iJRASET
International Journal For Research in Applied Science and Engineering Technology

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

**Volume:** 12 **Issue:** III **Month of publication:** March 2024

**DOI:** https://doi.org/10.22214/ijraset.2024.59323

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538*
*Volume 12 Issue III Mar 2024- Available at www.ijraset.com*

# Securing Medical Imaging: A Comprehensive Review and Prospective Paths for Image Authentication

Aruna S[1], Akkidasari Varshitha[2], K L Kalpana[3], Yash Santosh Karwa[4], Jyothi R[5]
*Department of Computer Science Engineering, Dayananda College Engineering, India* arunadpi@gmail.com

***Abstract:*** ***As medical image authentication systems depend more and more on cutting-edge technologies, the integrity and dependability of diagnostic procedures are seriously threatened by adversarial attacks. This abstract reviews the latest advancements in Deep Learning (DL)-specific image forgery detection techniques, highlighting common splicing and copy-move attacks as well. This survey covers a wide range of methods used in medical image forgery detection and highlights the role that sophisticated models play in maintaining the accuracy of medical images. The study looked at a range of deep learning and machine learning models as well as methods for isolating photos and using Generative Adversarial Networks (GANs) to detect tampering. The results showed that it is possible to reliably recognize intentionally created anomalies in medical imaging. The case studies show that deep learning performs exceptionally well in correctly identifying scans with injected tumours, especially when it comes to the localization of the region of interest. This works well in situations where localization is not feasible, as reduced-negativespace scans show.***

***Keywords: Convolutional neural networks (CNNs), Deep learning, Local Binary patterns (LBP) Generative adversarial networks (GANs), Medical imaging.***

## I. INTRODUCTION

Medical diagnosis and treatment planning have undergone a dramatic transformation in recent years due to the extensive incorporation of digital imaging technologies. Digital imaging modalities have smoothly replaced film-based radiography, improving medical procedures' efficiency but also posing new problems with regard to the quality and authenticity of medical images. The increasing dependence on digital medical imaging raises serious concerns for researchers and healthcare professionals regarding the possibility of malevolent manipulations and inadvertent adjustments.

A rising number of people are worried about the authenticity and integrity of digital images because of its widespread use in many different fields. With the use of a wide range of methods, image forgery detection has become an important field that protects digital image integrity while revealing modifications. Investigating both active and passive approaches, this study focuses on the use of CT GAN-based techniques as it explores the complex field of image forgery detection. Digital signatures and watermarking are examples of active forgery detection techniques that are essential to keeping digital images unchangeable. Passive methods of detecting forgeries, such as picture splicing and copy-move methods, use sophisticated algorithms and, most importantly, include CT GAN to improve the accuracy of identifying modified elements in images. This research limits its attention to the widely used techniques of image splicing and copy-move detection in the context of medical imaging, where the consequences of fraud can be fatal. The CT-GAN framework is one example of an adversarial technology that offers vulnerabilities that the research highlights and that could jeopardize the integrity of 3D medical images. The study delves into a thorough investigation of multiple strategies, including convolutional neural networks (CNNs), hybrid models, and deep learning techniques, to identify and counteract picture manipulation. It analyzes these techniques' effectiveness critically, pointing out both their advantages and disadvantages, and it deals with the constantly changing problems that emerge from new technology in the field of picture fraud detection. The following chapters cover copy-move forgery detection with CNNs, new segmentation techniques, and aggregation with Bayesian Sum Rule (BSR). Furthermore, in order to strengthen image forgery detection in smart healthcare systems, the research assesses the effectiveness of support vector machines and extreme learning machines in hybrid models.The paper presents a comprehensive overview of the state of picture forgery detection today by highlighting developments in the area while being open about the shortcomings and difficulties encountered by current approaches. By investigating these issues, the study hopes to add to the current discussion on picture authenticity by highlighting advancements and weaknesses in the field of counterfeit detection and suggesting new lines of inquiry.

©IJRASET: All Rights are Reserved 

A lot of study has been done in the field of image forgery detection in the last ten years. Figure 1 presents a bar chart that shows the number of publications pertaining to four different categories of forgery detection techniques (copy-move, image splicing, resampling, and retouching)**[1]** from 1998 to 2017. The detection of copy-move forgeries has significantly increased over the past ten years, highlighting the identification of image splicing. On the other hand, retouching detection has gotten relatively less attention, probably because it is thought to offer a lesser risk because altered images are usually not used for illegal activities. **[14]**

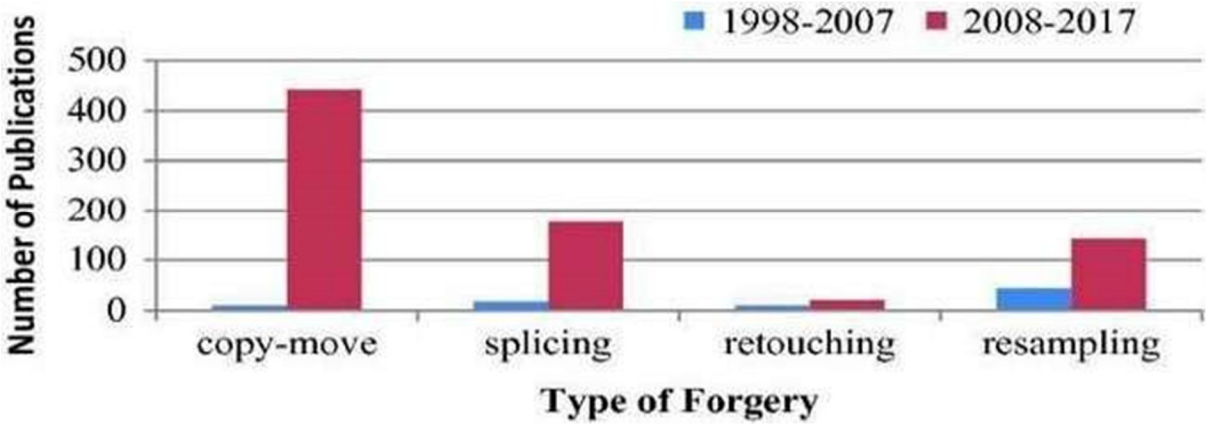



Fig. 1 Number of publications in the area of image forensics over the last two decades

## II. TYPES OF DETECTIONS

Image forgery detection employs a range of techniques to ascertain and validate the legitimacy of digital images. These strategies encompass both passive tactics, such as identifying image splicing and detecting copy-move forgery, as well as active methods like employing digital signatures and watermarks. The overarching goal is to expose various forms of image manipulation while upholding the integrity of the visual content.[1] The two primary categories of image forgery detection techniques are:

### *A. Techniques for Identifying Active Forgeries*

1) *CT GAN-Based Approaches:* Integrating cutting-edge advancements, like CT GAN (Generative Adversarial Network) technology, offers a robust means of ensuring tamper resistance. CT GANs can be employed to generate synthetic images that serve as digital signatures, harnessing cryptographic techniques for authentication.**[21]**
2) *Digital Watermarking:* Digital watermarking remains a stalwart method, introducing visible or invisible watermarks to images for traceability and authentication. This aids in swiftly identifying any unauthorized alterations, complementing the efforts of CT GAN-based approaches.

### *B. Methods for Detecting Passive Forgeries*

#### *1) Copy-Move Forgery Detection*

Incorporating CT GAN in the copy-move forgery detection process enhances the precision of identifying duplicate elements within an image. The synergy of CT GAN with block-based analysis, brute force, or keypoint-based algorithms fortifies the capability to detect subtle manipulations. **[3, 17, 18]**

#### *2) Picture Splicing Forgery Detection*

The detection of picture splicing forgeries undergoes refinement through CT GAN interventions. By amalgamating segments from various sources, CT GAN aids in recognizing modified images more effectively, thus fortifying the overall passive forgery detection. **[15, 20]**

#### *3) Image Retouching*

The focus on identifying alterations made to specific regions within an image gains added sophistication with the integration of CT GAN-based approaches. This ensures a nuanced understanding of subtle retouching, contributing to comprehensive forgery detection.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

In the realm of medical imaging, the two prevalent forgery detection methods revolve around image splicing and copymove detection. This discussion will delve deeper into these approaches, shedding light on their applications and efficacy in the context of medical imagery.

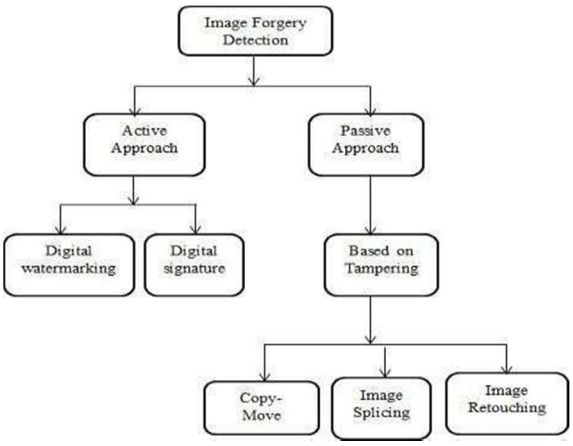



Fig. 2 Image forgery detection approaches

*C. CT-GAN-Based Approaches for Medical Image Tampering Detection*

Yisroel Mirsky **[21]** presented a new threat wherein adversaries can use deep learning to manipulate 3D medical imagery, specifically via a manipulation framework known as CT-GAN. Such attacks are explained and an attack vector is shown, along with their motivations. The use of easily obtainable medical pictures from the Internet is presented in this research to enable the CT-GAN framework to automatically detect or remove lung cancer from full-resolution 3D CT scans. The evaluation's findings highlight the need for care when drawing conclusions about the closed world because CT-GAN shows that it is capable of fooling both modern AI systems and radiologists. The research highlights the weakness of both sophisticated AI and human experts when total reliance is put on their observations.

