FORGERY DETECTION OF MEDICAL IMAGE

Sirisha Gudla
Department of Information Technology
Vignan Institute of Technology and Science Hyderabad, India
ORCID: 009-0030-7096-3718

Bhuvan Sai Teja Gabbita
Department of Information Technology
Vignan Institute of Technology and Science Hyderabad, India
ORCID: 0009-0006-1992-0124

Nirupama Chaganti
Department of Information Technology
Vignan Institute of Technology and Science Hyderabad, India
ORCID: 0009-0008-2966-3939

Srinivas Boddepally
Department of Information Technology
Vignan Institute of Technology and Science Hyderabad, India
ORCID: 0009-0005-2113-3982

Mayur Raj Singh Biasthakur
Department of Information Technology
Vignan Institute of Technology and Science Hyderabad, India
ORCID: 0009-007-2422-7671

I. ABSTRACT

Numerous features and amenities have been introduced to the healthcare system as a result of the development. New features and capacities are added to a smart healthcare framework when new communication technologies are developed. The features and facilities seek to give clients with a smooth, easy-to-use, accurate, and real-time healthcare service. Because health is such a delicate subject, it should be handled with extreme care and caution. This paper presents a novel medical picture forgery detection system for the healthcare framework to ensure that healthcare-related photos are not modified or altered. The system works on an image's noise map, applies a multi-resolution regression filter to it, and feeds the result to support-vector-machine-based and extreme-learning-based classifiers. The noise map is generated at an edge computing resource, while the

filtering and classification are performed in a core cloud computing resource. As a result, the system operates smoothly and in real time. The suggested system's bandwidth need is likewise fair.

II. INTRODUCTION

Technologies like edge computing and cloud computing have sparked several new revolutions in the healthcare industries in the future generation. From its previous era to the present, this has seen an enormous shift. In order to meet the demands of the public, several additional features have been implemented. People may now use a variety of sensor gadgets to check their blood pressure, diabetes, and pulse rate without physically seeing a doctor. This article is being offered to determine whether or not any image from a medical report is susceptible to falsification. For instance, if medical information is stolen or changed, the patient may feel let down or ashamed in public, while other individuals may benefit illegally. We have presented two techniques—intrusive and non-intrusive—to prevent these circumstances. In the intrusive technique, certain information is introduced to the data while keeping the data's message undisturbed. The data is referred to as a watermark. The watermark is removed from the data and compared with the original watermark if any doubt develops afterwards. The data is regarded as having been altered or faked if they do not match. The data is not given a watermark in the non-intrusive technique. By studying any unusual patterns, certain algorithms are employed to discover any distortion or alteration in the data.

In , various non-intrusive tactics have been suggested. In this post, we concentrate on non-intrusive methods of identifying fake images. You may find a decent review on this subject [3]. There are several methods for forging one or more photos. Splicing and copy-move forgeries are the most typical types of picture fraud. In a copy-move image forgery, a portion of the original picture is duplicated, then pasted into various sections of the original image. The main goal of this kind of forgery is to hide certain information from view. Splicing is the process of copying and pasting portions of one or more pictures into another one. The main goal of this kind of forgery is to malign a person. Image falsification may be a severe problem in the field of medicine.Although few, there are several extant medical picture forgery detection systems in the literature. A forgery detection technique employing a scale invariant feature transform (SIFT) and a rotation invariant local binary pattern (LBPROT) was proposed by Ulutas et al. The texture of the medical picture was defined using the LBPROT, and the key points were extracted using the SIFT. A comparison of the important points was used to determine if the document was forged.. A support vector machine (SVM)-based classifier received this histogram as input. The accuracy across many databases was good. One issue with this approach is that it uses a lot of sub-bands, which is unsuitable for real-time transmission in the context of cloud-based healthcare. In order to characterise the pictures and perform machine learning methods to determine whether or not the representation is forged, the detection of image forgery also uses some texture descriptions. With the use of the Weiner filter-based noise reduction in this instance, the picture is divided into various channels. A multi-resolution approach is used to determine the relationships between the pixels in order to do that. The support vector-based classifier and extreme learning machine are then used to deploy the output.

