JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Medical Image Forgery Detection for Smart Healthcare

[1]Pendyala Lakshmi Harika, [2]Peddisetti Ahitha, [3]Lankenapalli Saisree,[4]Pillarisetty Anvika, [5]Mrs. Indla Divya

[1]UG Scholar, [2]UG Scholar, [3]UG Scholar, [4]UG Scholar, [5]Assistant Professor

[1]Electronics and Communication Engineering,
[1]Narayana Engineering College, Nellore, India

Abstract: The main objective behind developing this system is for medical image forgery detection for health care using novel approach called feature descriptor points and feature transform, noise map and multi-resolution regression process. Next generation network technologies such as fifth generation (5G), edge computing, and cloud computing have revolutionized many sectors including the healthcare sector. Recently, the healthcare sector has seen drastic improvement in terms of facilities. Many new features have been added to improve people's satisfaction. People can now consult with doctors without visiting them, check diabetes, heartbeat, voice abnormality, and emotion using various sensors. While the healthcare sector is booming, several aspects need attention to make the healthcare facility more secure and private. With the invention of new communication technologies, new features and facilities are provided in a smart healthcare framework. The features and facilities aim to provide a seamless, easy-to-use, accurate, and real-time healthcare service to clients. As health is a sensitive issue, it should be taken care of with utmost security and caution. This project was proposed a novel approach for medical image forgery detection for health care using noise map and multi-resolution regression process.

IndexTerms - Feature Descriptor Points, Feature Transform, Noise Map, Multi-resolution regression filter

I. INTRODUCTION

Next-generation network technologies such as fifth generation (5G), edge computing, and cloud computing have revolutionized many sectors including the healthcare sector. Recently, the healthcare sector has seen drastic improvement in terms of facilities [1]. Many new features have been added to improve people's satisfaction. People can now consult with doctors without visiting them, check diabetes, heartbeat, voice abnormality, and emotion using various sensors. While the healthcare sector is booming, several aspects need attention to make the healthcare facility more secure and private. For example, if medical data are leaked or altered, the concerned patient may face social embarrassment or let down, while other people may gain an illegal advantage. Therefore, there should be a system in a smart healthcare framework that can check whether the medical data are changed during transmission by hackers or intruders [2]. There are two types of methods to check whether the data are changed or not: intrusive and non-intrusive. In the intrusive method, some information is added to the data in such a way that it does not hamper the message in the data. The information is called a watermark. Later, if any question arises, the watermark is extracted from the data and matched with the original watermark. If they do not match, the data are considered to be forged or changed. In the non-intrusive method, no watermark is added to the data. Some algorithms are used to find any distortion or change in the data by analyzing any abnormal patterns. The intrusive method sometimes is not feasible, because some data may not have watermarks intentionally or unintentionally. As the non-intrusive method does not require any watermark, any data can be verified against change or fraud. There are many non-intrusive techniques proposed in the literature. In this article, we focus on non-intrusive techniques to detect image forgery. A good review on this topic can be found in [3]. Image forgery can be done in many ways, involving one or more images. The most common image forgeries are copy-move forgery and splicing. In copy-move image forgery, one or some parts are copied and pasted into other parts in the same image. This type of forgery is mainly done to conceal some information in the image. In splicing, some parts of an image or more images are

copied and pasted into another image. This type of forgery is done mostly to defame a person. In the healthcare domain, image forgery can be serious. If a mammogram is hacked, and the intruder uses the copy-move forgery to enlarge the area of cancer, the diagnosis will be wrong, and the patient will be in life-threatening trouble. If there is an image forgery detection system in a healthcare framework, it can detect the forgery before starting the diagnostic process. In the case of a forgery, the system can ask for another sample from the patient. The intrusive method (e.g., embedding a watermark in the medical image) of forgery detection is not suitable in a cloud-based smart healthcare framework mainly because of two reasons: • Embedding a watermark needs extra information for transmission, which may require extra bandwidth and cause a delay in the transmission. • Embedding a watermark may decrease the visual quality of the image, which in turn affects the diagnostic process. There are some existing medical image forgery detection systems in the literature, although the number is small. Ulutas et al. proposed a forgery detection method using a rotation invariant local binary pattern (LBPROT) and a scale invariant