A concerning vulnerability that could enable hackers to manipulate 3D medical images and misdiagnose patients was revealed by the study **[21]**. An attacker could take advantage of the confidence that is placed in volumetric medical scans to influence treatment decisions by injecting or deleting evidence of medical conditions, like lung cancer. Attackers may do these for a variety of reasons, such as influencing elections or using ransomware or insurance fraud to make money. In addition to outlining several attack scenarios, the paper highlights the possible effects on patient diagnoses and healthcare integrity. Because lung cancer has a high death rate, the emphasis on injecting and eliminating lung cancer from CT scans highlights how serious the threat is. Recognizing the wider applicability to MRIs and

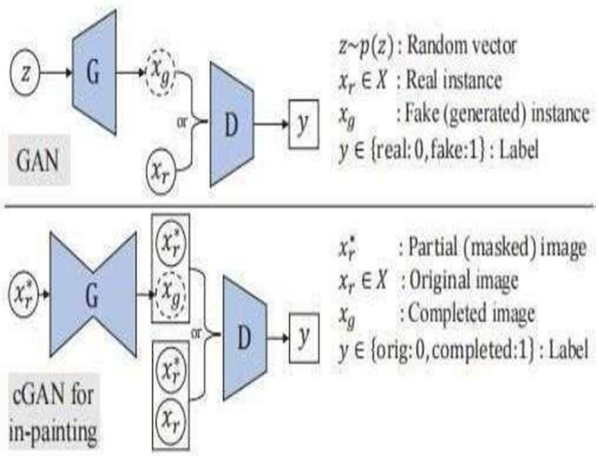



Fig.3 A schematic view of a classic cGAN (top) and a cGAN setup for in-painting

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

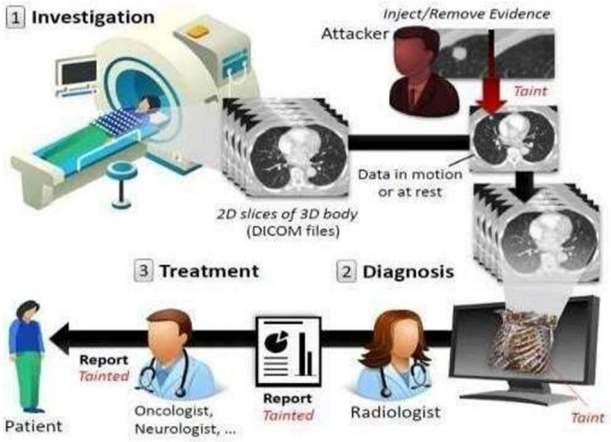
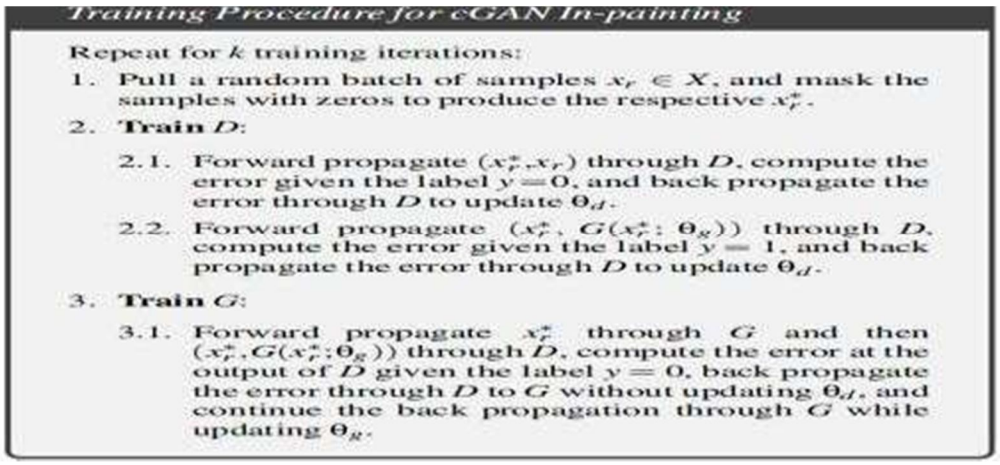



Fig. 4 By tampering with the medical imagery between the investigation and diagnosis stages, both the radiologist and the reporting physician believes the fallacy set by the attacker.



*Training Procedure for cGAN In-painting*

Repeat for $k$ training iterations:

1. Pull a random batch of samples $x_r \in X$, and mask the samples with zeros to produce the respective $x_r^*$.
2. **Train** $D$:
   - 2.1. Forward propagate $(x_r^*, x_r)$ through $D$, compute the error given the label $y = 0$, and back propagate the error through $D$ to update $\theta_d$.
   - 2.2. Forward propagate $(x_r^*, G(x_r^*; \theta_g))$ through $D$, compute the error given the label $y = 1$, and back propagate the error through $D$ to update $\theta_d$.
3. **Train** $G$:
   - 3.1. Forward propagate $x_r^*$ through $G$ and then $(x_r^*, G(x_r^*; \theta_g))$ through $D$, compute the error at the output of $D$ given the label $y = 0$, back propagate the error through $D$ to $G$ without updating $\theta_d$, and continue the back propagation through $G$ while updating $\theta_g$.

Fig.5 Training Procedure for cGAN In-painting

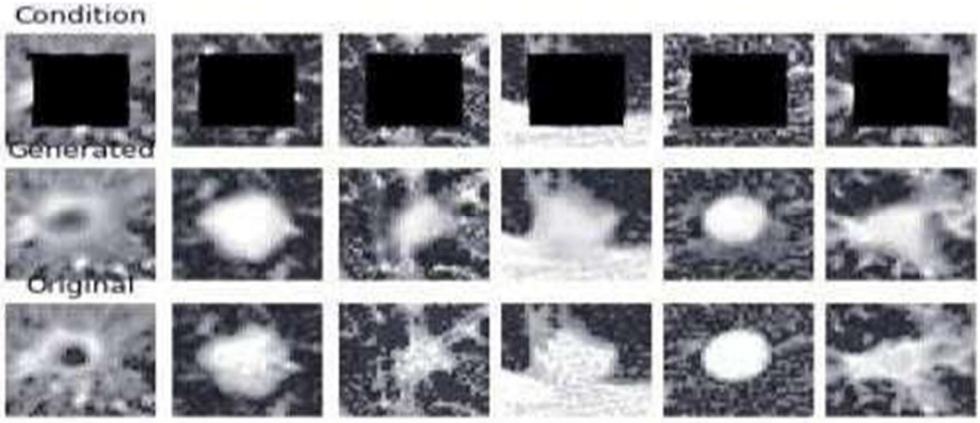



Fig.6 Training samples after 100 epochs showing the middle slice only. Top: the masked sample xr $*$ given to both the *generator Gin j* and *discriminator*

*Din j*. Middle: The in-painted image *xg* produced by the *Gin j*. Bottom: the ground-truth *xr* .Note, *Din j* sees either (xr $*$ , *xr*) or (xr $*$ , *xg*).

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

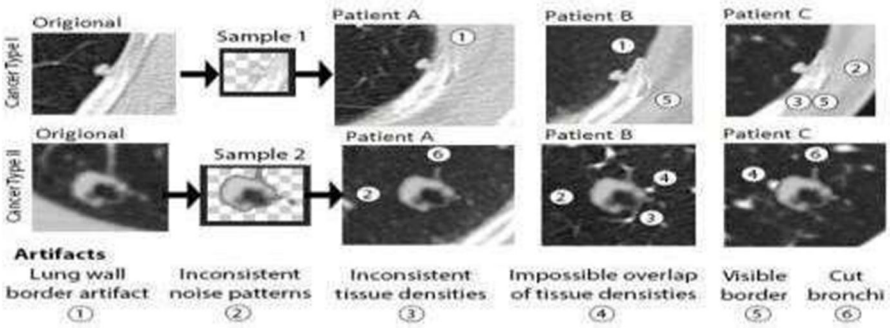



Fig.7 An illustration showing curiosities which can occur when using an *unsupervised* splice attack instead of CT-GAN.Only the middle slice is shown.

Though there are a number of issues and limitations to take into account, CTGAN is notably capable of producing artificial tabular data. As with other generative adversarial networks (GANs), CTGAN can experience mode collapse, which causes it to generate a small set of samples that are insufficient to adequately capture the variety of patterns present in the originally distributed data. The quality of the samples that are generated may also be impacted by CTGAN's inability to understand complex contextual relationships between variables. The model must be carefully tuned due to its sensitivity to hyperparameters, and determining the ideal configuration can be difficult. By reproducing statistical patterns from the training data, CTGAN raises privacy concerns by running the danger of unintentionally disclosing private information.

*D. Copy-move Forgery Detection*

In copy-move forgery, a portion of a picture is copied and pasted into another area of the same image. In order to deceive viewers, copy-move forgeries primarily aims to hide specific visual clues or duplicate features inside the image.The prominent reason behind the surge in copy-move forgery is the simplicity of this forgery. Figure 3 shows 2 images, The first image is real, whereas the second is the product of copy-move editing

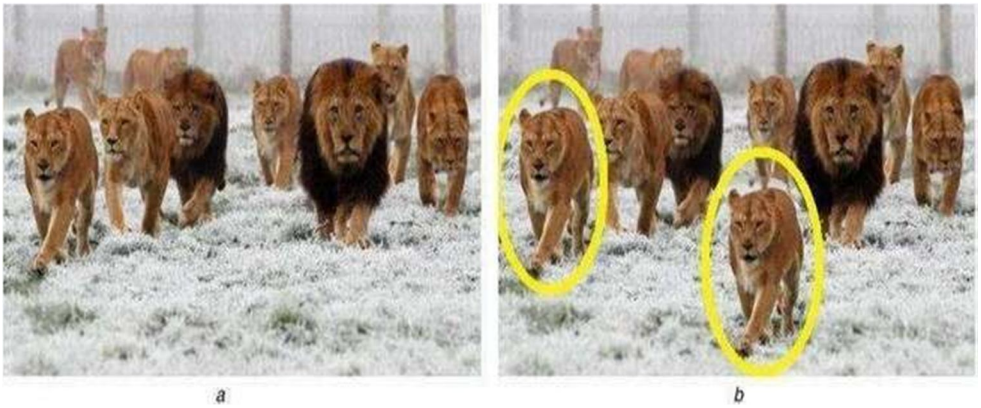



Fig. 8 Example of a Copy Move Image forgery

Muhammad Qadir, et al **[3]** have presented an approach for categorizing medical photos as original or counterfeit by detecting copy-move forgery using convolutional neural networks. Pre-processing entails scaling photos to 512x512 without cropping them. Three convolutional layers are used to extract features, and dense layers are used to aid with classification. Because there were no falsified medical photos available for public use, a dataset was built. This dataset is used to train and test the algorithm. Plans for the future include adding more kinds of forgeries, growing datasets with different organs and perspectives, and enlarging image sizes for better feature extraction. Figure 4 shows the proposed algorithm in their paper.

Three phases of Artificial Neural Networks (ANN) are used in this non-block-based image processing method: preprocessing, feature extraction, and classification. It uses four dense layers for classification, three convolutional layers with max-pooling for feature extraction, and input image scaling. The architecture classifies images as original or tampered, convolutional layers use the

ReLU activation function, and dropout minimizes overfitting—all of which demonstrate how AI and neural networks are integrated into modern image processing.

Three phases of Artificial Neural Networks (ANN) are used in this non-block-based image processing method: preprocessing, feature extraction, and classification. It uses four dense layers for classification, three convolutional layers with max-pooling for feature extraction, and input image scaling. The architecture classifies images as original or tampered, convolutional layers use the ReLU activation function, and dropout minimizes overfitting—all of which demonstrate how AI and neural networks are integrated into modern image processing.

