CC BY

Forgery Detection in Medical Image and Enhancement using Modified CLAHE Method

[1]Shivani Pakala, [2]Pravalika Mantri, [3]Madhuri Badri, [4]Dr. M. Naresh Kumar

[1] ECE, Vardhaman College of Engineering, [2] ECE, Vardhaman College of Engineering, [3] ECE, Vardhaman College of Engineering, [4] ECE, Vardhaman College of Engineering

[1]pakalashivani19@gmail.com, [2]mantripravalika72@gmail.com, [3] bmadhurigoud9@gmail.com, [4]nareshece84@vardhaman.org.

Abstract— Health care system is one of the country's most important and delicate sectors. Our key priorities are security and privacy as the healthcare sector expands. The method of Forgery detection in medical image needs more attention in order to gain patient's trust and reduce the likelihood of providing the wrong medicine. These advancements have the potential to render the healthcare system dependable, safe, and easy to utilize in real-time. The suggested process involves different algorithms like Weber Local Descriptor (WLD), Local Binary Pattern (LBP), Scale-Invariant Feature Transform (SIFT) key points and region information. Invariant features are extracted from a picture using SIFT, and subsequently blocks are extracted using Principal Component Analysis (PCA). The PCA algorithm creates a fresh collection of variables known as principal components. Output images are produced using SVM (Support Vector Machine) and ELM (Extreme Machine Learning). Additionally, segmentation techniques can be utilized to compare and find any forgeries. This approach is a part of smart healthcare framework which can determine whether outsiders or hackers have altered the medical data. If the data has been altered, it will indicate the locations where the data has been falsified and image will then be enhanced using the Contrast Limited Adaptive Histogram Equalization (CLAHE) approach.

Keywords—Medical Image Forgery, Image Enhancement, SIFT, LBP, WLD, PCA, SVM, ELM segmentation, CLAHE method.

I. INTRODUCTION

Healthcare system has developed many technologies in the medical sector. As this field of study is more important to our life, safety is our main concern. The patient's medical information is considerably interpreted by these advanced techniques during the treatment of patient. To enhance people's experience, numerous new features have been invented. Currently, patients can consult doctors without being physically meeting them. This can be possible by health check using different sensors that has an ability to detect diabetes, pulse, voice abnormalities and emotions using various techniques. Although the healthcare industry is expanding, there are still some issues that require addressing to make the medical information more private and safer. For instance, if medical information is stolen or changed, the patient may get improper health status which may lead to false treatment or being mentally affected, while other persons may benefit unfairly. In order to tackle this, a specialized system in a smart healthcare framework that should be able to determine whether hackers or other intruders altered medical data while

it was being transmitted. Moreover, to improve the quality of the health care industry, clinical image forgery detection for innovative medical practices was developed that locates the distorted area of the x-ray image.

Recently many techniques have been equipped to encounter the forgery of medical images. Both intrusive and non-intrusive techniques can be used to determine whether the data have been altered or not. Firstly, in intrusive approach definite information is added to the data while keeping the data undisturbed. The data is initially referred as a watermark. The watermark is then removed from the image and compared with the original watermark of an image if any doubt develops while processing. If they don't line up, the information is seen as counterfeit or altered. In contrast, the data is not given a watermark in the non-intrusive method. For examining any unusual patterns,
certain algorithms are employed to identify any distortion or modification in the input. As, some data may not purposefully or accidentally have watermarks, the intrusive method is occasionally not practical. Since there is no need for a watermark with the non-intrusive method, any data can be checked for changes or fraud.

Image Enhancement is also one of the famous techniques used now-a-days. As medical images are in gray scale form, they are not visible properly and for the individuals who had no idea about medical field will be in total confusion. Image Enhancement makes the medical image improve in terms of brightness, saturation, and clarity of image. Moreover, a CLAHE algorithm is used to enhance the quality of medical image to show the accurate forgered region in the X-ray.