III. LITERATURE SURVEY

Governments and businesses now have the chance to reconsider how they see healthcare thanks to the new era of mobile health that has been brought about by the widespread deployment of ubiquitous computing and mobile communications. At the same time, the global urbanisation process poses a tough task and draws attention to cities that are anticipated to attract larger inhabitants and offer residents services in an effective and compassionate way. Mobile health and smart cities are a result of these two phenomena. The context-aware addition to mobile health in smart cities is the new idea of smart health, which we explain in this paper. We give a summary of the key scientific disciplines that have been engaged in developing this novel idea.**[1]**

The smart grid concept is formed by combining traditional electricity networks with information and communication technology. Hopefully, research into the evolution of conventional power grid systems into smart grids will continue as communication and information technology advance. Smart grid system testing is typically done in simulation settings. A smart grid application, on the other hand, requires a real-world test environment known as a "testbed" in order to produce more effective real-world implementations. The smart grid, which combines traditional power lines with information and communication technology, is vulnerable to cyberattacks, which is a major problem in upgrading the smart grid. The intrinsic nature of information and communication technology makes smart grids vulnerable to cyberattacks. To identify effective remedies against cyber-attack capabilities in smart grid practises, testbeds where cyber-security research and studies may be undertaken are required. This study presents an evaluation of available smart grid testbeds with cyber security capabilities. First, a quick overview of the history, domains, research topics, and security challenges in smart grids is provided. The smart grid testbeds and functionalities are then discussed. Existing security-focused testbeds and their cyber-attack testing capabilities are also assessed. Finally, we wrap up the research and make some recommendations for security-focused testbed implementations.[2]

Cloud gaming's intriguing potential and new uses have piqued the curiosity of academics, business, and the general public. However, because of the trade-off between resource usage and player emotion, which is influenced by the game screen, offering a high-quality gaming experience in the cloud gaming framework is a difficult challenge. We address this issue by merging emotion-aware screen effects with remote display technologies in the cloud gaming framework. The framework's initial stage is the learning or training stage, which uses Gaussian mixture model-based classifiers to build a link between screen characteristics and emotions. A linear programming methodology delivers suitable screen adjustments in the operational stage depending on the real-time user emotion received in the first stage. Our experiments show that the proposed framework is effective. The findings suggest that our proposed architecture can deliver a high-quality gaming experience while providing a manageable workload for the cloud server in terms of resource usage.[3]

This study provides a unique and efficient face image representation based on textural information from local binary patterns (LBP). The face picture is separated into areas from which the LBP feature distributions are extracted and concatenated to form an improved feature vector that will be utilised as a face descriptor. The suggested method's performance in the face recognition issue is evaluated using various challenges. Other applications and extensions are also covered**.** [4]

Mammography is now one of the most extensively utilised procedures for detecting breast cancer. Breast cancer abnormalities include masses and calcifications. Breast cancer is the primary cause of mortality from cancer in women. Breast cancer screening is improved by combining advanced technology with existing imaging modalities. The most widely available data sets for mammographic pictures are the Mammographic Image Analysis Society (MIAS) and the Digital Database for Screening Mammography (DDSM). MAMMSIT is an additional data set for mammographic image analysis. MAMMSIT is the name of the mammogram data collection, which comprises normal and malignant group pictures of mammography. The database includes our suggested data set with relevant annotations such as age, background tissue, ultra sound screen location, and BIRADS level. [5]

IV. WORKING

Decompose the image into red, green, and blue channels if it is a colour image. There is no need for this step if the image is monochromatic. Each component of the colour picture or the monochrome image is subjected to the Wiener filter. This stage results in a noise-free picture (or component). The noise-free picture is subtracted from the original image to provide an approximation of the image's noise pattern. The noise pattern is said to be the image's fingerprint. This fingerprint will be altered if it is forged. The noise pattern is subjected to the multi-resolution regression filter. This filter depicts the regression filter: the adjacent eight-pixel locations have weight 1, the next surrounding pixels' places have weight 2, and so on. This filter's feature is that it captures the relative intensity of a centred pixel.