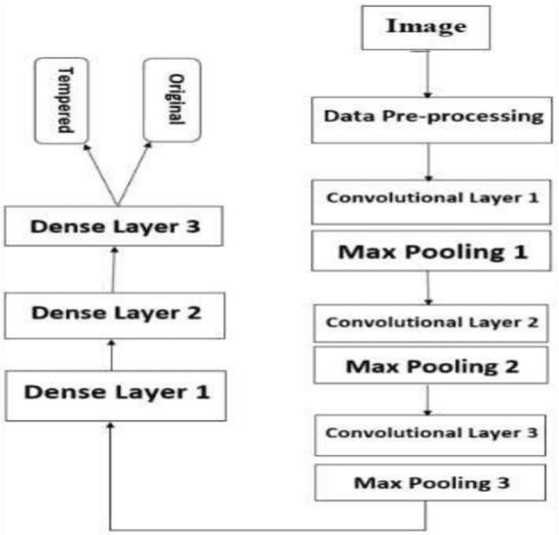



Fig. 9 Proposed copy move forgery algorithm for medical images

Datasets for experiment: Medical photos from CPTAC-LSCC , Data from Head and Neck Cancer CT Atlas , and applied copy move forgery on them because there isn't a publicly accessible dataset for fabricated medical images.The images are manipulated using Adobe Photoshop, which is the program most frequently used to insert fakes into photos. In some photos, items are additionally rotated before being pasted in while copymove forgery is being used. Greyscale JPEG files with 512 x 512 pixels are stored in this format. This collection has a variety of views of the spine, heart, lungs, and chest. Expert radiologists have been consulted for each annotation.

The suggested algorithm successfully detects forgeries in medical images, emphasizing the necessity for a customized method because the field of medical image forensics lacks a specific dataset. It also highlights shortcomings in existing watermarking and block-based methods. A comparison of the algorithm in the paper with other available approaches is shown in Figure 6.

His paper provides an overview of the latest developments in copy-move forgery detection (CMFD), as reported by Songpon Teerakanok et al. **[17]**.It presents a novel CMFD process pipeline and offers details on each processing step, including objectives, fundamental ideas, and related methods. Although there may not be many strategies available at this time for various phases of the proposed pipeline, the authors want to soon conduct additional surveys to provide updates. The purpose of the study is to provide field researchers with useful insights and up-to-date information.

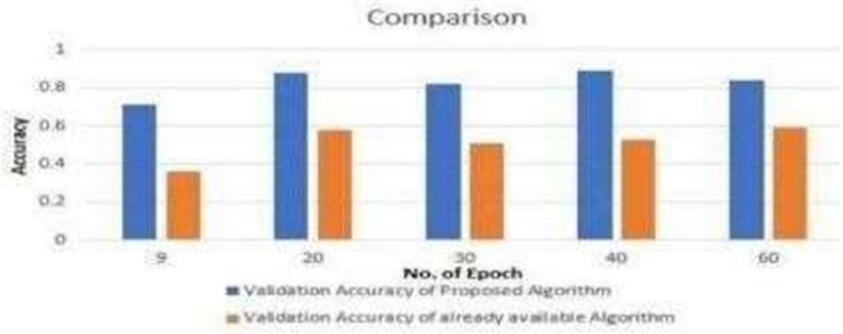



Fig. 10 Comparison of accuracy with existing system

Copy-move forgery (CMF) involves duplicating parts of an original image and pasting them back onto the same image after potential transformations or adjustments. The detection of copy-move forgery (CMFD) has seen various techniques, often categorized into block-based and keypoint-based methods. However, this paper introduces a new CMFD process pipeline that integrates these techniques into a unified framework, eliminating the traditional categorizations. As seen in Figure 7, the framework allows for flexibility in the order of steps, making some optional and skippable depending on certain goals. Part III describes the first step, Preprocessing, which includes converting or reducing the amount of information in the original image if desired. In order to improve subsequent detection processes such as color space transformation and segmentation techniques, it is imperative to preprocess the data when handling copy-move forgery detection in digital images. To identify forged areas, the procedure includes keypoint detection, feature extraction, matching, false match removal, and localization, all of which increase accuracy. In order to detect copy-move forgeries, a study contrasts deep learning with traditional techniques, emphasizing the superiority of deep learning in feature extraction and automatic classification. However, obstacles like a lack of training data and specialized applications prevent its general adoption. The study attempts to provide a thorough analysis of forgery detection techniques, as well as a detailed exploration of digital picture forgery and its classification of image forgery techniques.

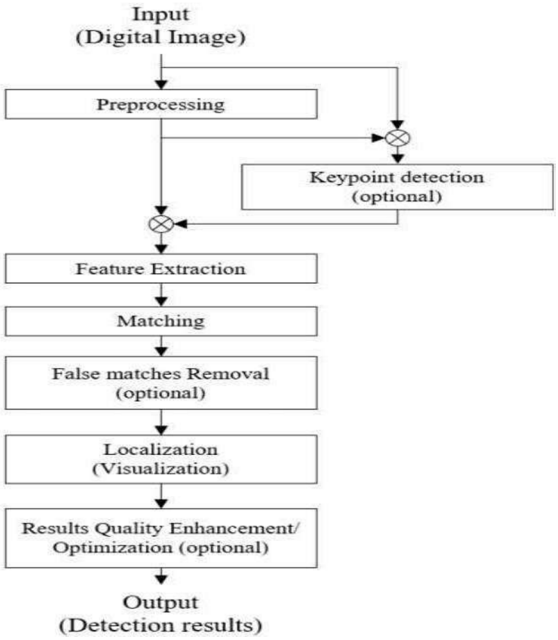



Fig.11 New CMFD Framework proposed in the paper

The role of deep learning approaches in Copy-Move Forgery Detection (CMFD) is highlighted in this research, which conducts thorough evaluations of modern methods in this field. Through an examination of existing approaches, it seeks to provide a succinct summary of the developments and difficulties in forgery detection. With important implications for practitioners and scholars alike, the study advances our knowledge of how deep learning improves the effectiveness and precision of CMFD.

Some of the algorithms used in Copy-Move Forgery Detection (CMFD) are resource-intensive due to issues including computational complexity. Maintaining balance between false positives and false negatives is an ongoing task, and robustness to transformations such as rotation and scaling is still a worry. Different image content may have different effects on performance, so it's important to have solutions that can deal with a variety of situations. Practical challenges include scalability for big datasets and device generalization. The process of improving CMFD capabilities is made more difficult by the need to obtain trustworthy ground truth data and deal with hostile threats. Sustaining these strategies in the face of developing digital image forgery tools requires ongoing research.

### *E. Image Splicing Forgery Detection*

The section of one image is copied and put into another to create a modified image, which is known as image splicing forgeries. An essential step in using a collection of photographs to create a photomontage is image splicing. Various postprocessing techniques,

including scaling, cropping, retouching, and rotating, can be applied to each component of the composite image to improve its realism. In order to hide any obvious impacts, additional postprocessing may be used following the splicing procedure.


Fig. 12 Example of image splicing forgery

S. Walia and K. Kumar emphasizes **[20]** a pixel correlation-based method for localizing spliced regions in images is presented and tested using the CASIA v1.0 and CASIA v2.0 datasets. The methodology considers overlapping blocks in the context of unsupervised localization and detection, while non-overlapping blocks are used in supervised methods. The GLCM descriptor is used to extract textural features, and experimental results show that the Hellinger distance performs better than the Euclidean distance in feature matching for the unsupervised technique.Using a linear kernel and featuring labeling, the supervised approach produces an 82.28% accuracy and 79.96% precision for the SVM classifier. Future research will focus on GLCM extension to multiple scales through techniques such as pyramid decomposition, hybrid classifiers for improved accuracy, and color effects. The primary objective of picture forgeries is to manipulate and remove important information from an image. The suggested methodology, which takes inspiration from a referenced work, is made to particularly detect this kind of tampering. There are two methods in this approach to image forgery detection: an unsupervised method and a supervised one.

The suggested technique for detecting image forgeries divides images into overlapping blocks and converts them to grayscale before using GLCM to extract features. To quantify the differences between blocks and help identify tampered regions, Euclidean and Hellinger distances are calculated. The forged area is localized on the image and a threshold value is applied for block selection. In the supervised method, an SVM classifier is used to learn the model after users generate a training set. The objective of both techniques is to improve the accuracy of forgery detection; the unsupervised method achieves a precision rate of 79.96%. Future research will examine the application of hybrid classifiers and the expansion of GLCM in an effort to further increase accuracy.

The suggested method performs well on publically accessible datasets and effectively detects image splicing in both supervised and unsupervised contexts, according to the results. The forgery detection method is tested on the CASIA v1.0 and CASIA v2.0 datasets, which contain a variety of authentic and forged images. In the unsupervised approach, images are reduced to 8 gray levels, divided into overlapping blocks, and GLCM is calculated. Euclidean and Hellinger distances are computed, and a threshold value of 0.3 yields optimal results for spliced region localization. The supervised approach makes use of non-overlapping blocks, GLCM calculation, and SVM classification, yielding an average accuracy of 82.28% and an average precision of 79.96%.

$$H(X, Y) = \frac{1}{\sqrt{2}}\sqrt{\sum_{i=1}^{k}\left(\sqrt{x_i}-\sqrt{y_i}\right)^2}$$

Hellinger distance is given above .N. Krishnamoorthy et al, **[15]** used Deep Learning (DL) technology to tackle image alteration problems, with a particular emphasis on splicing detection. With a f1 score of 0.96271 and good accuracy (0.9553), the DL model shows its efficacy in automatically detecting forged photos, especially those made via splicing techniques, using the CASIA V1.0 database.

MobileNet, which is renowned for its effectiveness in picture segmentation and classification, is used in the DL model selection process for image forgery prediction. MobileNet optimizes multi-add and parameter count by using depthwise separable convolution layers. The successive layers in MobileNet's internal structure, such as depthwise and pointwise convolutions, effectively reduce the size of images. By balancing channel depth and input image size, the model's hyperparameters—such as width and resolution multipliers—can be changed to improve network performance and speed.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

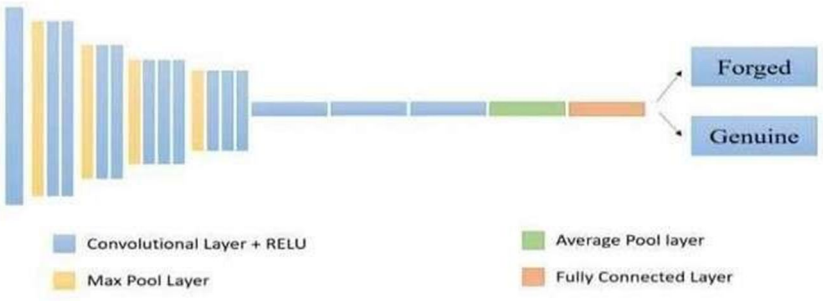



Fig. 13 Mobile Net Architecture

As a result, the CASIA V1.0 dataset is used to create a deep learning-based technique for detecting image splicing. Optimizing the data for model training involves applying preprocessing techniques like enhancing and resizing. The deep learning model's success in identifying spliced images is evaluated using important evaluation measures, such as accuracy, F1-score, and recall, during the 80-epoch training phase.