How image is forgered:

- Copy – Move Method:

Image falsification can be a severe problem in the medical industry. In the event that a mammogram is compromised and the hacker utilizes copy-move forgeries to expand the cancerous area, if the diagnosis will be incorrect and the patient will be in grave danger. A healthcare framework with an image forgery detection system can spot the fake before the diagnostic procedure even begins [8].

In this paper, a methodology is developed to detect the forgery in the medical images. Many techniques have been presented to overcome this forgery in images. A comparative analysis is done and finally focused on the forgery that had been done on medical image. The suggested system has shown the accuracies 94.9% and 96.2% with SVM and ELM respectively and with the combined accuracy of 98.3%.

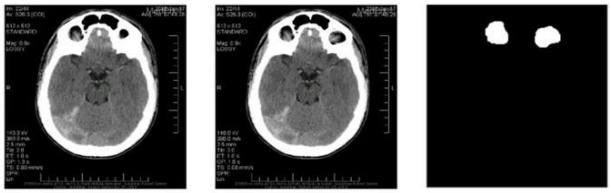

Fig.I.a. Copy Move forgery of brain X-Ray

Fig.I.b. Copy Move forgery of lungs X-Ray

If we analyze existing projects, G. Muhammad has proposed a unique copy move method for image forgery detection that involves Steerable Pyramid Transform (SPT) and Local Binary Pattern (LBP). The drawback of this project is time taking as it uses sub-bands and 2 channels [1]. Patel Purvish Dhaval Kumar has implemented a

deep learning strategy for detecting smart health care fraud using Convolutional Neural Networks (CNN). Here, the author made use of Support Vector Machine (SVM) to complete the final binary classification task with an accuracy of 80% using the retrieved features as input [2]. Deshan Yang has developed the automatic x-ray image contrast en-hancement based on the auto-optimization parameter and CLAHE method. The CLAHE preprocessing stage was employed before the Speeded Up Robust Features (SURF) technique. But it is resistant to copy move forgeries in only tiny areas. D. Warif has proposed a Block-based and key point-based approaches that make up two groups of Copy-Move Forgery Detection (CMFD) techniques. Real-world large data challenges cannot be solved with currently available methods. Techniques for dimension reduction including Principle Component Analysis (PCA), Discrete Wavelet Transform (DVD), and Singular Value Decomposition (SVD) have been proposed to speed up processing. Geometrical trans- forming procedures improve the reliability of keypoint-based algorithms like SIFT and SURF [4]. R.F. Olanrewaju has Proposed detection of forgery in medical image using Complex Valued Neural Networks (CVNN) algorithm. The obtained PSNR is between 46.7 dB to 72 dB. This research proposes a novel method for detecting forgeries in medical watermarked images using CVNN. Complex version of ANN, trained via Complex Back Propagation (CBP) methodology[5]. Farid has categorized five groups that were used to classify the forgery in image detection methods (pixel-based, format-based, camera-based, physically based and geometric- based). While certain forensic algorithms might miss more complex forgeries, other forgery detection methods are far more reliable in catching image faking[6]. Mahdian and Saic B has developed the forgery detection method on bibliography used for blind people. This method used SURF and segmentation algorithms. The major drawback is it requires cameras and a costly setup [7]. Same methodology using updated algorithms are proposed by B. Ansari and Saic [10]. A. Christien and team made use of hash-based copy-move detection algorithm to recognize duplicates [8]. Coming to digital image processing, G. K. Birajdar and V. H. Mankar used passive techniques like bispectrality analysis by the tampering process to detect forgery in digital image [9]. Zang H and his group has done operations on Gamma correction of Image fake detection using Gray level mapping functions and gamma estimation algorithm [11]. A. Shwetha, M. Salami and team has done developments on detection of retouching Para-metric model coefficients using Artificial Neural Network (ANN) [12]. A. Johnson and A. Shafi determined Complex-Valued Parametric Model Coefficients using Artificial Neural Network (ANN) and Complex-Valued Neural Network (CVNN) [13]. Moreover, M. S. Chen, R. Saikia, and A. B. Kandali evolved digital image authentication using Local Binary Pattern (LBP) and Histogram Orientation (HOG). Forgery in digital images like copy-move forgery, leaves little traces of spikes or edges. These subtle spikes or changes are described by the LBP and HOG features that are very sensitive to the shape of objects [14]. Finally, H. Key expanded a survey of forgery techniques and analyzed different methods like copy-move, image slicing, image

retouching, physically based and geometric based techniques [15].