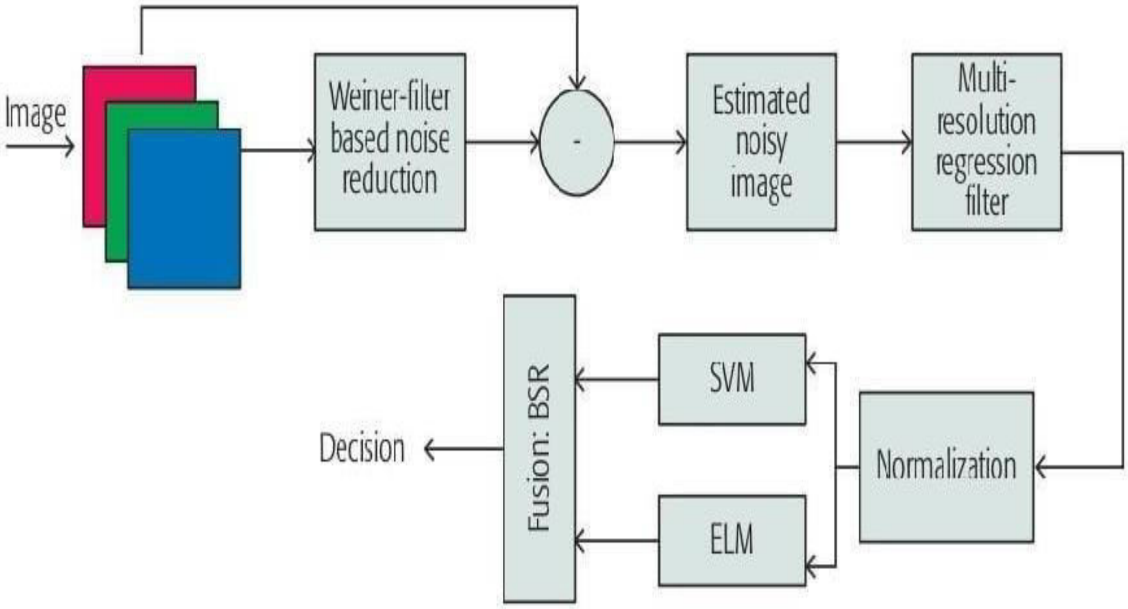


Image
Weiner-filter based noise reduction
-
Estimated noisy image
Multi-resolution regression filter
Normalization
SVM
ELM
Fusion: BSR
Decision

Fig 1. System Architecture

Matlab

Matrix Laboratory is an abbreviation for Matrix Laboratory. It is described as a technical computing environment" by its creator, Math Works. We'll take the more ordinary approach and say it's a programming language. MATLAB is a programme that was created to make the creation of numerical linear algebra functions easier. It has subsequently expanded into much more than that, and it is now used to build numerical algorithms for a wide range of applications.