II. RELATED WORK

Copy-move forgery is a prevalent and widely utilized technique in real-time applications. This type of forgery involves copying one region of an image within the same image and pasting it onto another area, thereby concealing significant information. Detecting such forgeries is exceptionally challenging, as the forged image closely resembles the authentic one. This method aims to make certain parts of the image appear to vanish by covering them with copied regions from elsewhere within the image. Typically, texture-rich segments like grass, foliage, rocks, or areas with uneven patterns are chosen as candidates for copying, as they blend seamlessly into the structure of the image, making the forgery imperceptible to the human eye and difficult for attackers to detect. Since the forged parts originate from the same image, they exhibit similar noise features, color palettes, and dynamic ranges as the surrounding segments. As a result, they seamlessly integrate with the rest of the image, making it challenging to distinguish between authentic and forged regions. This characteristic further complicates the task of identifying and mitigating copy-move forgeries, highlighting the need for advanced detection techniques in combating image manipulation.

Copy-Move forgery detection approaches can be subdivided two methods as Key point and Block based method are shown in Fig 1.4 Key-point methods are invariant to statistical features includes scaling and rotation. Block-based methods are mostly used to detect forgery in flat regions, it can manage the multiple attacks and which are robust against JPEG compression and noise. Detecting imperceptible forged images presents a formidable challenge. Any form of forgery establishes a correlation between the forged image and the original image, a correlation crucial for successful forgery detection. Illustrated in Figure 1.2 are various image forgery detection techniques. Among these techniques, several proficient methods are employed for passive image forgery detection, falling into distinct categories. Passive image forgery detection methods operate without necessitating preprocessing or embedded information, relying instead on inherent properties and inconsistencies within the image itself. These methods encompass diverse techniques, such as analyzing pixel-level inconsistencies, scrutinizing statistical anomalies, detecting duplicated regions, and identifying inconsistencies in lighting or shadows. Each method possesses its strengths and challenges, and the effectiveness of forgery detection often hinges on the specific characteristics of the image and the type of forgery attempted. As technology continues to advance, the development of more sophisticated and reliable detection techniques becomes imperative in the ongoing battle against digital image 6 forgery. .Image Forgery Detection Techniques Pixel Based Techniques Pixel-based techniques focus on the digital image pixels which are the basic building blocks. These techniques work on different statistical anomalies which are introduced at the pixel level. The working of these techniques is based on the alterations underlying statistics of the image. The most common forgery detection technique is the copy-move technique. Resampling detection and splicing detection are other major techniques in this category. Format Based Techniques Format based techniques performed based on the image format and normally utilized image format is JPEG format. In JPEG format the blocking effect is employed to detect forgery. Generally, in copy-move forgery, the manipulation of image causes the modification of block artifact grids. The main three characteristics of format based 7 techniques are JPEG Quantization, JPEG blocking and double JPEG are widely used to detect forgery also for compressed images. Suppose the given image is compressed then it is difficult to find the forgery in the image. Camera-Based Techniques A digital camera is an essential equipment to capture digital images. After capturing the image from a digital camera, the image moves from the camera sensor to the memory and it undergoes several processes such as quantization, colour correlation, gamma correction, white adjusting, filtering, and JPEG compression. These steps are processed by capturing to saving the image in

the memory may move on the start of camera model and camera collectibles. Camera response, sensor noise, colour filter array and chromatic aberration are the essential parameter works on camera-based forgery detection techniques. Physical Environment Based Techniques The variance in the 3D interaction between the camera, light and the physical objects are processed to detect the forgery depend on the physical environment. Utilizing the techniques of splicing it is conceivable; however, the making of the correct match in the lighting impacts is regularly troublesome with that of the original photograph. Here the background lighting difference can be utilized as the altering proof. The algorithms work based on distinction in the lighting condition. 2D light detection, 3D light detection, and light Environment are the techniques used in physical environment techniques. Geometry Based Techniques These techniques measure the objects and their camera relative position. The two main fundamental strategies incorporate principal point and metric measurement. The projection of the camera focus to the image plane is denoted as principal point which is located near the center of the image. When the image object is converted, the principle point also changes proportionally. The distinction in the assessed principle point of the image can be utilized as the confirmation of forgery. Acquiring metric measurement from a single image is extremely helpful in forensic settings where real- world measurements.