In a nutshell, there are few drawbacks with the presently available technologies. Firstly, all systems require human interpretation and thus cannot be automated. Secondly, being the problem of localizing the forgery. Moreover, problem is of robustness to common image processing operations like blurring, JPEG compression, scaling, and rotation.

II. PROPOSED METHODOLOGY

To identify the image fraud, it have to be operated either at the segment level or at the pixel level. The affinity between the intensities of the pixels in the pixel level procedure determines the texture of the image. Segment level algorithms compare the segments of a picture. Segmenting the image is thought to add additional overhead to the algorithms. Block division of the image is possible in the pixel level. In the literature, image forgery detection is performed using several techniques that work on pixel-level. Among them, LBP is one which is computationally faster but less immune to noise. Another is the Weber local descriptor (WLD), which is computationally more expensive than LBP but less susceptible to noise. Other texture descriptors, such as histogram of gradients, a circular LBP, and a Markov chain, are also employed in the identification of forgeries.

Hence, a unique method is suggested that involves deploying of an image forgery detection system within the scope of smart healthcare. The system is made up of a different number of parts including two classifiers, a multi-resolution regression filter, and noise-pattern extraction.

The system's work flow Fig. III.a is broken down into the following steps:

- Deconstruct the image Fig.V.a & Fig.V.b into its red, green, and blue channels if it is a color image. This step is not necessary if the image is in monochrome. Each color or monochrome element of the image is subjected to the Wiener-filter. This process produces a noise-free image (or component).
- To estimate the image's noise pattern, the original image is subtracted from the noise-free one. The noise pattern is regarded as the image's distinct signature. This fingerprint is warped if any forgery is attempted.
- The noise pattern is set as input to the multi-resolution regression filter. The filter utilizes the specific notations, weight 1 is assigned for the nearby eight-pixel locations, following set of surrounding pixels are considered as weight 2 and the next as weight 3 respectively. The relative intensity of a central pixel is what this filter is particularly good at capturing. The final weight is normalized between 0 and 255 to preserve the grayscale image's Fig.IV.a & Fig.IV.b intensity level.

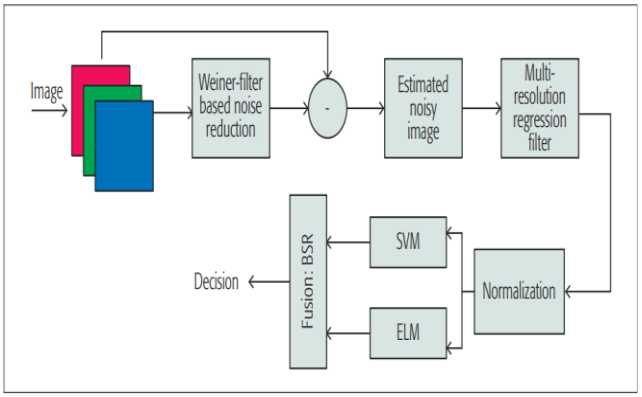

Fig.III.a. Block diagram of the proposed methodology

- The SVM classifier and the ELM classifier both receive

input from the filter's output Fig.V.c & Fig.V.d. Further, the output is analyzed through the linear, polynomial, and Radial Basis Function kernels (RBF) of SVM. Combination of SVM and ELM image will be obtained in Fig.V.e. The BSR is used to combine the SVM and ELM results, which gives output as merged image Fig.V.f. Based on the rate of BSR decision is made Fig. V. g

The image is further processed by an image enhancement technique which is based on the CLAHE model. Its primary objective is to do away with the use of contrast dye in MRI scan procedures. Although Histogram Equalization (HE) is a recognized technique, it is unsuccessful when the contrast is unevenly distributed throughout the image. The alternative to this limitation is to map each pixel produced by the histogram. CLAHE is yet another acceptable method. It eliminates over-enhancing of noise and lessens the sting shadowing effect of limitless AHE by reducing enhancement in highly uniform parts of the image. After employing AHE and CLAHE to enhance the image, the contrast of their attributes is carried out [3]. To facilitate proper patient's everyday treatment arrangement and afterwards the offline review, tissue contrast must be produced that is optimized for each treatment location. The cutting-edge technique that involves the 2D x-ray images are processed through a noise reduction filter, a high pass filter and later through a CLAHE filter to enhance the image.