Open GUI Layout Editor

Syntax

```
Guide
guide('filename.fig')
guide('fullpath')
guide(HandleList)
```

Description

Dataset

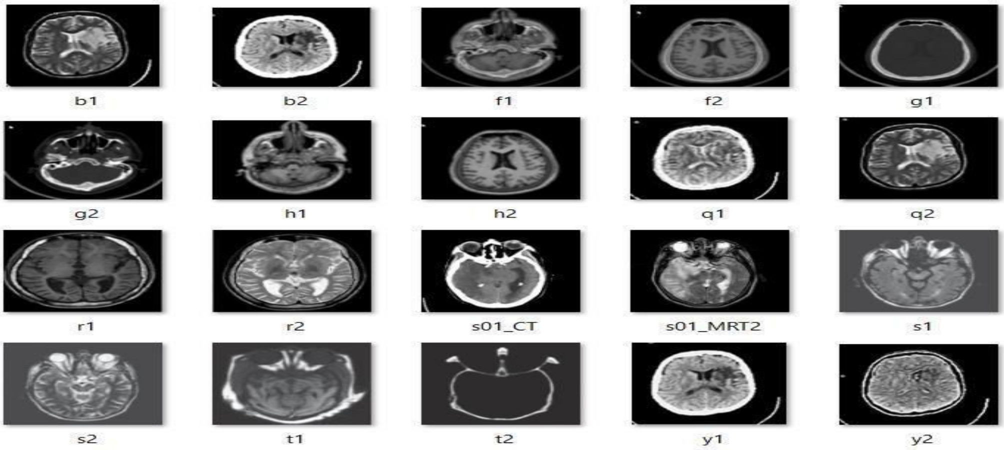


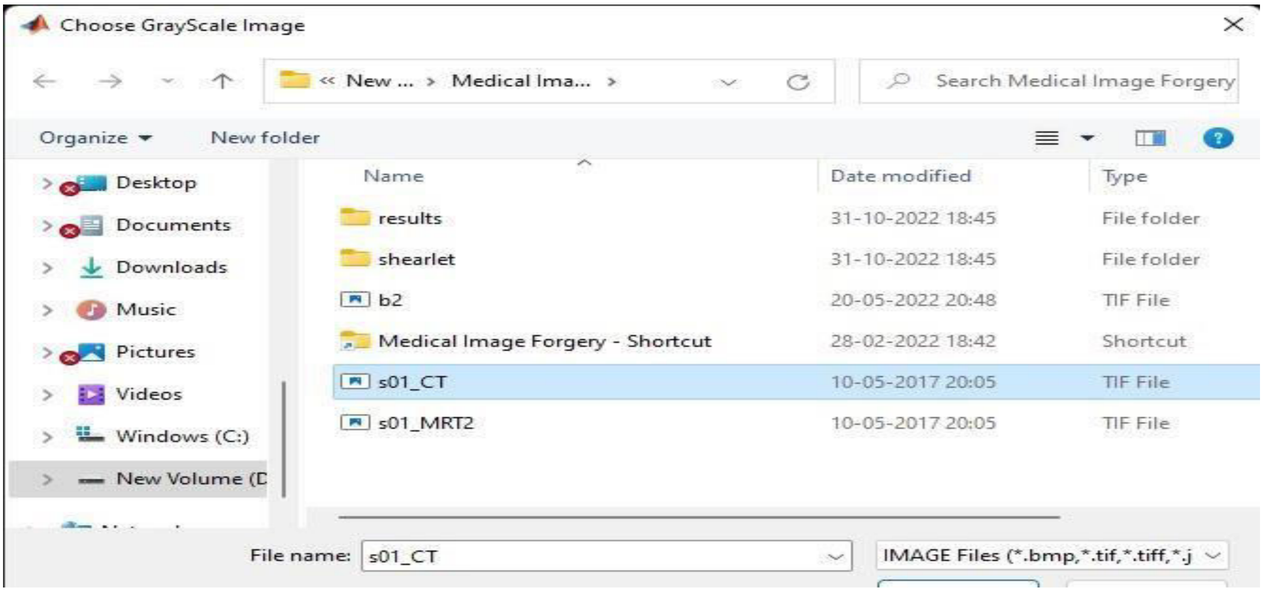
Fig 2. Dataset

Firstly, it's important to ensure that the dataset consists of high-quality images that accurately represent the medical conditions or anatomical structures being depicted. This will help ensure that any modifications or forgeries made to the images are as realistic as possible. Secondly, it's important to ensure that the dataset contains a diverse range of image modalities, such as X-rays, CT scans, and MRI scans. This will help ensure that the forgery detection methods are applicable across a range of medical imaging techniques. Thirdly, it's important to ensure that the dataset includes both original images and their duplicates with various types of forgeries and modifications. This will help evaluate the accuracy and effectiveness of forgery detection methods in detecting different types of forgeries.

V. METHODOLOGY

Copy-move forgery imaging is a special type of forgery that involves copying parts of an image and then pasting the co ied parts into the same image. Hence, image forensics associated with copy-move forgery detection have become increasingly important in our networked society. The technology used in image forensics can b categorized into passive detection or active detection. The active detection method requires prior informati n derived from an image to identify the image authenticity, such as watermarking. Contrary to active detect on methods, passive detection methods are not required to obtain previous information on an image. Passive detection methods can utilize the advantages of the detective strategy to find the tampering regions. Hence, a large majority of image forgery detection methods adopt a passive-based strategy to perform the type of tampering identification discussed in the present study. Passive detection technology can be categorized into block-based methods and key point-based methods. In the present study, we focus on the key point-based approach.