III. PROPOSED SYSTEM

With the rapid advancement of technology, numerous features have been integrated into healthcare systems to enhance people's satisfaction and accessibility to medical services. Nowadays, individuals can consult with doctors remotely, monitor health metrics such as diabetes, heartbeat, voice abnormalities, and emotions using various sensors. Despite the significant progress in the healthcare sector, attention is required to address security and privacy concerns within healthcare facilities. The leakage or alteration of medical data can have severe consequences, leading to social embarrassment or disadvantage for affected patients and unauthorized advantages for 27 others. Hence, it is essential to implement a robust system within smart healthcare frameworks to verify the integrity of medical data during transmission, safeguarding them against hackers or intruders. Two primary methods are employed to ensure data integrity: intrusive and nonintrusive techniques. In the intrusive method, information called a watermark is embedded into the data without affecting the message. This watermark can later be extracted and compared with the original to detect any alterations or forgeries. However, the intrusive method may not always be feasible, as not all data may have intentional or unintentional watermarks. In contrast, non-intrusive methods do not rely on adding watermarks to the data. Instead, algorithms analyze the data for abnormal patterns or distortions that may indicate tampering or fraud. Non-intrusive techniques offer flexibility as they can verify any data against changes or fraud without requiring additional modifications. Numerous non-intrusive techniques have been proposed in the literature, particularly focusing on detecting image forgery. These techniques leverage sophisticated algorithms to identify inconsistencies or irregularities in images, enabling the detection of various forms of manipulation or forgery. By prioritizing non-intrusive methods, healthcare facilities can enhance data security and integrity while ensuring patient confidentiality and trust in digital healthcare solutions.

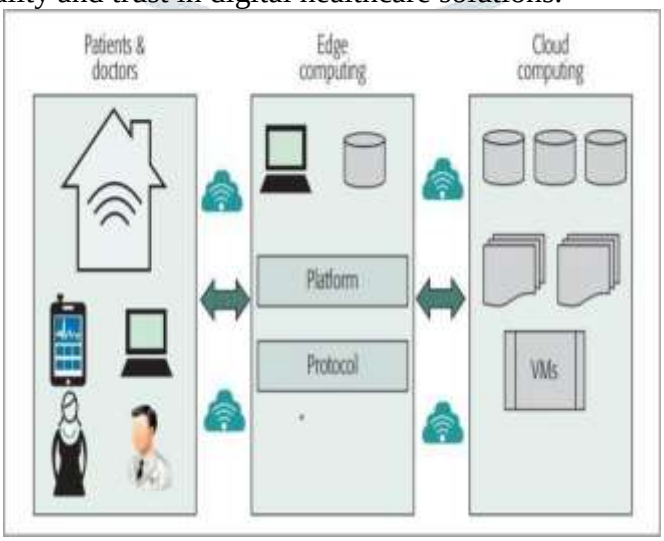

Fig 1 The proposed smart healthcare framework

Every camera maker has an intrinsic pattern embedded in the image. This pattern is destroyed when there is a forgery in the image. The irregularity in the Markov chain pattern can reveal the forgery. Although this method of detecting forgery is interesting, it may not be suitable for detecting medical image forgery because the intrinsic pattern is more prominent in color images, and the medical images are

mostly gray images. This article presents a new image forgery detection system, which can be implemented in the smart healthcare framework. In the system, a noise map is extracted from the image using a Wiener-filterbased noise reduction technique. A multi-resolution regression filter is applied to the noise map to find an inter-relationship between a pixel and the neighbouring pixels. The output of this filter is normalized and fed into an SVM based classifier. We also use an extreme learning machine (ELM)-based classifier and combine the scores of these two classifiers using a Bayesian sum rule (BSR).
The proposed smart healthcare framework consists of several components. One component contains patients (clients) and doctors, another component comprises edge computing, and yet another component covers cloud computing. Figure 3.1 shows these three components of the proposed framework. The patients can reside in smart homes in a smart city, while the doctors and caregivers can be located at any designated hospitals and clinics.

Image Forgery Detection The image forgery detection algorithms either work at the pixel level or at the segment level. In the pixel level algorithm, the relationship between the intensities of the pixels is captured to define the texture of the image. In the segment level algorithms, segments of an image are compared. The segmentation of the image is considered as an extra overhead of the algorithms. In the pixel level case, the image may be divided into blocks. This article proposes a pixel level algorithm to detect image forgery. There are several pixel level algorithms that are used in image forgery detection in the literature. The most famous one is LBP, which is fast to compute, but vulnerable to the presence of noise. Another one is the Weber local descriptor (WLD).