The sample of metrics score attained in the training phase for the first 10 epochs is detailed in Figure 13

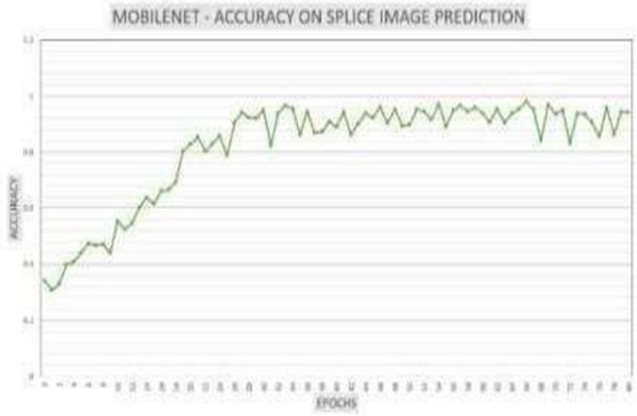




Fig. 14 F1 Score plot of MobileNet Fig. 15 Accuracy plot of MobileNet

It appears from all of figures 11, 12, and 14 that the DL model can recognize the faked image. Thus, the MobileNet architecture has been finalized, and the model has been tested.

Figure 15 displays the MobileNet's results. The model will have an accuracy of 0.9553, an F1-score of 0.96271, and a recall score of 0.9514. following the model's total data testing. Each image is predicted independently by the model.

| Epoch | F1 Score | Accuracy | Recall |
|---|---|---|---|
| 0 | 0.200479 | 0.341898 | 0.329642 |
| 1 | 0.433931 | 0.307594 | 0.456227 |
| 2 | 0.559049 | 0.329657 | 0.425686 |
| 3 | 0.407383 | 0.3992 | 0.441641 |
| 4 | 0.497467 | 0.408379 | 0.450413 |
| 5 | 0.475148 | 0.440113 | 0.501131 |
| 6 | 0.551245 | 0.473335 | 0.514517 |
| 7 | 0.538045 | 0.466125 | 0.531037 |
| 8 | 0.559736 | 0.47123 | 0.553519 |
| 9 | 0.681787 | 0.440285 | 0.579688 |
| 10 | 0.614478 | 0.552713 | 0.588992 |

Fig. 16 DL Model Evaluation for Splice Image Detection

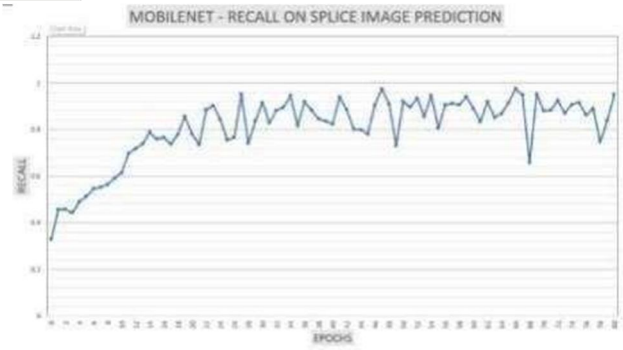




Fig. 17 Recall Plot of MobileNet Fig. 18 Test Performance of MobileNe

The difficulty of identifying picture splicing forgeries stems from the intricacy of the editing methods utilized by the criminals, like morphing and blending. Advanced detection algorithms' real-time effectiveness may be constrained by their computational cost, particularly when dealing with high-resolution photos. These algorithms are constantly vulnerable to adversarial attacks, necessitating adaptable defenses. It can be difficult to compile representative and diverse datasets for training, which affects the creation and assessment of detection algorithms. Maintaining a balance between false positives and negatives is still a common problem and is essential for practical use. Complexity is increased by variation in image information, such as variations in illumination and compression, and maintaining generality over a range of settingsisa continuous goal. Furthermore, the pursuit of efficient forgerydetection gives rise to privacy problems, which makes ethical considerations necessary for algorithm development and implementation.

## III. IN RESPONSE TO THESE CHALLENGES, WE CONDUCTED LITERATURE SURVEY

### *A. Detection of Medical image tampering using CNN*

S.K. Kabilesh et al, study **[2]** emphasizes the need of reliable and trustworthy healthcare and stresses the need of accurate identification of medical picture forgeries. With over 90% accuracy in copy-move identification and an astounding 99% accuracy in spliced image detection, the CNN-based model performs well. The outcome is the development of a deep learning-based technique for detecting image splicing using the CASIA V1.0 dataset.

This healthcare system employs a Modified Convolutional Neural Network (CNN) for medical image forgery detection, ensuring the integrity of healthcare-related images. The approach involves decomposing images, applying Wiener filtering, and extracting noise patterns to identify potential forgeries. Leveraging multi-resolution regression filtering and classifiers, the system operates in an edge-cloud architecture, achieving real-time efficiency with an 84.3% success rate based on database evaluation.

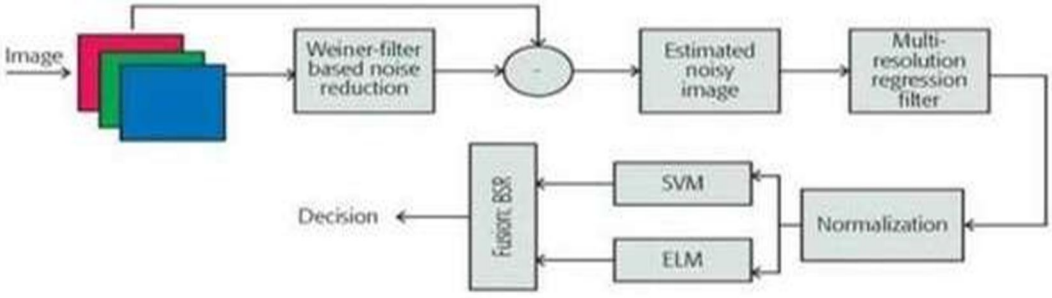



Fig. 19 Proposed Methodology in the paper [2]

The results show how effective the system with Extreme Learning Machine (ELM) as a classifier is; on two different databases, the system achieved remarkable accuracy rates of 97.4% and 98.2%. In addition, the combination of ELM and Bayesian Sum Rule (BSR) with Support Vector Machine (SVM) provided better results than other setups, with the databases' best accuracy levels of 98.8% and 98.9% achieved by the combination. These findings highlight how well the suggested method works to distinguish real from changed photos, especially when combined with a classifier technique. We can infer from the results above that the recommended approach was effective in identifying if a picture was made up or not. The suggested method produced excellent accuracy when using the database. It is more precise than alternative techniques.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

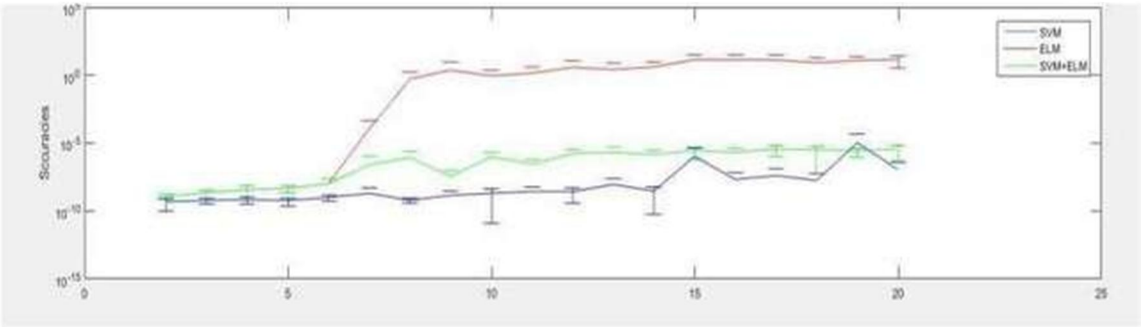



Fig. 20 Results of the Comparison [2]

Sajid Habib Gill et al **[4]**, introduced a model employing CNN and ELA for detecting medical data forgery, showcasing its efficacy with a 92% accuracy on the COVID-19 dataset. The proposed model addresses the increasing concerns around digital data manipulation in healthcare, offering a valuable tool for ensuring trust and accuracy in medical records.

The study employs a five-phase approach, utilizing CNN to classify forged and non-forged COVID-19 images based on histogram data, achieving a state-of-the-art accuracy of 92%. The method involves dataset preprocessing, histogram preparation, CSV file construction, CNN classification, and iterative fine-tuning for optimal performance.

The open-source website Github.com provided the dataset that was used to train and evaluate the model. It included chest X-ray data, mostly in its original form, from a number of COVID-19-positive individuals. There were a total of 544 photographs in the dataset; 400 were used for training (200 of which were original and 200 of which were tampered with), and the remaining 144 were used for testing.

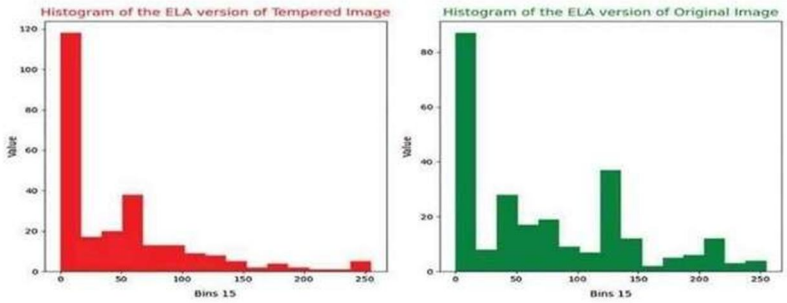



Fig. 21 Histogram of Tampered and Original image [4]

The study significantly enhanced CNN accuracy from 71% to 92% by optimizing the model through noise removal, layer adjustments, activation function tuning, and selecting an optimal optimizer with a learning rate of 0.005. The resulting stable and high accuracy indicates the effectiveness of the refined CNN model

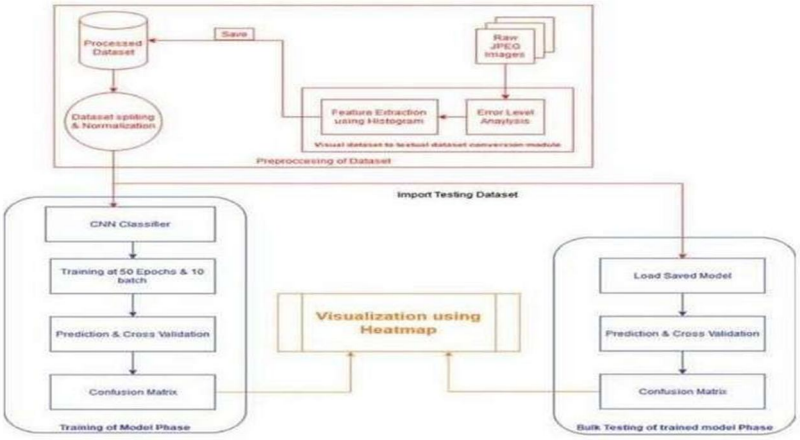



Fig. 22 Block Diagram of Proposed System [4]

*B. Image Tampering Detection in Smart HealthCare*

The term "smart health" (s-health) was first used by A. Solanas et al. [19] in their study, which examined how electronic and mobile health services intersect with smart city settings. The widespread use of information and communication technologies (ICT) in urban settings is responsible for the rise of smart cities, and the combination of ICT and mobile technologies in the healthcare industry has led to the development of electronic health services and ubiquitous patient monitoring.The authors introduce s-health, a novel idea that aims to combine electronic and mobile health services with smart city integration, in recognition of the need for a unified framework. The paper establishes the foundation for targeted research, addressing obstacles, and foreseeing countless opportunities for the advancement of healthcare in the future by defining the scope of s-health.

