International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 03 | March - 2023 Impact Factor: 7.185 ISSN: 2582-3930

A Survey on the Effective Machine Learning Approaches for Medical Images Forgery Detection

Divya Mohan[1], Aleena Carolin[2], Anaya Babu[3], Diya P.S[4], Natasha K George[5]

[1] Professor, Department of Computer Science & Engineering, Albertian Institute of Science & Technology, India

[2] Student, Department of Computer Science & Engineering, Albertian Institute of Science & Technology, India

[3] Student, Department of Computer Science & Engineering, Albertian Institute of Science & Technology, India

[4] Student, Department of Computer Science & Engineering, Albertian Institute of Science & Technology, India

[5] Student, Department of Computer Science & Engineering, Albertian Institute of Science & Technology, India

---

Abstract - In today's scenario medical image forgery has turned out to be unsophisticated because of capable PCs, propelled image editing softwares and high resolution capturing gadgets. Insurance fraud is a deliberate deception perpetrated against or by an insurance company or agent for financial gain. The only downside that the health insurance industry has faced is the rise in the number of health insurance frauds. An endeavor is prepared to review the current improvements in the research area of advanced medical image fraud detection and comprehensive reference index has been exhibited on different methods for medical forgery identification.

Key Words: CNN, Forgery detection, medical images

1.INTRODUCTION

Since the invention of photography, individuals and organizations have often sought ways to manipulate and modify images in order to deceive the viewer. Whilst originally a fairly difficult task requiring many hours of work by a professional technician, with the advent of digital photography it is now possible and fairly trivial for anyone to easily modify images and even easier to achieve professional looking results. This has resulted in wide reaching social issues ranging from the reliability of the images reported by the media to the doctrine of photographs of models in order to improve their looks or body image. With the sheer amount of methods available in which to manipulate an image, image forgery detection has become a growing area of research in both academia and the professional world alike. Many methods exist in order to detect forgery within digital images, however it is difficult to find which are the most efficient and practical to implement and run. Whilst one algorithm may have a good detection rate, it could also have a large rate of false positives. In addition, runtime is a major factor that contributes to the efficiency and overall usability of an algorithm but tends to only be mentioned academically as opposed to in real world terms.

One of the most pressing issues is that there are many different ways of modifying an image and due to digital images complex nature it's impossible to have an algorithm that detects every type of image forgery. Because of this, image forgery detection isn't widely used in the professional world. The underlying concept would be highly useful in the majority of professional fields that deal with images on a day to day basis where the reliability and credibility of these images is crucial. In addition, with the large increase in the use of social media, individuals would also benefit greatly from being able to detect forgeries within images. Convincingly manipulated images are widely circulated on social media platforms and are able to be spread rapidly within communities who believe them to be true. In order to detect these image forgeries, it is required that we understand some typical methods used in order to manipulate images. These include:

- Copy-paste Cloning - This is where existing areas within an image are cloned allowing regions to be covered or objects to be duplicated. This is a commonly used method as the forgeries have the potential to look very convincing due to the fact that they have come from the source image to begin with.
- Image Splicing - Whereby objects from another image are spliced together with the source

image, adding objects that weren't present in the original image. Various blending techniques exist such as blurring edges, reducing the contrast and utilizing cloning to help disguise the new object in with the surrounding area.

- Modification of existing regions - This is similar to copy-paste cloning but instead of being an exact duplication, existing regions are modified inorder to suit the needs of the forgery. This can include simply resizing the object, mirroring or skewing it, or splicing two existing objects together. In all of these cases however, the duplicated region has been resampled, meaning that it has been modified enough not to be recognized by any clone detection algorithm.