We propose an image forgery detection system to be deployed in the smart healthcare framework. The system consists of several components, such as noise pattern extraction, the realization of a multi-resolution regression filter, and two classifiers. Fig 2 shows a block diagram of the proposed system. The steps of the work flow of the system are given below.

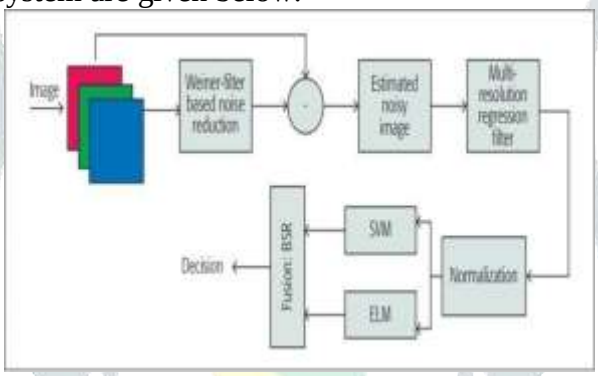

Fig 2 Block diagram of the proposed image forgery detection system.

Step 1: If the image is a colour image, decompose it into red, green, and blue channels. If the image is a monochrome image, there is no need for this step.
Step 2: The Wiener-filter is applied to each component of the colour image or the monochrome image itself. The output of this step is an image (or component) free from noise.
Step 3: The noise-free image is subtracted from the original image to get an estimated noise pattern of the image. The noise pattern is considered as the fingerprint of the image. If any forgery is done, this fingerprint is distorted.
Step 4: The multi-resolution regression filter is applied to the noise pattern. The regression filter is illustrated in Fig.3.2 In this filter, the nearest eight-pixel positions have weight 1, while the next neighbouring pixels' positions have weight 2, and so on. The characteristic of this filter is to capture the relative intensity of a center pixel. The final weight is normalized between 0 and 255 to maintain the intensity level of a gray image.
Step 5: The output of the filter is fed to two classifiers: the SVM classifier and the ELM classifier. We investigated different kernels of the SVM: linear, polynomial, and radial basis function (RBF).
Step 6: In the proposed system, the scores from Support Vector Machine (SVM) and Extreme Learning Machine (ELM) classifiers are fused using the Binary Score Fusion (BSR) method to determine whether an image is forged or not. The decision is made based on the score obtained from BSR. Utilizing the Wiener-filter-based noise reduction technique is preferred because of its local operation within an image, ensuring preservation of important information, particularly crucial in medical image analysis where data integrity is paramount. While alternative noise reduction methods exist, caution must be exercised to prevent loss of vital data.
Both SVM and ELM classifiers are employed in the system due to their effectiveness as binary classifiers and their complementary nature. SVM utilizes kernel functions to project data from a low-dimensional to a high-dimensional space, facilitating the separation of samples from different classes by a hyperplane.

On the other hand, ELM boasts a single hidden layer, ensuring rapid convergence without issues of overfitting. This combination of classifiers enhances the robustness and accuracy of the forgery detection system, contributing to its efficacy in detecting manipulated images.

IV. RESULTS

The figure 3 is original image which is medical report of brain after that will divide the image into stacks for clear vision where forgery has done then the image is divided into clusters and find the local minima and maxima based on that values key point localization has done and descriptor points are located where the forgery has expected to done. Based on the intensity variations will tell that image is forgered or not. Finally the result of the medical image forgery detection is showed.