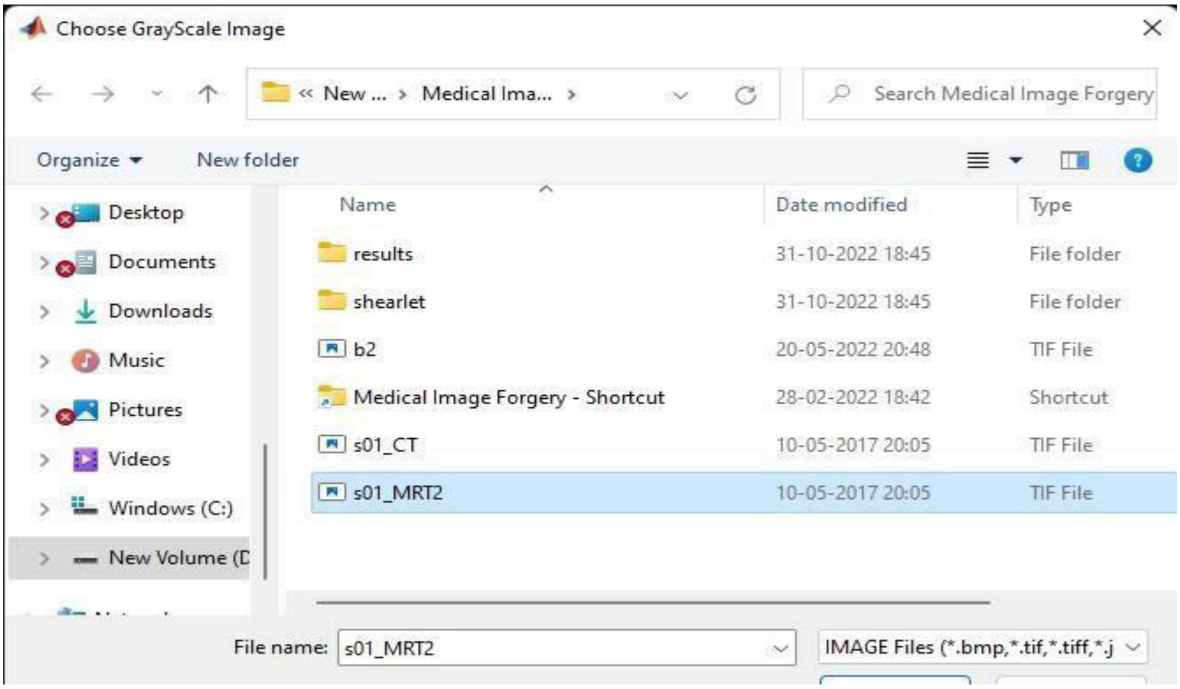
VI. RESULT



Name	Date modified	Type
results	31-10-2022 18:45	File folder
shearlet	31-10-2022 18:45	File folder
b2	20-05-2022 20:48	TIF File
Medical Image Forgery - Shortcut	28-02-2022 18:42	Shortcut
s01_CT	10-05-2017 20:05	TIF File
s01_MRT2	10-05-2017 20:05	TIF File

File name: s01_CT

Fig 3. Grey Scale Image 1



Name	Date modified	Type
results	31-10-2022 18:45	File folder
shearlet	31-10-2022 18:45	File folder
b2	20-05-2022 20:48	TIF File
Medical Image Forgery - Shortcut	28-02-2022 18:42	Shortcut
s01_CT	10-05-2017 20:05	TIF File
s01_MRT2	10-05-2017 20:05	TIF File