The concept of S-health, which was presented in this talk, goes beyond M-Health (mobile health) to include smart city sensing. Although both ideas share health technology, there are some significant distinctions between them. Patient data serves as the main information source in mobile health, with a constant focus on the user. However, by combining data from a second, independent source—the sensing infrastructure of a smart city—s-health goes beyond patient-generated data.This distinction modifies information flows in addition to expanding the sources of information. In contrast to m-health, which is focused on individualized user-centric data exchange, s-health addresses both user- and city-centric issues. The integration of smart city data impacts not just personal health results but also more general urban behavioural changes. One example is when ambulances arrive on time by modifying traffic lights, which goes above and beyond what can be done with conventional mobile health interventions.

While edge computing and the Internet of Things enable Smart Healthcare Systems (SHS) to provide enhanced security, flexibility, and efficiency, V. Srilakshmi [7] highlights the susceptibility of system integrity to image fraud. Extreme Learning Machines (ELM) and Support Vector Machines (SVM) are two methods used in a suggested model for image forgery detection to address this problem. The findings are aggregated using the Bayesian Sum Rule (BSR). By incorporating this model into SHS, security is improved, system vulnerabilities are decreased, and the integrity of vital medical images used in treatment operations is guaranteed.

It contains various steps such as noise pattern identification, multi-regression filter, and classifiers. This is shown in the following six steps:

1) *Step 1:* To create the red, green, and blue components, convert the raw image.
2) *Step 2:* For every component, apply a different Weiner filter.
3) *Step 3:* Subtract filtered image from raw image to obtain noise pattern.
4) *Step 4:* By applying a multi-regression filter to process the noise pattern, weights depending on image intensity are provided.
5) *Step 5:* Feed the weighted output through different kernels into SVM and ELM classifiers. Step 6:To get the final result, combine the classifier scores using the Bayesian sum algorithm.

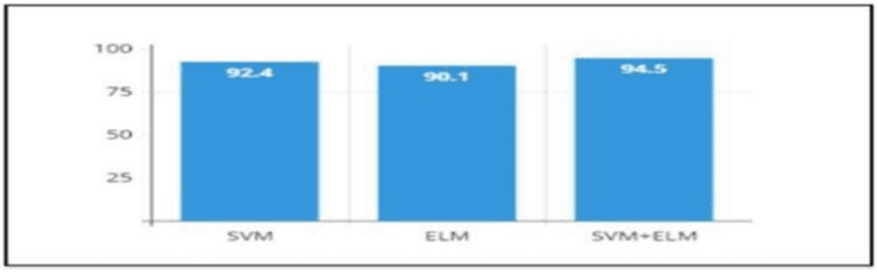



Fig. 23 Accuracy with 80% training data

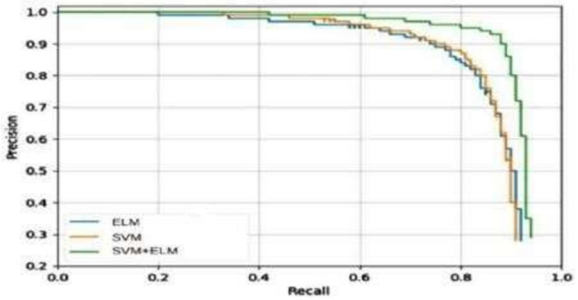



Fig. 24 Precision vs Recall curve

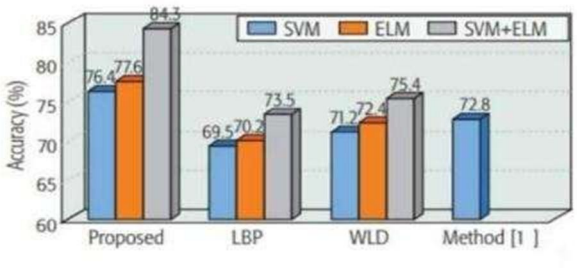



Fig. 25 Comparison of accuracy

The results show that the hybrid model, which combines SVM and ELM, detects photo forgeries with a higher accuracy of 94.5% than the individual accuracies of SVM (92.4%) and ELM (90.1%). The proposed method, which makes use of core cloud resources as well as edge computing, is adaptable to a range of use cases. Its ability to successfully classify forged and unforged photographs serves as an example of this, demonstrating the synergy between edge computing empowerment and the potency of the SVM-ELM combination.

*C. Other Approaches Related to Medical Image Forgery Detection*

Rithin Krishna Dilipkumar [10] highlighted the need for strong cybersecurity measures in the context of medical picture forgeries and the possible repercussions of incorrect diagnoses and unethical practices in his study. This worry stems fromthe fact that medical professionals are not required by law to verify the authenticity of medical photos, which emphasizes the significance of precise detection methods.

The main objective of the study is to provide a trustworthy approach for identifying changed medical photographs. The goal of this project is to reduce the possibility of false positives and stop any abuse, which could have serious consequences for the healthcare sector.

An effective method for categorizing CT scan pictures using machine learning and deep learning—more specifically, the Random Forest and ResNet50 algorithms—is described in Samir Elmuogy's 2021 paper. In order to demonstrate a thorough methodology for medical image forgery detection, the research entails opening a Jupyter Notebook via PyCharm, loading a dataset of human lung CT scans, standardizing image scales, defining and training Random Forest and ResNet-50 models, specifying the Rectified-Adam optimizer, and iteratively testing and training until the desired accuracy is achieved.

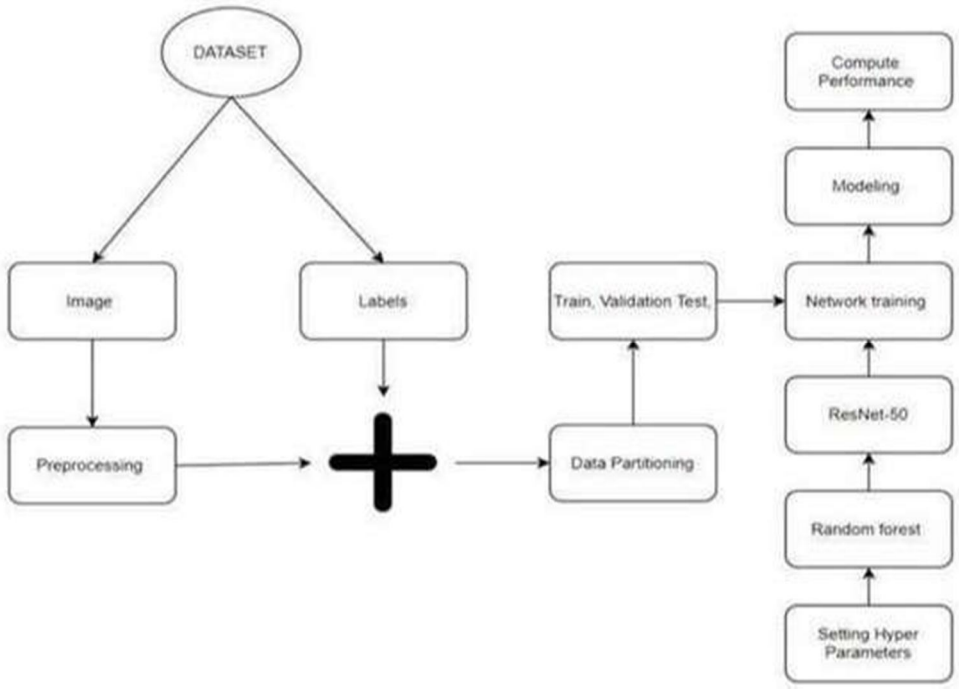



Fig. 26 Implementation of random forest and ResNet50 in medical image forgery

The project's outcomes demonstrate ResNet50's superior efficacy over Random Forest in detecting forged medical images, as evidenced by 100% accuracy for ResNet50 compared to 48% for Random Forest, aligning with the study's goals and yielding a satisfactory conclusion

V. Kalpana et al, **[11]** put a light on the increasing problem of digital picture counterfeiting is addressed in this work, with an emphasis on creating efficient classifiers and algorithms. The suggested method uses a novel segmentation strategy for identifying fake photos by using the Ncut segmentation technique and feature extraction via Kernel Principal Component Analysis (KPCA). Medical pictures from MRIs, x-rays, and microscopic modalities are used in the evaluation. The KPCA image forgery detection approach performs better than DL-based and SF-based Forgery Detection (FD) in terms of precision, accuracy, recall, and specificity The study makes suggestions for possible uses of various image forgeries in upcoming system upgrades.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538*
*Volume 12 Issue III Mar 2024- Available at www.ijraset.com*