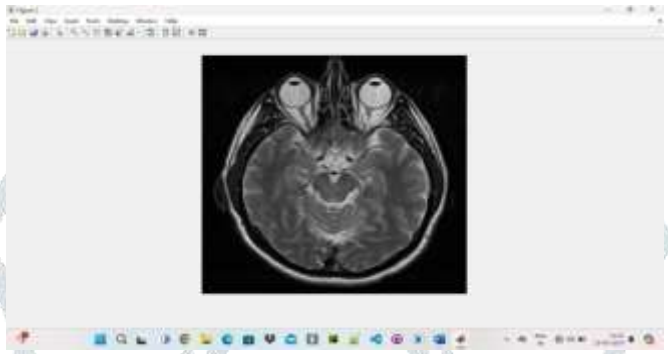

Fig 3 Original Image of Brain

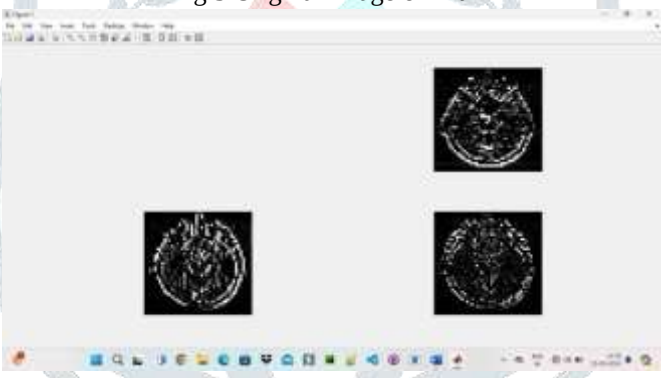

Fig 4 Dividing Image into Stacks

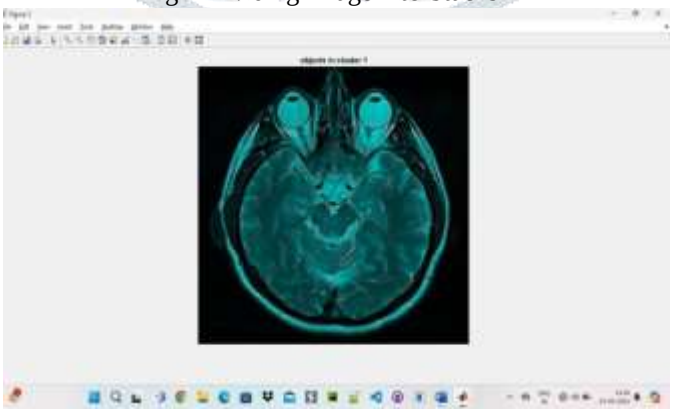

Fig 5 Objects in cluster 1

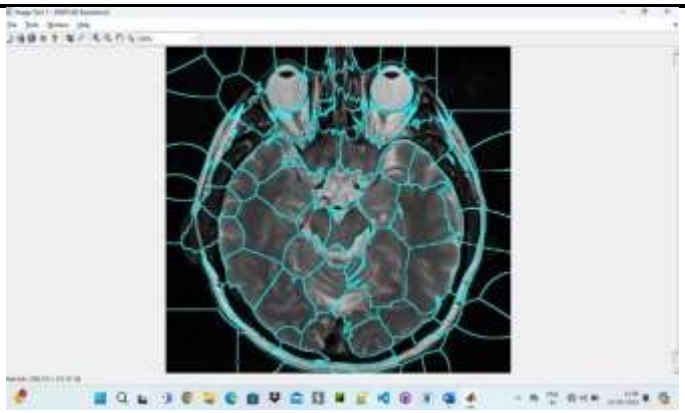

Fig 6 Dividing image into cluster

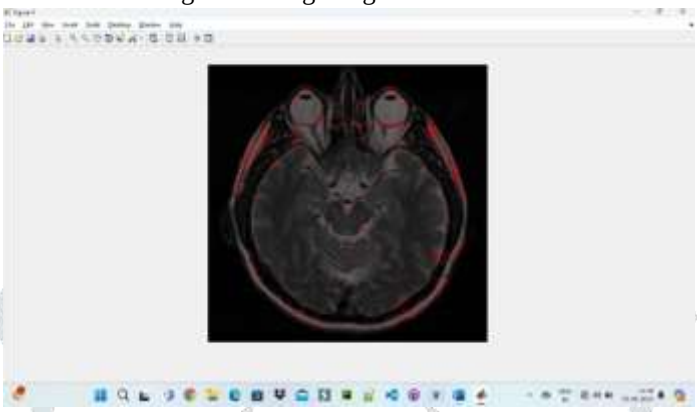

Fig 7 Key point Localisation

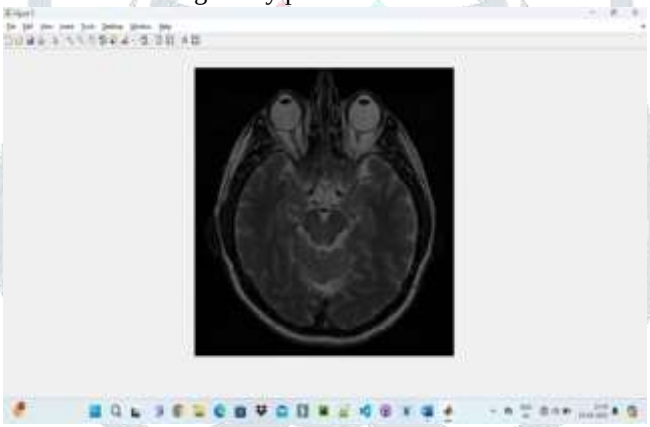

Fig 8 Descriptor Point Localization

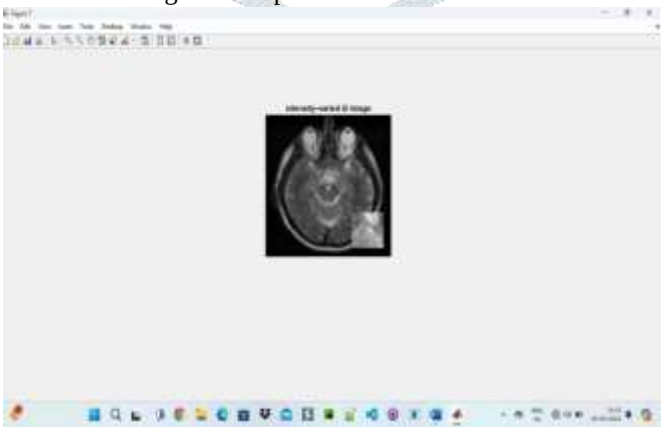