An effort less and computationally light technique is extensively used for the enhancement of images called as Histogram Equalization. A Contrast Limited Adaptive Histogram Equalization (CLAHE) is utilized for improving the grey scale image [15].

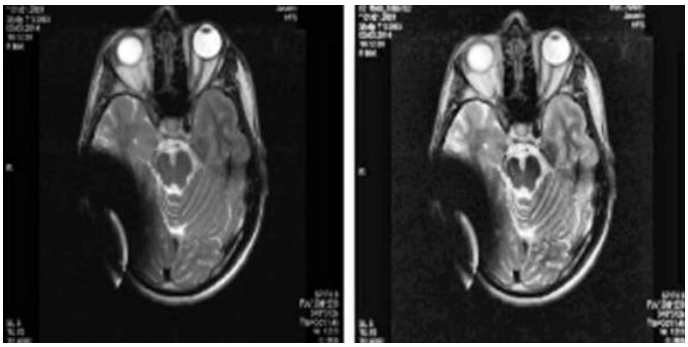

Fig. II.b.Enhanced brain X-Ray

III. DATASETS

A Dataset is an organized set of data which is saved digitally in a computer system. Our 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. Through copy-move and slicing, the images are fabricated. The copy-move technique is used to counterfeit about half of the photos. The photos are 384 x 256 pixels in size and saved in the JPEG format. In the CASIA 2 database, there are 5000 fake photos and more than 7400 real ones. JPEG, TIFF, or BMP are the three picture formats available. The image sizes are not set in stone. Before pasting, the copied object is subjected to several geometric modifications in both databases, including rotation, scaling, and flipping. These two dataset images have nothing to do with medicine, but we used the images in the tests to verify the correctness of the suggested approach. Another database of mammography images is used in the process. The database contains the Digital Mammography screening dataset (DDSM). The database has more than 2000 mammograms, and renowned radiologists

have marked the cancerous spots on each image. The pictures are all in grayscale.

All of the photos were subjected to copy-move forgery. The pasted regions and copied portions were chosen at random. The duplicated pieces are rotated at various angles before being pasted.

IV. TRAINING DETAILS

A CT scan image and MRT scan image are considered as the first and second input images for the proposed methodology. When the input fig IV. a is given to all the blocks, first output will be sufficient texture pattern of two input images. Then, SVM and ELM of the images evolved where image enhancement takes place using Modified Contrast Limited Adaptive Histogram Equalization (CLAHE) Method. After all these steps final output will be obtained that is fusion image using Basic Statistical Return (BSR). Decision image is obtained where the final decision of forgery is made.

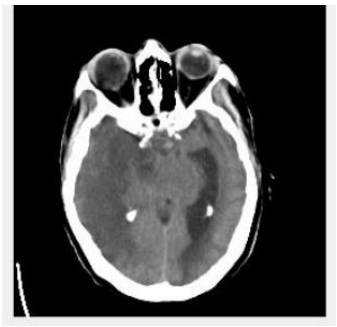

Fig.IV.a. CT scan (First image)

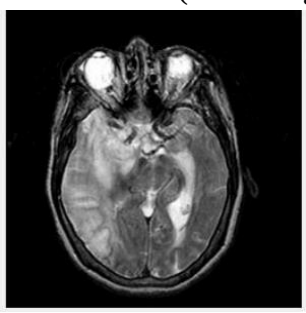

Fig. IV. b. MRT scan (Second image)