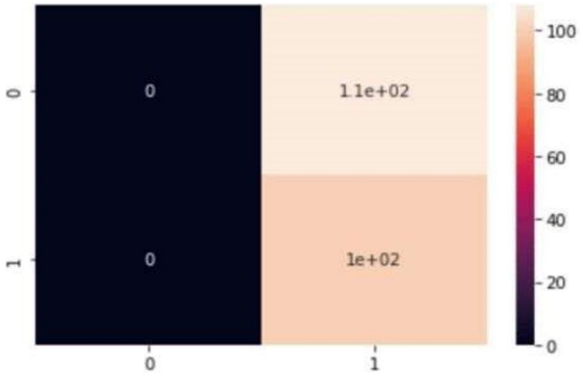



Fig. 27 Confusion matrix of random forest algorithm

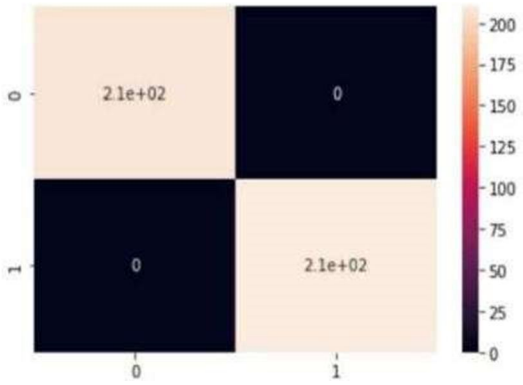



Fig. 28 Confusion matrix of ResNet50

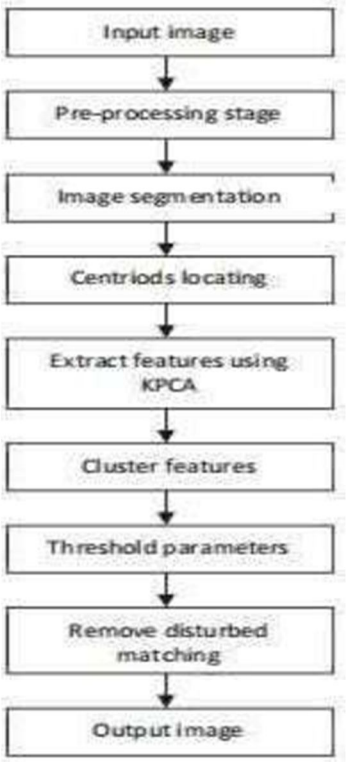



Fig. 29:Framework of Image Forgery Detection

Figure 31 shows the framework for the effective segmentation technique in Kernel Principal Component Analysis (KPCA) image forgery detection. The procedure starts with pre-processing the input image and then segments the forged image using the NCut segmentation algorithm. The centroids of each region are then found, and KPCA is used to extract features. Next, related features are clustered using K-Mean clustering, and feature pair matching is evaluated.Unmatched pairs display copied regions, and false matches are eliminated according to preset criteria. This technique effectively identifies recurring regions in the fabricated image. The ensuing subsections go into detail about each step, which includes pre-processing, segmentation, feature extraction, clustering, and matching.

Unmatched pairs display copied regions, and false matches are eliminated according to preset criteria. This technique effectively identifies recurring regions in the fabricated image. All images undergo forgery through image processing algorithms and are then tested using the proposed system. The primary objective is forgery detection while enhancing computation time, accuracy, precision, recall rate, and specificity of the algorithm. The method demonstrates accurate identification of region duplication forgery. Sample images utilized in the evaluation are illustrated in Figure 32.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

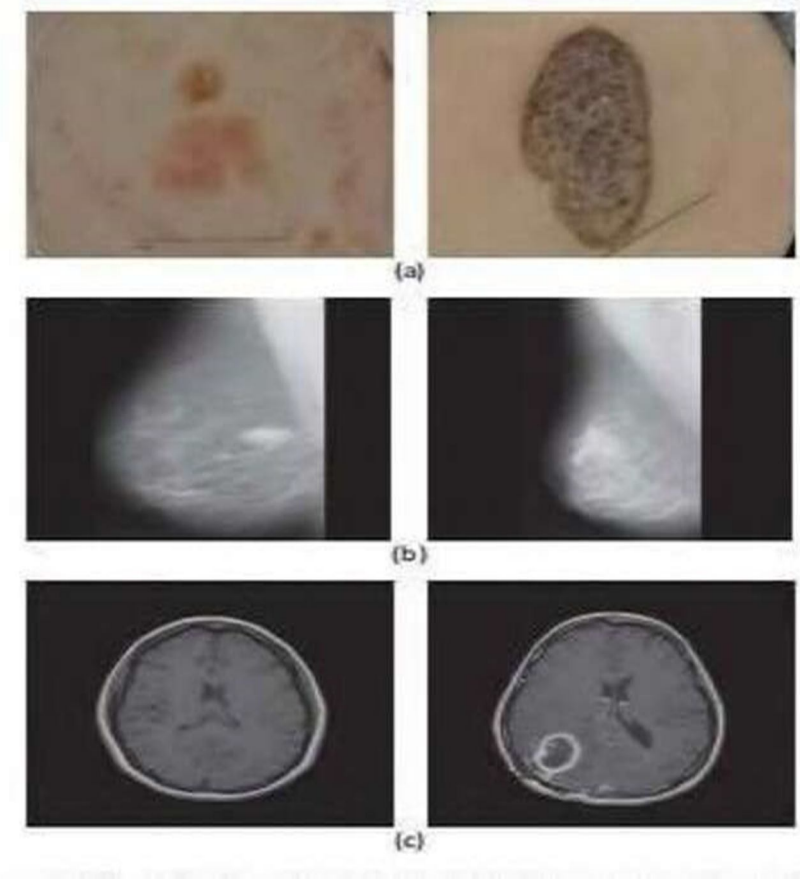



Fig. 30 (a) Derm7pt skin images (b) MIAS Mamo-gram (c) MRI Brain images

A systematic literature review (SLR) was carried out by M. S. Rana et al. [16] to look into the most recent techniques for identifying Deep Fake across 112 studies from 2018 to 2020. The paper emphasizes how convolutional neural networks (CNN), in particular, are widely used in deep learning for Deep Fake identification. The FF++ dataset is used extensively in the experiments, and detection accuracy is the main performance parameter.

The outcomes demonstrate the effectiveness of deep learning methods, since CNN models typically outperform their nondeep learning equivalents. Although there has been progress, the assessment notes that Deep Fake detection remains challenging given the speed at which multimedia technology is developing. It seeks to serve as an important tool for the scientific community, encouraging the creation of reliable detection techniques and defenses.

The methodologies suggested in software engineering by Budgen et al. and Zlatko Stapic et al. are followed in this systematic literature review (SLR). The review procedure is divided into three steps: planning the review, conducting the review, and reporting the review. The emphasis in the Planning stage is on identifying the need, developing criteria and procedures, and evaluating them.

The defining of research questions, creating a search strategy, establishing study selection and quality assessment criteria, extracting and monitoring data, and finally synthesizing data are all steps that are carried out during the Conducting stage. The guiding concepts for these actions come from earlier research. The final Reporting stage entails presenting the findings in a format suitable for distribution to the intended audience. This methodical approach ensures a thorough and unbiased examination of Deep Fake detection research.

| | | Actual | |
|---|---|---|---|
| | | **Positive** | **Negative** |
| Prediction | Positive | True Positive (TP) | False Positive (FP) |
| | Negative | False Negative (FN) | True Negative (TN) |

Fig.31 .Confusion Matrix

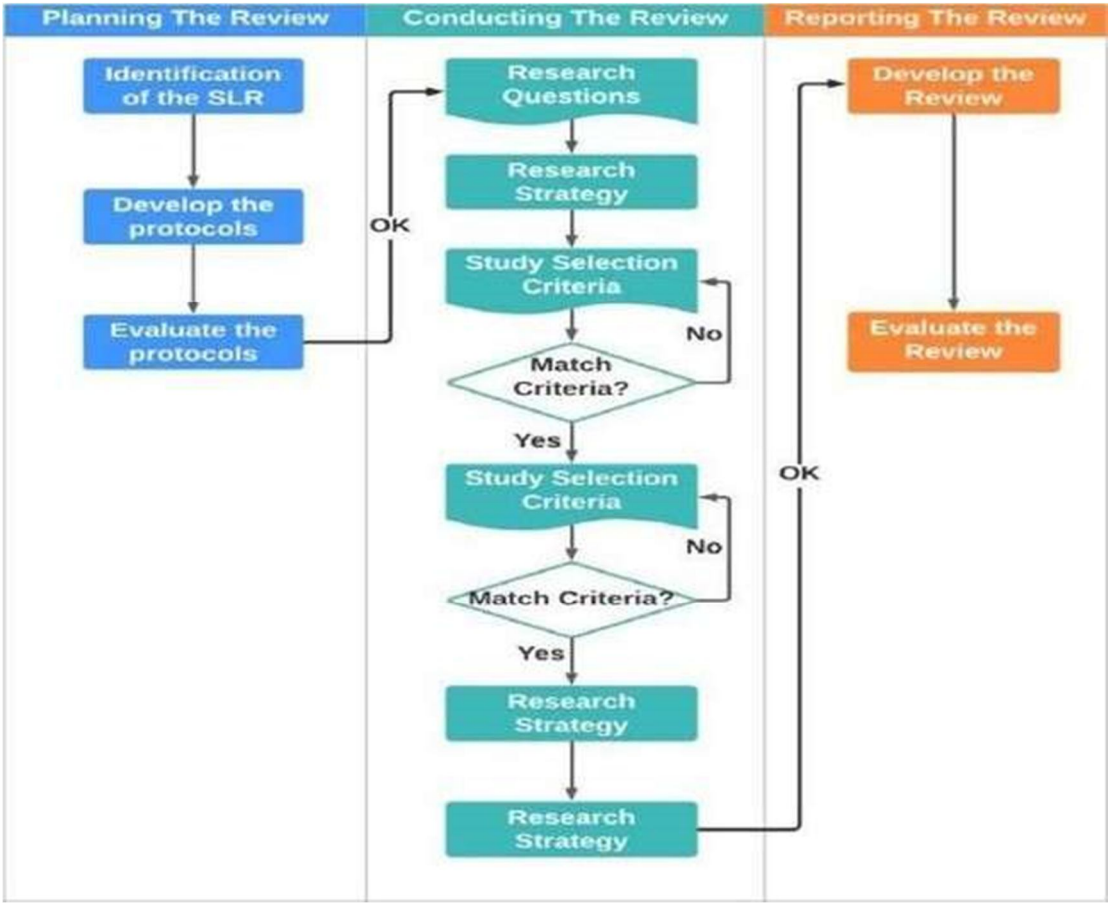



Fig.31 The process of the SLR

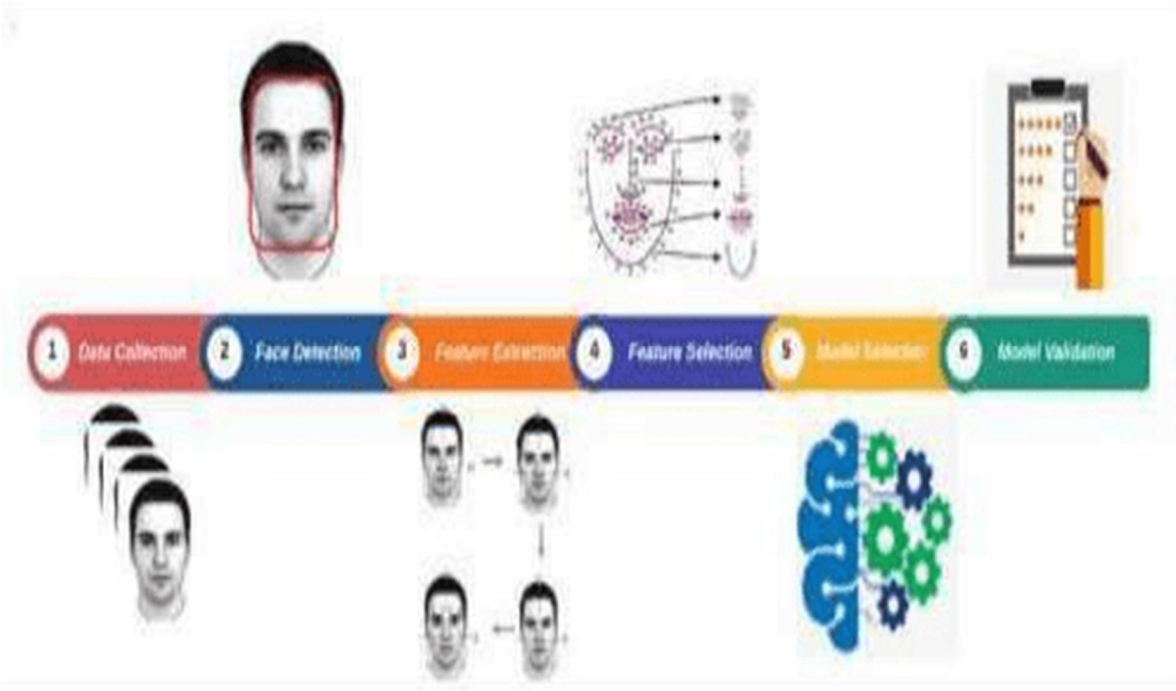



Fig.33.Steps of Deep fake detection.