Fig 9 Intensity Variation Image

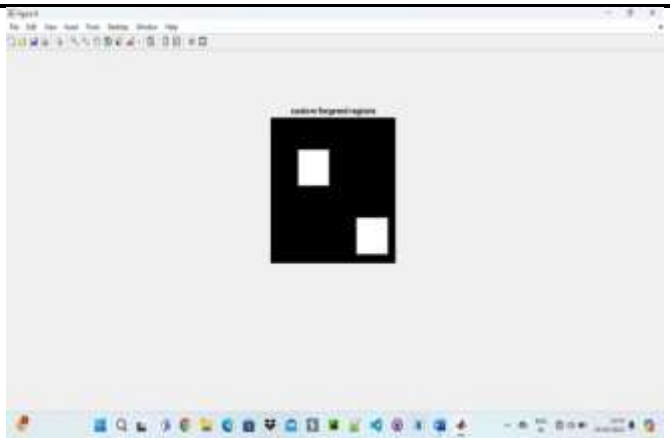

Fig 10 Custom Forgered Regions

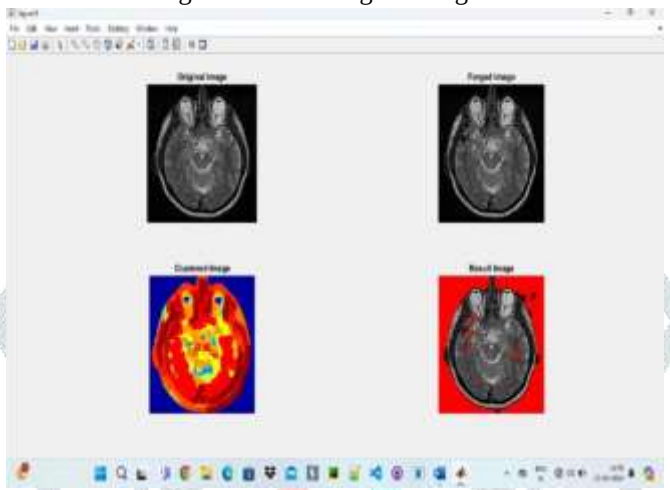

Fig 11 Result of Medical Image Forgery Detection

Finally, the figure 11 is the result of medical image forgery detection which can have the difference between the original image and the forgered images along with custom forgered regions and the forgered regions are indicated with red colour blocks easy to identify where the forgery has done.