2. Literature Survey

2.1 A Deep Learning Approach to Detection of Splicing and Copy-Move Forgeries in Images

In this paper [1], a novel image forgery detection approach is proposed which utilizes a convolutional neural network (CNN) to automatically learn hierarchical representations from the input RGB color images. The proposed CNN is specifically designed for image splicing and copy-move detection applications. It consists of 8 convolutional layers, 2 pooling layers and a fully-connected layer with a 2-way softmax classifier. The input volume of the CNN are patches of size 128×128×3. The first and second convolutional layers have 30 kernels with a receptive field of 5×5 while other layers all have 16 kernels of size 3×3. For activation function, Rectified Linear Units (ReLU) is applied to neurons to make them selectively respond to useful signals in the input. Both the second and forth convolutional layers are followed by a non-overlapping max-pooling with filter of size 2×2, which resizes the input spatially and discards 75% of the activations. To improve the generalization, local response normalization is applied to the feature maps before the pooling layer where the central value in each neighborhood is normalized by the surrounding pixel values. Finally, the extracted 400-D features (5×5×16) are passed to the fully-connected layer with 2-way softmax classifier through "dropout" which sets to zero the neurons in the fully-connected layer with probability of 0.5. The primary contributions are summarized as follows: (1) First a supervised CNN is trained to learn the hierarchical features of tampering operations (splicing and copy-move) with labeled patches (p×p) from the training images. The first convolutional layer of the CNN serves as the pre-processing module to efficiently suppress the effect of image contents. Instead of the random strategy, the kernel weights of the first layer are initialized with the 30 basic high-pass filters used in calculation of residual maps in spatial rich model (SRM), which helps to improve the generalization ability and accelerate the convergence of the network. (2) Then the features for an image are extracted with the pre-trained CNN on the basis of p×p patch by applying a patch-sized sliding-window to scan the whole image. The generated image representation is then condensed by a simple feature fusion technique, i.e. regional pooling, to obtain the final discriminative feature. (3) Finally, a SVM classifier is trained based on the resulting feature representation for binary classification (authentic/forged). The experimental results on several public datasets demonstrate that the proposed scheme can outperform some state-of-the-art methods

2.2 Discriminating Original Region from Duplicated One in Copy-Move Forgery

Copy-move forgery detection methods are mostly based on finding similar regions by providing a binary mask as their output in which each pixel is identified as either background or copy-move pixels [2]. Since the original and forged region are parts of the same image, detecting the duplicated snippet is a challenging task. In this paper, a method for discriminating the duplicated region from the original one is presented. This method employs texture information of the border regions of detected copy-move regions. The image texture describes the local arrangement of color and intensities. Local texture consistency might be damaged after any manipulation performed to mask the trace of forgeries. As a result, texture analysis can be exploited to discover local inconsistency. Local binary patterns (LBP) is a kind of visual descriptor and one of texture analysis methods which generate proper features for texture classification. Since LBP extracts statistical and structural features of the textures, they are considered as a powerful tool for texture analysis. In LBP, pixel brightness (intensity) is compared with the neighboring pixels brightness. Neighboring pixels can be selected in different radiuses and get a value zero or one based on differences with the central pixel. The values of neighboring pixels are converted from binary into decimal. In order to discriminate against the forged patches, LBP is applied to the grayscale image. Since

the forged regions are usually modified by a low pass filter in order to disappear its borders with the background, it is expected that the LBP histogram of duplicated regions will be smoother. By calculating the standard deviation of the LBP histogram, it is possible to detect the copied patches.

The proposed method has been validated using the GRIP dataset. The presented method can detect the forged regions with accuracy of 67.5%.

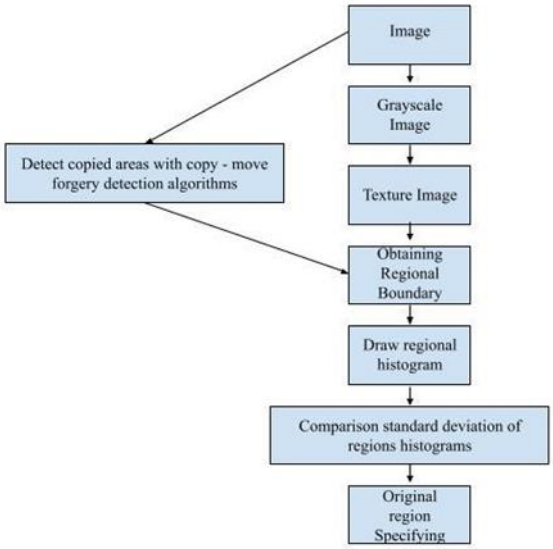

Fig -1: Flowchart finding original & copied region

2.3 Forgery detection in medical images with distinguished recognition of original and tampered regions using density based clustering technique

