectors in the sorting list is done. The evaluation of accumulated number of each of the shift vectors is done. The region with large accumulated number is decided to be the presence of a duplicated region. Hence large accumulated numbers for all the feature vectors corresponding to the shift vectors are detected. Lastly, the medium filtering and connected component analysis are performed on the detected region to obtain the final result. Compared with other methods, radix sort is more efficient because it does not degrade the detection quality. It works good in noisy, compressed image.[5]

III. PROPOSED WORKS

The advent of the computer technologies led to the rise of various image processing techniques. We proposed a medical image forgery detection system to verify that the images related to the healthcare are not altered. The idea is to group different forgery detection algorithms that are described. It outlines the strength and weakness of existing methods in forgery detection.

The proposed smart healthcare system Medco consists of several components. The patients can consult the doctors from remote areas itself. It is not necessary to go to hospital for basic checkups. They do not require a face to face interaction. Nowadays they have facilities to interact via mobile phones, web apps etc. The mobile app or the web app can be used by the patients to capture and upload the medical images.

The work flow of the proposed system is given below.

Step 1: The input image will be a color image. The most important step in image processing is to convert the image to the gray scale. The given input image is converted to gray scale so that we can extract the key features easily from a gray scale than a color image.

Step 2: The dataset consists of several manipulated medical images, normal medical images and diseased images. These datasets are trained in the .Net with the Accord.MachineLearning package. The trained dataset helps in differentiating the images. (i.e.) to verify whether the medical image is manipulated or not.

Step 3: The next step is to apply the CNN (Convolution neural network) algorithm to the gray image. It is used here to detect the smallest parts of the image. CNN algorithm is used for image classification. The convolution layer consists of various convolution filters. The resultant values are passed to the next layer. In the pooling layer, reduction of data dimensionality is done. Classification is done in the fully-connected layer according to the learned results. As a result, local features are extracted.

Step 4: KNN captures the idea of similarity. Here we calculate the distance between features on the image. As a resultthere may be missing values that we should either fill or remove from the data or there may be some mismatch of values.

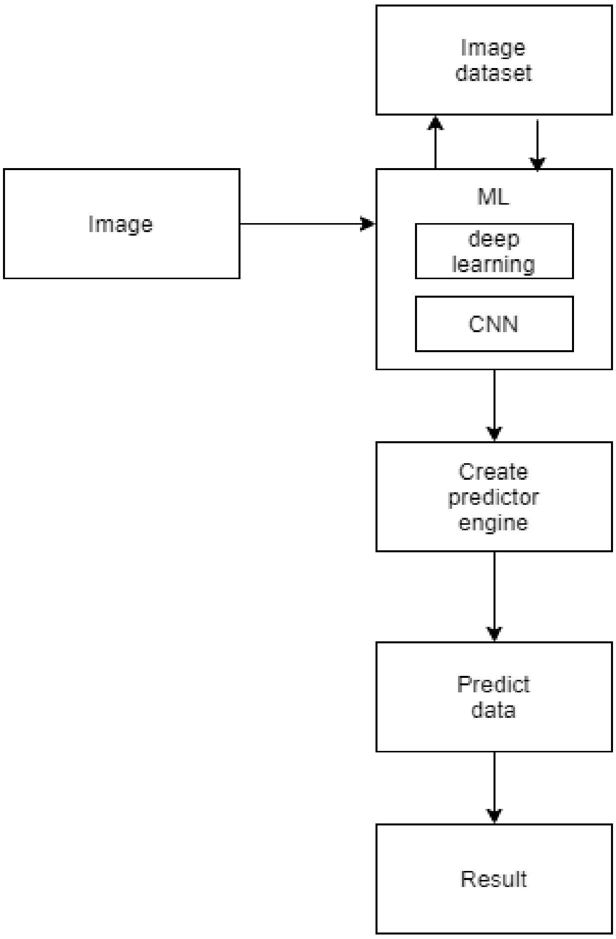


Fig.1 Architecture of Proposed System

Step 5: The predictor engine is used to find whether the image is manipulated or not with reference to the trained dataset.

Step 6: Thus the output concludes whether the image is resized image or replaced image or disfigured image.