File name: s01_MRT2

Fig 4. Grey Scale Image 2

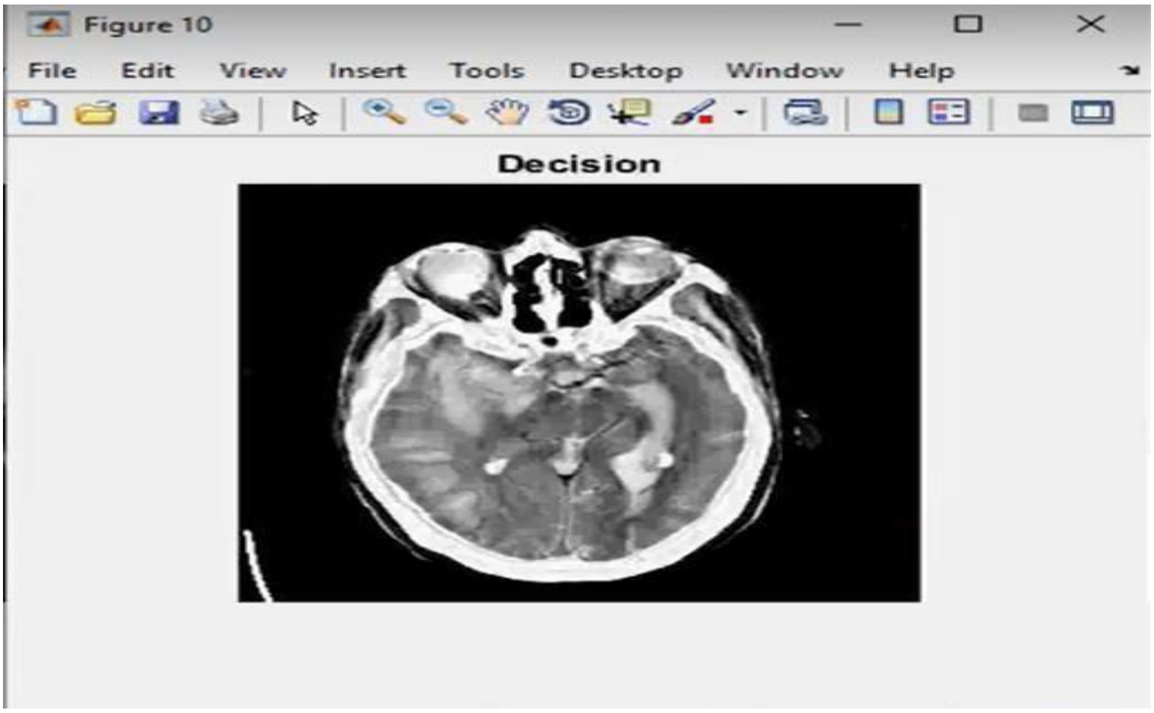


Fig 5. prompt representing the forged image as final output

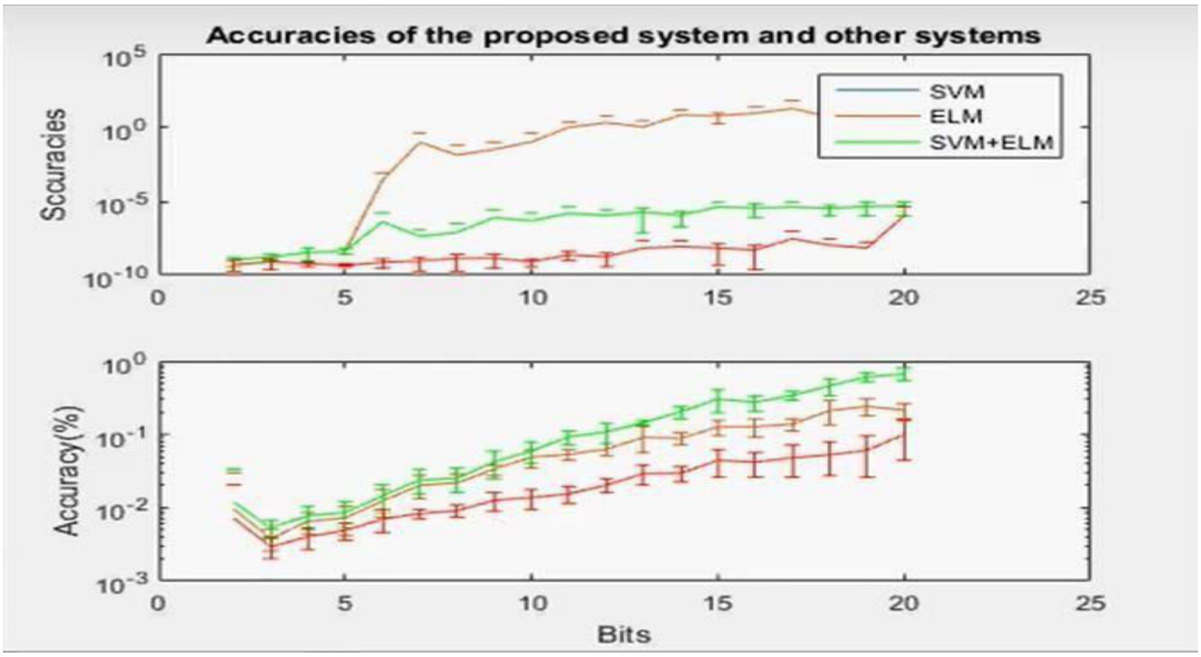


Fig 6. Accuracies of the system

VII. CONCLUSION

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 84.3percent 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.

REFERENCES

[1] Solanas et al., “Smart Health: A Context Aware Health Paradigm within Smart Cities,” Aug. 2014

[2] C. Bekara, “Security Issues and Challenges for the IoT Based Smart Grid,” 2014.

[3] M. S. Hossain et al., “Audio-Visual Emotion-Aware Cloud Gaming Framework,” Dec. 2015.

[4] T. Ahonen, A. Hadid, and M. Pietikainen, “Face Description with Local Binary Patterns: Application to Face Recognition,” 2006.

[5] G.-B.Huang et al., “Extreme Learning Machine for Regression and Multiclass Classification,” Apr. 2012.