This paper [3] proposes a passive keypoint-based approach for forgery detection in medical images. They applied boundary extraction followed by Laplacian blob detection to find the regions of the image having similar properties. For keypoint extraction from image, they applied Good Features To Track (GFTT) technique. To compute descriptors for extracted keypoints, BinBoost technique is used. For identification of similar descriptors, Hamming distance-based nearest neighbor search technique is utilized. Clustering over keypoints with similar descriptors is performed using Ant Colony Density-based Clustering (ACDC). Further, Fast Sample Consensus (FSC) technique is applied for selection of correct matches and removal of imprecise keypoints. Correlation map generation is utilized for localization of forged regions within an image. After detection of the forged region, the rectangular area is selected around the copy and moved regions with extended pixels in the surrounding area. The selected region is divided into blocks. Feature descriptor for each block is computed using GLCM and Haralick texture features. Further, Pearson product-moment correlation coefficient is computed for feature descriptors. The average value for correlation coefficient corresponding to the localized regions is computed. The region having high correlation value is distinguished as the original region of image while the other region is considered as a duplicated or cloned region. To analyze the performance of the proposed technique, images are collected from various medical image repositories such as NIH, TCIA, NAMIC, SICAS, etc. Medical images belonging to different modalities such as CT scan, Digital X-rays, Ultrasound, MRI, and PET are utilized for experimentation. This technique is able to detect forged medical images even when they are distorted using several post-processing and geometrical attacks. Proposed scheme has achieved improved forgery detection results as compared to state-of-the-art techniques. In addition, the proposed technique can also distinguish between original and tampered regions present within forged medical images using Haralick texture features and Pearson product-moment correlation coefficient computation. This technique has achieved better results while distinguishing between authentic and forged regions of image as compared to state-of-the-art methods.

2.4 Image forgery detection using Deep Neural Network

In this paper [4], a unique image forgery detection system based on neural networks and deep learning, emphasizing the CNN architecture approach is provided. To achieve satisfactory results, the suggested method uses a CNN architecture that incorporates variations in image compression. The difference between the original and recompressed images is used to train the model. The proposed technique can efficiently detect image splicing and copy-move types of image forgeries. It is a lightweight CNN-based architecture designed to detect image forgery efficiently.

The system will take the forged image and then recompress it. It is compressed using JPEG compression. When an image is recompressed, if it contains a forgery, the forged portion of the image

compresses differently from the remainder of the image due to the difference between the source of the original image and the source of the forged portion. Now due to the difference in the source of the forged part and the original part of the image, the forged part gets highlighted. As a result, it is used to train the CNN-based model to categorize an image as a forged image or a genuine one.

- CNN model consists of 3 convolutional layers after which there is a dense fully connected layer - The first and second convolutional layers consist of 32 filters of size 3-by-3, stride size one, and "relu" activation function.
- The third convolutional layer consists of 32 filters of size 7-by-7, stride size one, and "relu" activation function, followed by max-pooling of size 2-by-2.
- It is then followed by a dense layer that has 256 neurons with "relu" activation function, finally which is connected to two neurons (output neurons) with "sigmoid" activation.

The proposed technique explores numerous artifacts left behind in the image tampering process, and it takes advantage of differences in image sources through image recompression. While most existing algorithms are designed to detect only one type of forgery, this technique can detect both image splicing and copy-move forgeries and has achieved high accuracy in image forgery detection. Compared to existing techniques, the proposed technique is fast and can detect the presence of image forgery in significantly less time. Its accuracy and speed make it suitable for real-world application as it can function well even on slower devices.