V. OUTPUT OF BRAIN X-RAY IMAGE

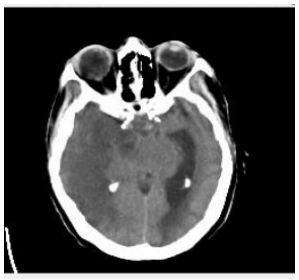

Fig.V.a. Sufficient texture pattern of first image

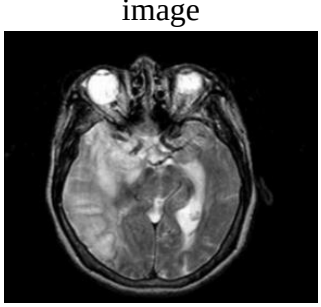

Fig.V. b. Sufficient texture pattern of second image

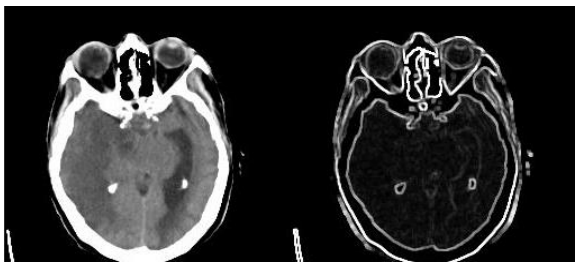

Fig.V.c.SVM of first input

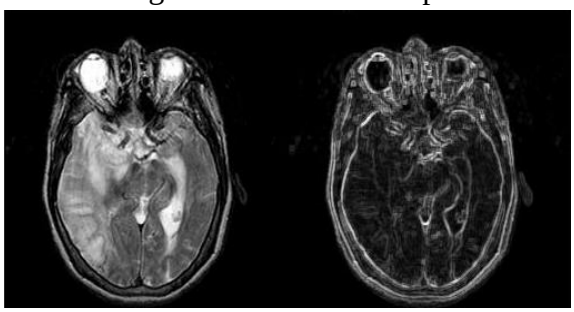

Fig.V. d. ELM of second input

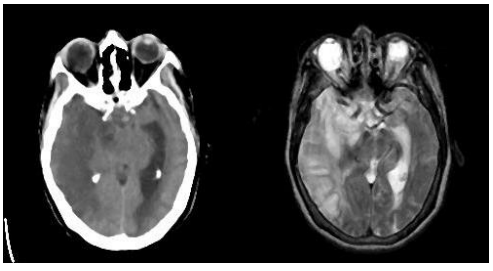

Fig.V. e. ELM+SVM(fusion of first and second image)

Image fusion is the process of combining all the important information

from the given images by enhancing it first to single image.This single image is more informative and accurate compared to the single source images.

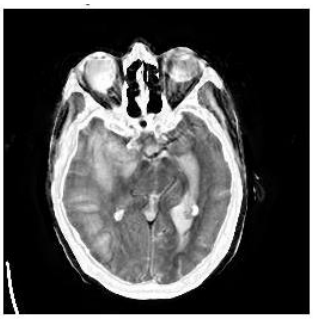

Fig.V.f. Fusion image using BSR

Fig.V. g. Decision image

VI. ACCURACY

The accuracy of the suggested system is shown in the figure below. A comparative study of the accuracies of the proposed system is provided. A system with SVM as its only operation has the maximum accuracy whereas the system with only ELM has very low accuracy. So, to get the better of these variations, a combined system with the union of SVM + ELM is presented. This combination is well agreed with both the natural and medical images giving the mean accuracy of both individually. The proposed system is further compared with existing techniques described in the literature and can infer that the suggested system surpasses them. Practically, the system has shown the accuracies of 94.9 and 96.2 percent for SVM and ELM methodologies respectively. The combined accuracy of the introduced system is 98.3% overcoming the individual systems.