## IV. LITERATURE SURVEY

| S.NO | AUTHORS | Methodology | Datasets Used | Challenges |
|---|---|---|---|---|
| 1 | Nan Wang, Liping Yi, Gang Wang and Xiaoguang Liu[12] | By incorporating memory-enhanced attention mechanisms into the U-Net architecture, this paper showcases promising results in accurately localizing image manipulations. | Since there is no medical image forgery dataset publicly available, by using the copy-move and splicing forgery operations, manually tampered and annotated two forged medical image datasets: OIAT (eye) and COVIDLT (lung) to verify the generality of the proposed model. | Data Quality and Availability,Forgery Techniques,Complexity of Medical Images,Interpretable Algorithms,Computational Resources,Generalization,Ethical Considerations,Real-Time Application,robustness to Variations,Evaluation Metrics |
| 2 | N Krishnamoorthy, C. Amruthadevi, M. K. Geetha, Poli Lokeshwara Reddy, Anitha Rani K , and R.Gopinathan.[15] | By leveraging deep learning techniques, this paper addresses the challenging task of detecting splicing-based image forgeries through Deep learning | "The study used a Deep Learning (DL) model named MobileNet to distinguish between authentic and manipulated images. Both the training and testing of the DL model make use of the CASIA data." | Data Diversity,Forgery Variability,Data Annotation,Generalization,Complexity of Deep Learning Models,Adversarial Attacks,Large-Scale Deployment,False Positives,Interpretability,Data Privacy and Ethics,Real-World Noise and Artifacts,Evaluation Metrics |
| 3 | Ahmed Ghoneim, Ghulam Muhammad, Syed Umar Amin, and Brij Gupta.[9] | By addressing the specific challenges posed by medical image manipulation, the research underscores the importance of trustworthy data for informed medical decision | "Two publicly available image databases for the experiments. These databases are CASIA 1 and CASIA 2. Both databases consist of authentic and forged images. The CASIA 1 database contains 800 authentic and 921 forged images.Another database where the images are mammograms. The database is the Digital Database for Screening Mammography (DDSM) . There are more than 2000 mammograms in the database, and the cancer regions are annotated by expert radiologists. " | Data Privacy and Ethics,Data Availability,Forgery Techniques,Subtle Alterations,Lack of Ground Truth Label,Generalization,Interpretable Models,Real-Time Application,Adversarial Attacks,Imbalanced Datasets,Computation and Resource Constraints,Integration with Healthcare Systems,Validation and Clinical Trials |
| 4 | V. Srikanthi, D Purushotham, Chinta Abhinav, Nikhil Godalla , and S. V. Varshith[7] | By incorporating a hybrid approach, this research effectively addresses the critical issue of detecting image forgeries within the context of smart healthcare systems | "The dataset is obtained from the "Kaggle" website for training and testing and then is split into train and test data. The whole dataset is located in a directory, which contains all the data in the form of image files. In the data set, there exist 3000 images of which 2551 are forged and 500 are non-forged. It contains various steps such as noise pattern identification, multi-regression filter, and classifiers." | Data Privacy and Ethics,Data Availability,Complexity of Medical Images,Forgery Techniques,Intermodal Integration,Model Interpretability,Generalization,Real-Time Application,Adversarial Attacks,Computation and Resource Constraints,Imbalanced Datasets,Integration with Healthcare Systems,Integration with Healthcare Systems,Human Expertise |
| 5 | Muhammad Qadir, Samabia Tehsin , and Sumaira Kausar[3] | By applying deep neural networks, the study offers a robust and automated method for identifying instances of copy-move forgery, a critical issue in medical image integrity | "A database of 100 images from the dataset by the University of Columbia was composed by Davarzani et al and Columbia color, CASIA 1, and CASIA 2. " | Data Availability,Forgery Realism,Scale and Rotation Variations,Large Image Sizes,Complex Anatomy and Structures,Interpretable Results,Generalization,Imbalanced Datasets,False Positives,Data Privacy and Ethical Concerns,Adversarial Attacks,Validation and Clinical Impact,Integration with Healthcare Systems,Limited Annotated Data |
| 6 | Chi-Man Pun, Senior Member, IEEE, Xiao-Chen Yuan, Member, IEEE, and Xiu-Li Bi[8] | By utilizing over-segmentation and feature point matching techniques, this research provides an effective and robust method for identifying imageaberations. | "This dataset is formed based on 48 high-resolution uncompressed PNG true color images, and the average size of the images is 1500 1500. In the dataset, the copied regions are from the categories of living, nature, man-made and mixed, and they range from overly smooth to highly textured; the copy-move forgeries are created by copying, scaling and rotating semantically meaningful image regions. In summary, the dataset has 1826 images in total, which are realistic copy-move forgeries." | Data Diversity,Forgery Realism,Adaptive Over-Segmentation,Feature Point Extraction and Matching,False Positives,Generalization,Real-Time Processing,Large Image Sizes,Data Annotation,Interpretability,Ethical Considerations,Evaluation Metrics,Security and Adversarial Attacks |
| 7 | Sirisha Gudla ,huvan Sai Teja Gabbita ,Nirupama Chaganti ,Srinivas Boddepally ,Mayur Raj Singh Biasthakur[5] | This research addresses a critical need for healthcare security by proposing a noise map-based system for detecting medical image forgery, utilizing advanced technologies like edge and cloud computing. | The dataset contains a diverse range of image modalities, such as X-rays, CT scans, and MRI scans | Data Diversity,Forgery Realism,Variability in Imaging Modalities,Clinical Significance,Scale and Resolution,Imbalanced Data,Data Annotation,Interpretability,Generalization,Real-Time Detection,Adversarial Attacks,Ethical and Regulatory Compliance,Validation and Clinical Impact,Integration with Healthcare Systems |

| | | | | |
|---|---|---|---|---|
| 8 | S.K. Kabilesh, D. Divya, C. Blessy Vinolin, D. Priyadharshini, S. Saravanakumar[2] | By Addressing the growing concern of image counterfeiting in healthcare, this approach contributes significantly to enhancing security in smart healthcare systems and ensuring accurate diagnostics. | Customised Dataset | Data Diversity,Data Privacy and Ethical Concerns,Duplicate Definition,Scale and Resolution Variability,Data Annotation,False Positives,Clinical Significance,Real-Time Detection,Integration with Healthcare Systems,Generalization,Adversarial Attacks,Interpretability,Regulatory Compliance |
| 9 | Shivani Pakala, Pravallika Mantri, Madhuri Badri, Dr. M. Naresh Kumar[13] | By incorporating segmentation techniques, it not only identifies forgeries but also enhances compromised medical images, contributing to the accuracy of diagnoses within a smart healthcare framework. | "A Dataset is an organized set of data which is saved digitally in a computer system. The work uses two databases for this. They are known as CASIA 1 and CASIA 2. There are real and fake photographs in both databases. There are 800 real photos in the CASIA 1 database and 921 fakes. " | Data Privacy and Ethical Concerns,Data Availability,Forgery Techniques,Subtle Alterations,Interpretability,Image Enhancement,Generalization,Real-Time Processing,Adversarial Attacks,Integration with Healthcare Systems,Regulatory Compliance,Validation and Clinical Impact,Data Annotation |
| 10 | Sajid Gill ,Semina Rajper ,Noor Zaman Jhanjhi[4] | By focusing on error level analysis (ELA) and identifying anomalies indicative of data tampering, this approach offers a robust solution to safeguard the integrity of critical medical information. | The effectiveness of the proposed scheme was evaluated on the basis of six benchmark datasets, i.e., DVMM, CASIA v2.0, Columbia CASIA v1.0, IFS-TC, and DSO-1 datasets. | Data Privacy and Ethical Concerns,Data Availability,Forgery Techniques,Subtle Alterations,Interpretability,Generalization,Real-Time Processing,Adversarial Attacks,Integration with Healthcare Systems,Regulatory Compliance,Validation and Clinical Impact,Data Annotation,Model Training |
| 11 | R.F. Olanrewaju, Othman. O. Khalifa, Aisha- Hassan Hashim, Akram M. Zeki and A.A. Aburas[6] | By the ability to maintain perceptual quality while pinpointing modifications makes it highly valuable for applications in medical image authentication, tamper detection, and blind detection, particularly in the context of telemedicine and telediagnosis. | "The details of the breast mammogram taken from different views for screening:<br>i. Cranio-caudal (CC) is taken from above a horizontally compressed breast.<br>ii. Medio Lateral Oblique (MLO) is taken from the side and at an angle of a diagonally compressed breast.<br>" | Data Privacy and Ethical Concerns,Data Availability,Complex-Valued Data Handling,Forgery Techniques,Subtle Alterations,Interpretability,Generalization,Real-Time Processing,Adversarial Attacks,Integration with Healthcare Systems,Regulatory Compliance,Validation and Clinical Impact,Data Annotation,Model Training |

## V. CONCLUSIONS

In conclusion, it is critical that we address the growing threat of adversarial attacks with ever-more-advanced and flexible solutions as we traverse the changing terrain of medical image authentication. Strong approaches that go beyond conventional forgery detection are desperately needed, as the complex interactions between technical developments and the vulnerabilities present in medical image data highlight. In the face of splicing and copy-move attacks, the paper emphasizes how important Deep Learning (DL) is to maintaining the integrity of diagnostic processes.

Investigating state-of-the-art DL-specific forgery detection methods, such as those based on Generative Adversarial Networks (GANs), shows a promising path toward increased precision and robustness. The efficacy of machine learning and deep learning models in protecting the confidentiality of diagnostic data is highlighted by the high confidence levels that have been shown in identifying artificial deformities in medical imaging. Interestingly, deep learning combined with regionof-interest localization is a powerful method to identify subtle abnormalities, especially in tumor injection scans.