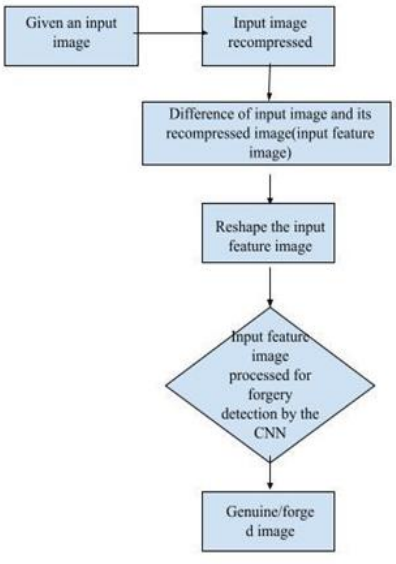

Fig -2: Flowchart finding original & forged region

The experimental results are highly encouraging and they show that the overall validation accuracy is 92.23%, with a defined iteration limit.

2.5 BusterNet: Detecting Copy-Move Image Forgery with Source/Target Localization

This paper [5] introduces a novel deep neural architecture for image copy-move forgery detection (CMFD), code-named BusterNet. BusterNet is a pure, end-to-end trainable, deep neural network solution. It features a two-branch architecture followed by a fusion module. The two branches localize potential manipulation regions via visual artifacts and copy-move regions via visual similarities, respectively. Extensive studies demonstrated in this paper states that BusterNet outperforms state-of-the-art copy-move detection algorithms by a large margin on the two publicly available datasets, CASIA and CoMoFoD and that it is robust against the proposed two-branch DNN-based CMFD solution. Dashed blocks are only activated during branch training. Output mask of the main task, i.e. MX c, is color coded to represent pixel classes, namely pristine (blue), source copy (green), and target copy (red). Output masks of auxiliary tasks, i.e. MX m and MX s, are binary where white pixels indicates manipulated/similar pixels of interest, respectively.

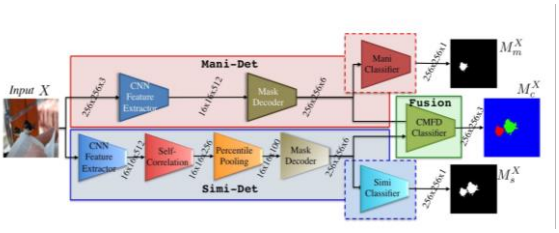

Fig -3: Overview of the proposed two-branch DNN-based CMFD solution

Main-Det branch to detect manipulated regions such that its feature is good for property (i), while Simi-Det branch to detect cloned regions such that its feature attains property (ii), and finally use both features in Fusion to predict pixel-level copy-move masks differentiating pristine, source copy, and target copy classes.

The manipulation detection branch can be thought of as a special segmentation network whose aim is to segment manipulated regions. More precisely, it takes input image X, extracts features using CNN Feature Extractor, up samples the feature maps to the original image size using Mask Decoder and applies Binary Classifier to

fulfill the auxiliary task, i.e. producing a manipulation mask MX m .Any convolutional neural network (CNN) can serve as CNN Feature Extractor. Here, we use the first four blocks of the VGG16 architecture. BusterNet Fusion - Fusion module takes inputs of the Mask Decoder features from both branches and jointly considers these two branches and makes the final CMFD prediction.

2.6 Composition of Visual Feature Vector Pattern for Deep Learning in Image Forensics

In this paper [6], the feature vector extraction method utilizes least-squares solution. Suspicious images are treated as matrices and their solutions are taken as coefficients to form feature vectors. Two such solutions are obtained from the original image and its median filter residual. These features are then combined into a visual pattern and fed into a CNN deep learning model to classify various transformed images. A new CNN net layer structure is also proposed [10] which uses the inception module and the residual block for classifying the visualized feature vector patterns. The proposed image forensics detection (IFD) scheme is evaluated with seven types of transformed images, including average filtered (window size: 3 × 3), gaussian filtered (window size: 3 × 3), JPEG compressed (quality factor: {90, 70}), median filtered (window size: {3 × 3, 5 × 5}), and unaltered images. The visualized patterns are input to the image input layer of the designed CNN hybrid model.