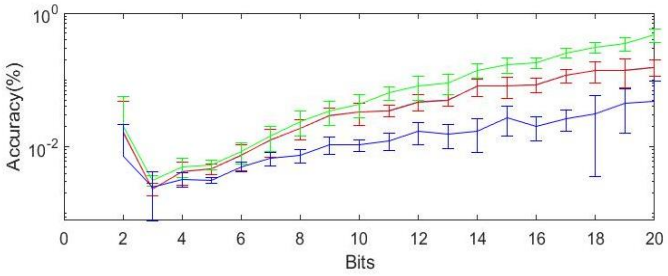

Fig.VI.a. Accuracy of proposed systems

As depicted in the Fig. VI. a. It can be analyzed that the accuracy of the SVM is indicated in red color. Individual ELM accuracy is indicated in blue color. While, combined SVM and ELM methodologies accuracy is indicated in green color

VII. CONCLUSION

Sports, legal services, medical imaging, journalism, surveillance systems, intelligence systems, forensic investigation, and criminal investigation are just a few of the many fields in which images play an impressive role. In the past ten years, significant study has been done in the area of forgery detection. Medical images are different from other types of images because they are very sensitive and provide information on the condition of inside organs that cannot be seen with the naked eye. To earn the trust of patients, the field of medical image forgery detection requires further attention. These technologies can be used to shape the real-time and secure healthcare systems. The project's objectives include protecting patient medical images, identifying fraudulent images, and increasing accuracy. Three separate databases, two with real-world photos and one with mammograms, were used to evaluate the system. The technique worked

best when the results of two classifiers are combined. These new methodologies can be used to create a real-time, dependable, secure, and user-friendly healthcare system. Based on a review of the literature, we identified a few shortcomings that include, accuracy and low PSNR values.

Therefore, to improve the accuracy and simplicity of picture enhancement and applied various techniques such as ORB, Principal Component Analysis (PCA), and Contrast Limited Adaptive Histogram Enhancement (CLAHE).

VIII. REFERENCES

1. G. Muhammad et al. "Image Forgery Detection Using Steerable Pyramid Transform and Local Binary Pattern, Machine Vision and Applications". In: 25.4 (May 2014), 98595.
2. Patel Purvisha DhavalKumar. *Smart healthcare forgery detection using deep learning*. 2019.
3. J. Qiu, Harold Li, Zhang H., Ma T., F., and D. Yang. "Automatic x-ray image contrast enhancement based on parameter auto-optimization". In: *Journal of Applied Clinical Medical Physics* 18.6 (2017).
4. N. B. A. Warif, A. W. A. Wahab, and M.Y. Idris. *I.* : Copy-move forgery detection: survey, chal-lenges and future directions. J. Netw. Comput. Appl, 2016.
5. R. F. *olanrewaju and H*. Haas, forgery detection in medical image using complex valued neural networks (CVNN) algorithm, 2015.
6. H. Farid. ": A survey of image forgery detection techniques". In: *IEEE Signal Process. Mag* 26 (2009).
7. Mahdian, Saic B., and S. ": A bibliography on blind methods for identifying image forgery". In: *SignalProcess. Image Commun* 25 (2010).
8. A. Christien, M. Salami, and A. Shafie. *"Approach to copy-move forgery detection"*. pp: 1, 2010.
9. G. K. Birajdar and V. H. Mankar. ": Digital image forgery detection using passive techniques: asurvey". In: *Digit. Investig* 10 (2013).
10. B. Ansari and S. Saic. ": A bibliography on blind methods for identifying image forgery". In: *SignalProcess. Image Commun* 25 (2009).
11. J. Cao, Harold Li, Zhang H., Ma T., F., and D. Yang. "Detection of Gamma correction of Image forgery detection". In: *Journal of Applied Clinical Medical Physics* 18.6 (2017).
12. A. Shwetha, M. Salami, and A. Shafie. "Detection of retouching Para- metric Model Coefficients Using Artificial Neural Network Technique". 2010.
13. A. Johnson and A. Shafie. "Determination of Complex-Valued Parametric Model Coefficients Using Artificial Neural Network Technique". Advances in Artificial Neural Systems, pp: 1-11, 2010.
14. M. S. Chen, R. Saikia, and A. B. Kandali. Digital Image authentication using Local Binary Patterns (LBP) and Histogram of Oriented Gradients (HOG). 2019.
15. H. kee. ": A survey of image forgery detection techniques". In: *IEEE Signal Process. Mag* 26 (2009).