V. CONCLUSIONS AND FUTURE SCOPE

An image forgery detection system was proposed in the smart healthcare framework. The system was tested using three different databases, two having natural images and one having mammograms. The system achieved accuracies over 98 percent for natural images and 84.3 percent for medical images. The system performed best when we combined the scores of two classifiers. The area of medical image forgery detection needs more attention to gain the trust of patients and to avoid their embarrassment. There is still a long way to go in this research. The next generation of network technologies bring immense computing power and ubiquitous service. We can take advantage of these technologies to make the healthcare system seamless, real-time, trustable, secure, and easy to use. The future directions of this research can be as follows: Investigate the use of deep learning techniques in medical image forgery detection. Scramble the medical image before transmitting it to the cloud. Develop a robust forgery detection technique against a high degree of compression which will lead to a real-time application.

The future of medical image forgery detection looks bright, focusing on several key areas. We expect to see better integration of advanced AI and deep learning techniques, which will make the detection of tampered images more accurate and faster. Systems will become more scalable, allowing them to handle large volumes of images from various sources, and will work across different types of medical scans like MRI, CT, and X-rays. User-friendly interfaces and automated workflows will make it easier for healthcare professionals to use these systems. Emphasis on privacy and security, including the use of blockchain, will ensure that patient data remains safe and authentic. Collaboration between healthcare institutions and the development of standardized regulations will further enhance the reliability and consistency of these technologies. Ongoing research will continue to drive innovation, making forgery detection a crucial part of future healthcare practices.

REFERENCES

[1] Solanas et al., "Smart Health: A Context Aware Health Paradigm within Smart Cities," IEEE Commun. Mag., vol. 52, no. 8, Aug. 2014, pp. 74–81.

[2] C. Bekara, "Security Issues and Challenges for the IoT Based Smart Grid," Proc. COMMCA-2104, Procedia Computer Science 34, 2014, pp. 532–37.

[3] M. A. Qureshi and M. Deriche, "A Bibliography of Pixel-Based Blind Image Forgery Detection Techniques," Signal Processing: Image Communication, vol. 39, Part A, Nov. 2015, pp. 46–74.

[4] M. S. Hossain et al., "Audio-Visual Emotion-Aware Cloud Gaming Framework," IEEE Trans. Circuits and Systems for Video Tech., vol. 25, no. 12, Dec. 2015, pp. 2105–18.

[5] J.O. Fajardo, I. Taboada, and F. Liberal, "Radio-Aware Service-Level Scheduling to Minimize Downlink Traffic Delay through Mobile Edge Computing," Mobile Networks and Management, 2015, pp. 121–34.

[6] T. Ahonen, A. Hadid, and M. Pietikainen, "Face Description with Local Binary Patterns: Application to Face Recognition," IEEE Trans. Pattern Anal. Mach. Intell., vol. 28, 2006, pp. 2037–41.

[7] J. Chen et al., "WLD: A Robust Local Image Descriptor," IEEE Trans. Pattern Anal. Mach. Intell., vol. 32, no. 9, Sept. 2010, pp. 1705–20.

[8] J. Dong and W. Wang, "CASIA Tampered Image Detection Evaluation (TIDE) Database, v1.0, and v2.0," 2011; http:// forensics.idealtest. org/.

[9] M. Heath et al., "The Digital Database for Screening Mammography," Int'l. Work. Dig. Mamm., vol. 212–8, 2000.

[10] G.-B.Huang et al., "Extreme Learning Machine for Regression and Multiclass Classification," IEEE Trans. Sys., Man, Cybern. B, Cybern., vol. 42, no. 2, Apr. 2012, pp. 513–29.

[11] G. Muhammad et al., "Image Forgery Detection Using Steerable Pyramid Transform and Local Binary Pattern," Machine Vision and Applications, vol. 25, no. 4, May 2014, pp. 985–95.

[12] X. Zhao et al., "Detecting Digital Image Splicing in Chroma Spaces," Proc. Int'l. Wksp. Digital Watermarking, 2011, pp. 12–22.

[13] G. Ulutas et al., "Medical Image Tamper Detection Based on Passive Image Authentication," J. Digital Imaging, vol. 30, no. 6, Dec. 2017, pp 695–709.

[14] M. S. Hossain et al., "Toward End-to-End Biomet ric-Based Security for IoT Infrastructure," IEEE Wireless Commun., vol. 23, no. 5, Oct. 2016, pp. 44–51.

[15] G. Gao et al., "Reversible Data Hiding with Contrast Enhancement and Tamper Localization for Medical Images," Info. Sciences, vol. 385–86, 2017, pp. 250–65.