The proposed scheme consists of three steps, as follows and the flowchart is depicted as:

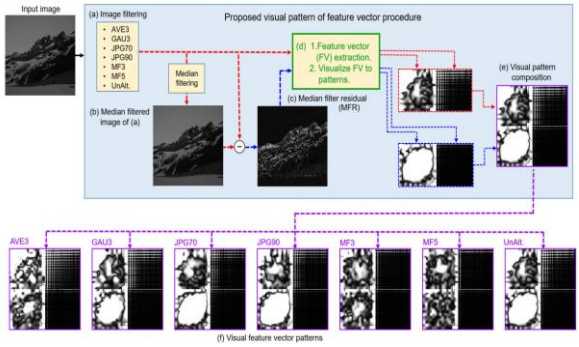

Fig -4: The proposed image forensics detection scheme

Step 1: Suspicious image is fed to the proposed scheme.

Step 2:

(a) The image is transformed - seven types of filters are mainly used:

• AVE3: average filtered (w: 3 × 3),

• GAU3: gaussian filtered (w: 3 × 3),

• JPG70: JPEG compressed (QF: 70),

• JPG90: JPEG compressed (QF: 90),

• MF3: median filtered (w: 5 × 5),

• MF5: median filtered (w: 5 × 5),

• UnAlt: Unaltered.

(b) The median filtered image (MF3) of (a).

(c) The median filter residual (MFR).

(d) With (a) and (c), the visual feature vector is generated as the afterward subsection A.

(e) The feature vectors of (a) and (c) are visualized to the pattern according to (d).

Step 3: The visual feature vector patterns (f) are configured corresponding to the transformed images (a).

The experiment results show that the accuracy of median filtering detection is over 98%. The proposed IFD scheme also achieves an area under the curve (AUC) by sensitivity (true positive rate) and 1-specificity (false positive rate) that approaches 1 on the designed CNN hybrid model.

2.7 Disentangling copy-moved source and target areas

In this paper [7] a source and target disentangling approach based on a local statistical model of image patches. The proposed method acts as a second-stage detector after a first stage of copy-move detection of duplicated areas. We had the following intuition: even if no manipulation (e.g. scaling and rotation) is added on the target area, its boundaries should expose a statistical deviation from the pristine area and the source area; further, if the target area is manipulated, the deviation should appear not only on the boundaries but on the full zone. It relies on machine learning tool with Gaussian Mixture Model [8] to describe the likelihood of image patches. Likelihoods are then compared between the pristine region and the candidate source/target areas as identified by the first-stage detector.

The given image to be analyzed is the input of this method and the binary mask produced by a first-stage

detector in which duplicated areas are identified indifferently.

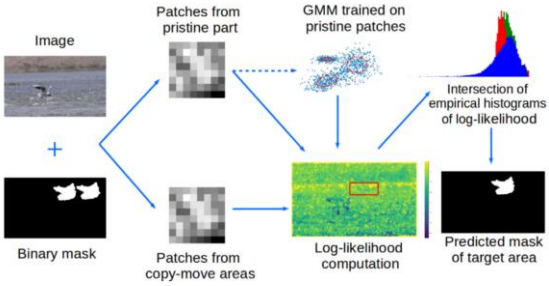

Fig -5: Graphical summary of the main steps of our method to disentangle copy-moved source and target areas

To discern source and target areas, first patches are extracted from the identified pristine region (black region in binary mask) and train a GMM to represent the statistics of pristine patches. The next step is to construct the empirical histogram of patch log-likelihood of all the connected components (CCs) in the binary mask, including the pristine region as well as the candidate source/target areas (white CCs in binary mask). Then compute the intersection between the histogram of pristine region and that of each candidate source/target area. The candidate area with the largest intersection is considered as the source area and the other(s) as target.

3. FINDINGS

This paper was written with the objective of conducting a survey on the different machine learning approaches used for medical images forgery detection. The survey mainly focused on the better performance of works in which deep learning approaches were used. The main reason for this is because deep learning models are nowadays highly used in image processing yielding better and superior results compared to the ones using classical machine learning methods. The task of medical images forgery detection can be extensively used in less explored area of fraud detection in claiming insurances. This will definitely be helpful to the officials in insurance domain and have better understanding of the same, which would otherwise lead to fraud practices.