These conclusive findings highlight how important it is to secure the accuracy of medical images and highlight how urgent it is to address the numerous issues raised by digital manipulations in the fields of medical diagnosis and treatment planning. The unrelenting advancement of deep learning techniques is a beacon in the quest to strengthen the validity of medical imaging. It shows the way toward a future in which the accuracy of diagnostic data will not falter in the face of changing adversarial threats.

## REFERENCES

[1] Shijo Easow, Dr. L. C. Manikandan.: "A Study on Image Forgery Detection Techniques." International Journal of Computer (IJC), Vol. 33 No. 1 (2019), https://ijcjournal.org/index.php/InternationalJournalOfComputer/article/view/1411

[2] S.K. Kabilesh, D. Divya, C. Blessy Vinolin, D. Priyadharshini, S. Saravanakumar.: "Detection of Duplicate Medical Image using Convolution Neural Network." International Journal of Scientific Research in Science, Engineering and Technology Volume 9 | Issue 12 | May-June 2022, https://ijsrset.com/IJSRSET22912114

[3] Muhammad Qadir, Samabia Tehsin, Sumaira Kausar, "Detection of Copy Move Forgery in Medical Images Using Deep Learning", 2021 International Conference on Artificial Intelligence and Mechatronics Systems (AIMS), pp.1-6, 2021, https://ieeexplore.ieee.org/document/9466005

[4] "Extended forgery detection framework for covid-19 medical data using convolutional neural network," Computers, Materials & Continua, vol. 68, no.3, pp. 3773–3787, 2021, https://www.techscience.com/cmc/v68n3/42466

[5] Sirisha Gudla, Bhuvan Sai Teja Gabbita, Nirupama Chaganti, Srinivas Boddepally, Mayur Raj Singh Biasthakur.: "FORGERY DETECTION OF MEDICAL IMAGE." Journal of Engineering Sciences ICETT- Vol 14 Issue 05(S), pp.11-19, 2023, https://jespublication.com/special-issue.php

[6] 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)." Australian Journal of Basic and Applied Sciences, 5(7), pp. 1251-1264,2011,https://www.researchgate.net/publication/232708501_Forgery_detection_in_medical_images_using_Complex_Valued_Neural_Network_CVNN

[7] V. Srilakshmi, D Purushotham, Chinta Abhinav, Nikhil Godalla, S. V. Varshith.: "Hybrid Model for Image Forgery Detection In Smart Healthcare." International Conference on Computer, Electronics & Electrical Engineering & their Applications (IC2E3), 2023, https://ieeexplore.ieee.org/document/9466005/citations#citations

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

[8] C. -M. Pun, X. -C. Yuan and X. -L. Bi, "Image Forgery Detection Using Adaptive OverSegmentation and Feature Point Matching," in IEEE Transactions on Information Forensics and Security, vol. 10, no. 8, pp. 1705-1716, Aug. 2015, https://ieeexplore.ieee.org/document/7086315

[9] A. Ghoneim, G. Muhammad, S. U. Amin and B. Gupta, "Medical Image Forgery Detection for Smart Healthcare," in IEEE Communications Magazine, vol. 56, no. 4, pp. 33-37, April 2018, https://ieeexplore.ieee.org/document/8337892

[10] Rithin krishna Dilipkumar.: "Medical Image Forgery Detection." Masters thesis, Dublin, National College of Ireland, 2022, https://norma.ncirl.ie/id/eprint/5998

[11] V. Kalpana, M. Jayalakshmi, V. Vijaya Kishore. Medical Image Forgery Detection By A Novel Segmentation Method With KPCA. Cardiometry; Issue 24; November 2022; p.1079-1085; DOI: 10.18137/cardiometry.2022.24.10791085; https://www.cardiometry.net/issues/no24-november2022/medical-image-forgery

[12] N. Wang, L. Yi, G. Wang and X. Liu, "MemAU-Net: Memory-Enhanced Attention U-Net for Medical Image Forgery Localization," 2023 International Joint Conference on Neural Networks (IJCNN), Gold Coast, Australia, 2023, pp. 1-7, https://ieeexplore.ieee.org/document/10191370

[13] Shivani Pakala, Pravalika Mantri, Madhuri Badri, Dr. M. Naresh Kumar.: "Forgery Detection in Medical Image and Enhancement using Modified CLAHE Method." Journal of Survey in Fisheries Sciences, Vol. 10 No. 4S (2023): Special Issue 4, https://sifisheriessciences.com/journal/index.php/journal/article/view/1419

[14] Meena, K.B., Tyagi, V. (2019). "Image Forgery Detection: Survey and Future Directions." In: Shukla, R.K., Agrawal, J., Sharma, S., Singh Tomer, G. (eds) Data, Engineering and Applications. Springer, Singapore. https://doi.org/10.1007/978-981-13-6351-1_14

[15] N. Krishnamoorthy, C. Amuthadevi, M. K. Geedtha, P. L. Reddy, A. R. K. S and R. Gopinathan, "Splicing Image Forgery Detection by Deploying Deep Learning Model,"2022 InternationalConference on Automation, Computing and Renewable Systems (ICACRS), Pudukkottai, India, 2022, pp. 1116-1120, https://ieeexplore.ieee.org/document/10029055

[16] M. S. Rana, M. N. Nobi, B. Murali and A. H. Sung, "Deep fake Detection: A Systematic Literature Review," in IEEE Access, vol. 10, pp. 25494-25513, 2022, https://ieeexplore.ieee.org/document/9721302

[17] S. Teerakanok and T. Uehara, "Copy-Move Forgery Detection: A State-of-the-Art Technical Review and Analysis," in IEEE Access, vol. 7, pp. 40550-40568, 2019, https://ieeexplore.ieee.org/abstract/document/8673945

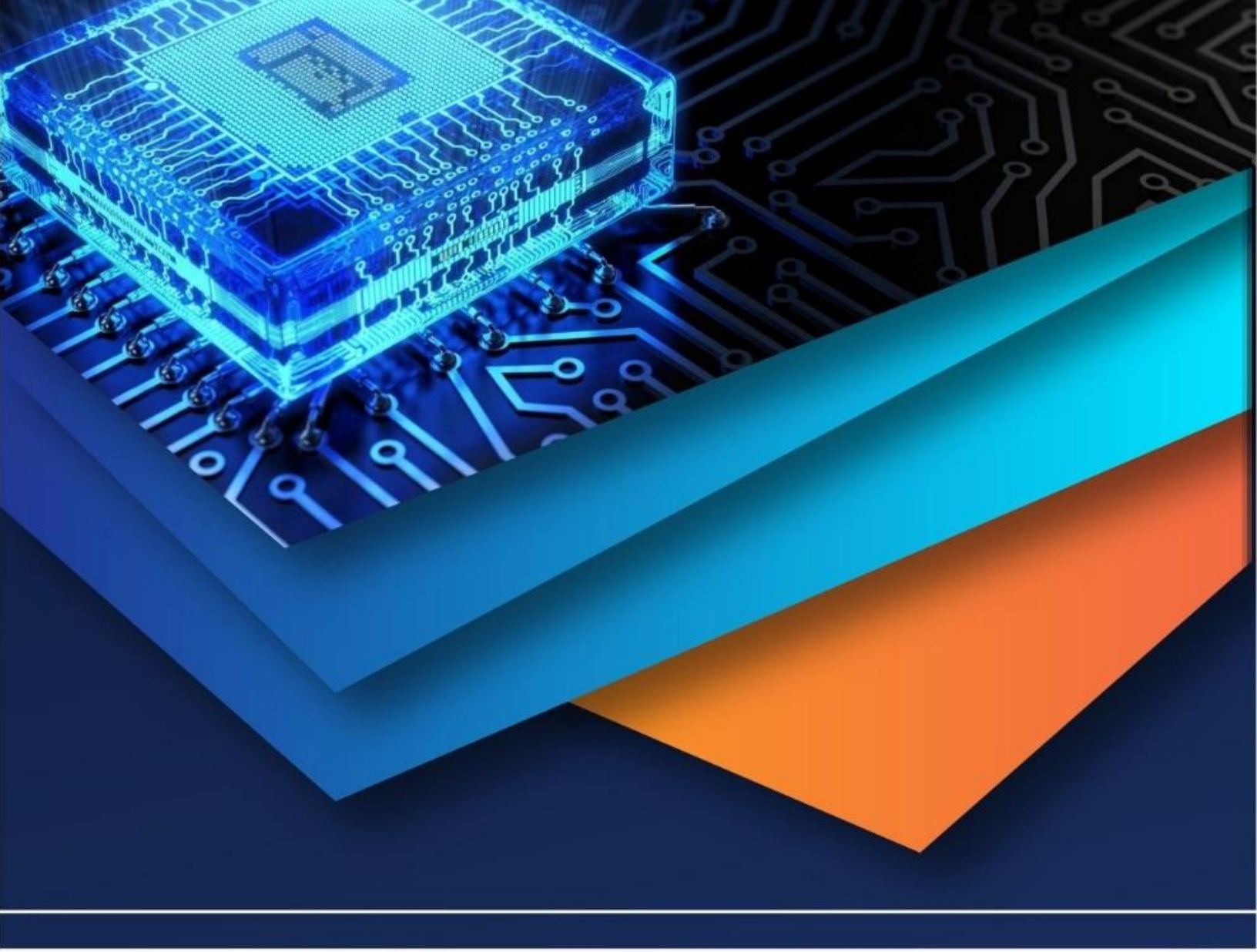
[18] A. B. Z. Abidin, H. B. A. Majid, A. B. A. Samah and H. B. Hashim, "Copy-Move Image Forgery Detection Using Deep Learning Methods: A Review," 2019 6th International Conference on Research and Innovation in Information Systems (ICRIIS), Johor Bahru, Malaysia, 2019, pp. 1-6,https://ieeexplore.ieee.org/document/9073569

[19] A. Solanas et al..:"Smart health: A context-aware health paradigm within smart cities,"in IEEE Communications Magazine, vol. 52, no. 8, pp. 74-81, Aug. 2014, https://ieeexplore.ieee.org/document/6871673

[20] S. Walia and K. Kumar.: "Characterization ofsplicingin digitalimages using grayscale co-occurrence matrices,"2019 Twelfth International Conference on Contemporary Computing (IC3), Noida, India, 2019, pp. 1-6, https://ieeexplore.ieee.org/document/8844881

[21] Yisroel Mirsky, Tom Mahler, Ilan Shelef, Yuval Elovici.: "CT-GAN: Malicious Tampering of 3D Medical Imagery using Deep Learning." 28th USENIX Security Symposium (USENIX Security 19) https://www.usenix.org/conference/usenixsecurity19/presentatio

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)