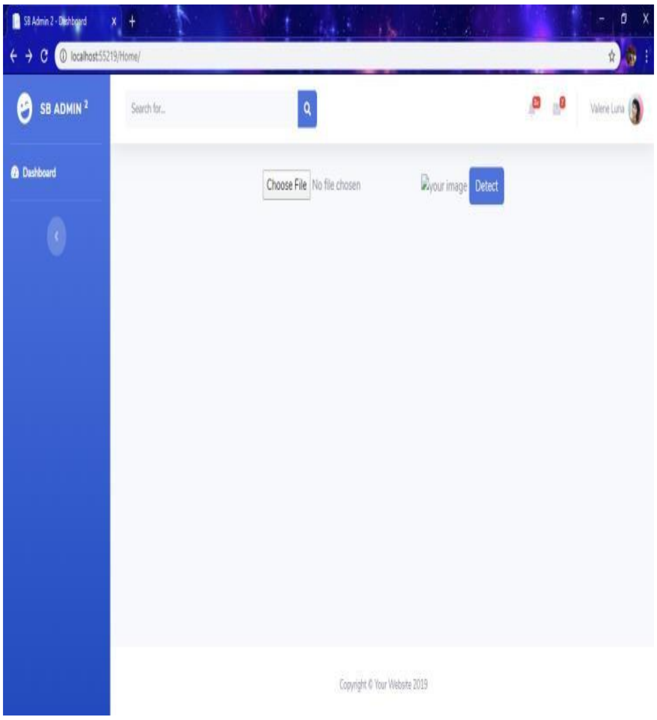
A. LIST OF MODULES

- GUI
- Detection of altered regions
- Output

3.1 GUI

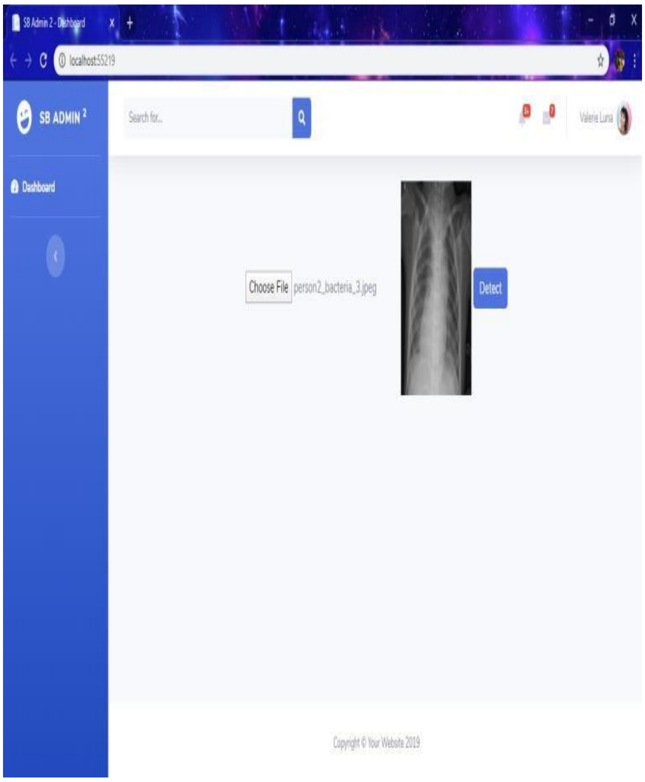
The MEDCO has a user friendly interface which helps the user to navigate through the process easily. It consists of three buttons. The "Choose File" button which allows us to choose the medical image.

After uploading the image, the "Detect" button is used to detect whether the image is forged or not.



3.2 DETECTION OF ALTERED REGIONS

The input image is converted into gray scale image. The image is classified into 10 parts. And each of the part is further classified. The pixel value of each part is then compared with the neighboring pixel so as to detect if it is forged or not. If the image is forged, the MEDCO detects what type of alteration has been done, like image resizing, replaced image, disfigured image.



3.3 OUTPUT

The final module is the output. After the detection process has been completed, it is necessary to display the output. An alert is used to show the result.

IV. EXPERIMENTAL RESULTS

The result of our project is well defined, the outputs of each modules are well defined above with the screenshots and it will work effectively in any conditions since we have used the best algorithm and CNN.

V. CONCLUSION

As the internet advances rapidly in modern society, there are many social networks such as Facebook, Instagram and so on which have been used for both good and bad reasons. Under these situations, forgery on videos are happening for illegal reasons. Digital methods are needed to detect these illegal purposes. Things that we see today are not there on the next day. Any image can be forged and misused for advertising, political purpose etc. In this paper we have proposed a system for medical image forgery detection to check whether the medical image is forged or not. The Image forgery detector is something that detects the tampered images with high accuracy.

REFERENCES

1. Ahmed Ghoneim, Ghulam Muhammad, Syed Umar Amin, and BrijGupta "Medical Image Forgery Detection for Smart Healthcare", April 2018.
2. Yuan Rao1, Jiangqun Ni2 "A Deep Learning Approach to Detection of Splicing and Copy-Move Forgeries in Images", 2016.
3. R.F. Olanrewaju, Othman. O. Khalifa, Aisha- Hassan Hashim, Akram M. Zeki and A.A. Aburas, "Forgery Detection in Medical Images Using Complex Valued Neural Network (CVNN)" , July 2015.
4. Cao Y, Gao T, Fan L,Yang Q," A robust detection algorithm for copy-move image forgery of digital images", August 2012.

AUTHORS PROFILE

Mr. K. Premkumar pursed Bachelor degree from Adhipara Sakthi Engineering College and Master degree in Computer Science and Engineering from Sathyabama Deemed University, Chennai. He is pursuing his P.hd in the field of Vanet at Manonmaniam Sundaranar University, Tirunelveli. He has 16 years of teaching experience.

J. Preethi is pursuing Bachelor of Technology in the stream of computer science and Engineering at Sri Manakula Vinayagar Engineering College, Puducherry affliated to Pondicherry University, Puducherry, India. Her field of interest includes Database Management System, Oops and Android development.

J. Sandhya is pursuing Bachelor of Technology in the stream of computer science and Engineering at Sri Manakula Vinayagar Engineering College, Puducherry affliated to Pondicherry University, Puducherry, India. Her field of interest includes Database Management System, Oops and Internet of things (IOT).s

Inti Satyapriya Harshini is pursuing Bachelor of Technology in the stream of computer science and Engineering at Sri Manakula Vinayagar Engineering College, Puducherry affliated to Pondicherry University, Puducherry, India. Her field of interest includes Database Management System, Oops and Internet of things (IOT).