Table 1 summarizes different approaches to image forgery detection mentioned earlier. It is observed that the models which are designed using convolutional neural networks provide more accuracy compared to other approaches [9]. Traditional approaches of forgery detection use handcrafted features for tampering detection. Instead, newer approaches based on deep neural networks (DNN) can outperform traditional methods due to their ability to extract complex features from the image.

4. CONCLUSIONS

The paper presented different approaches to medical image forgery detection. A comparative analysis of various detection methods, their features, and their effectiveness are discussed.

Some methods classify the image as original or tampered whereas some methods can detect the tampered region also. However there are only a few approaches which display the percentage of forgery.

REFERENCES

1. Yuan Rao, Jiangqun Ni, A Deep Learning Approach to Detection of Splicing and Copy-Move Forgeries in Images, 2017

2.Saba Salehi, Ahmad Mahmoodi-Aznaveh, Discriminating Original Region from Duplicated One in Copy-Move Forgery,2019

3.Anuja Dixit, Rahul Dixit, Forgery detection in medical images with distinguished recognition of original and tampered regions using density-based clustering technique,2022

4.Syed Sadaf Ali, Iyyakutti Iyappan Ganapathi, Ngoc-Son Vu,Syed Danish Ali, Neetesh Saxena and Naoufel Werghi,Image Forgery Detection Using Deep Learning by Recompressing Images,2022

5.Yue Wu , Wael Abd-Almageed , and Prem Natarajan, BusterNet: Detecting Copy-Move Image Forgery with Source/Target Localization, 2018

6. Kang Hyeon Rhee, Composition of Visual Feature Vector Pattern for Deep Learning in Image Forensics,2020

7.Ludovic Darmet, Kai Wang , François Cayre, Disentangling copy-moved source and target areas, 2021

8. R. F. Olanrewaju, O. Khalifa, A. H. Hashim, A. Zeki, A. Aburas, Forgery detection in medical images using Complex Valued Neural Network (CVNN), 2018

9. Ahmed Ghoneim, Ghulam Muhammad, Syed Umar Amin, Brij Gupta, Medical Image Forgery Detection for Smart Healthcare,2018

10.Sameer Khan; Suet-Peng Yong, A Deep Learning Architecture for Classifying Medical Images of Anatomy Object, 2018

Table -1: Comparison between different approaches of medical image forgery detection system

Sno.	Title	Algorithms used	Dataset	Performance
1	A Deep Learning Approach to Detection of Splicing and Copy-Move Forgeries in Images (2016)	• Convolutional Neural network • SVM classifier	CASIA v1 CASIA V2 1725	Accuracy: 98%
2	Discriminating Original Region from Duplicated One in Copy-Move Forgery (2019)	• DCT-For overlapping blocks. • LBP to find original region & duplicate region	IMD MICC-F220 MICC-F2000 SBU-CM16 GRIP 2800	Accuracy: 67%
3	Forgery detection in medical images with distinguished recognition of original and tampered regions using density based clustering technique(2022)	• Laplacian blob detection • Good Features To Track (GFTT) and BinBoost techniques • Ant Colony Density-based Clustering (ACDC) technique • Fast Sample Consensus (FSC) technique	NIH Open access biomedical search engine CoMoFoD CASIA v2	• For dataset CoMoFoD, Accuracy :42% • For dataset CASIA V2, Accuracy 50%
4	Image forgery detection using Deep Neural Network(2022)	• Convolutional Neural network	CASIA V2 7200 (ORIGINAL) 5132(FORGED)	• Using RESNET50 , Accuracy: 95% • Using CNN sharpen ELA, Accuracy: 97%
5	BusterNet: Detecting Copy-Move Image Forgery with Source/Target Localization	• BusterNet, • end-to-end DNN	CASIA TIDEv2.0 CoMoFoD	Accuracy: 78%
6	Composition of Visual Feature Vector Pattern for Deep Learning in Image Forensics	• Hybrid CNN model of GoogleNet and ResNet	BOWS2 UCIDver.2	Accuracy: 96%
7	Disentangling copy-moved source and target areas (2021)	• Binary mask • GMM • Compare the histograms.	CASIA2 and CoMoFoD	Casia2 Accuracy 41.81% CoMoFoD Accuracy 34.50%