ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

A Survey on Biometric Liveness Detection Using Various Techniques

Anita Babu[1], Dr. Vince Paul[2]

M.Tech Student, Dept. of Computer Science & Engineering, Sahrdaya College of Engineering & Technology, Kodakara, Kerala, India[1]

Associate Professor, Dept. of Computer Science & Engineering, Sahrdaya College of Engineering & Technology, Kodakara, Kerala, India[2]

ABSTRACT: Biometric systems are increasingly used for authentication purposes in various security systems. Face, Fingerprint and Iris are the biometric modalities commonly used in the present authentication system. Simplicity of use, reliability and uniqueness are important features of biometric based authentication systems. This kind of techniques can solve the typical problem of systems based on use of password which can be forgotten or stolen. Biometric systems play a significant role in personal, national, and global security. Despite the increase in usage of biometric based systems, these are quiet susceptible to sophisticated spoofing attacks. Various spoofing attacks are present to defeat such biometric authentication systems. To improve the level of security, it is necessary to augment the reliable liveness detection tools as software modules along with the existing authentication systems. This paper targets the countermeasures for the biometric spoofing attacks and also suggests technical measures for implementing the biometric liveness detection systems. The research in this field is very active, with local descriptors. Inorder to overcome the shortcomings of alredy existing liveness detection tools,in this work we propose two different feature extraction techniques for software-based liveness detection: Convolutional Networks and Local Binary Patterns. Both techniques were used in conjunction with a Support Vector Machine (SVM) classifier. Dataset Augmentation was used to increase classifier's performance and a variety of preprocessing operations were tested, such as frequency filtering, contrast equalization, and region of interest filtering.

KEYWORDS: liveness, convolutional networks, local binary patterns, data augmentation, support vector machines

1. INTRODUCTION

Biometrics systems have significantly improved person identification and authentication, playing an important role in personal, national, and global security. Biometric systems are more and more often used for authentication in various security applications. By relying on physiological attributes of each individual they offer simplicity of use and reliability at the same time, avoiding typical problems of systems based on the use of passwords, which can be forgotten, transferred or stolen. Despite their many advantages, biometric systems, like any other security application, are vulnerable to a range of attacks. Fingerprint, face, and iris are the biometric traits most frequently used in present authentication systems . Of course, biometric systems have their own weaknesses, in particular they are relatively vulnerable to some sophisticated forms of spoofing. For example, it is possible to fool a fingerprint-based system by reproducing the biometric pattern on simple molds made of materials such as silicone, Play-Doh, clay or gelatin . Likewise, iris-based systems can be attacked with fake irises printed on paper or on wearable plastic lenses while face-based systems can be fooled with sophisticated 3D masks (easily bought online once a few photos of the subject are provided) or, again, with faces printed on paper . Biometric authentication systems are quite vulnerable to sophisticated spoofing attacks. To keep a good level of security, reliable spoofing detection tools are necessary, preferably implemented as software modules.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

Clearly, these attacks have elicited a race towards some reliable anti-spoofing systems, and in particular towards liveness detection techniques, which use various physiological properties to distinguish between real and fake traits. In principle, besides being reliable, blocking attackers and allowing legitimate users in the systems, liveness detection methods should posses other important properties , being non-invasive, user friendly, fast, and low cost.

A large number of methods have been proposed in recent years to combat spoofing . Some of them rely on the detection of vitality signs at the acquisition stage. Hence they require additional hardware embedded in the sensor which verifies vitality by measuring particular intrinsic properties of a living trait, such as temperature, odor, sweat, blood pressure, or reflection properties of the eye , sometimes also in response to specific stimuli . By combining multiple sources of information, this approach turns out to be more resilient to specific attacks, providing a very good reliability. However, it is a relatively expensive and rigid solution, potentially vulnerable to attacks not considered at design time.On the contrary, software-based methods, based on signal-processing techniques, are certainly more appealing, for their reduced cost and invasiveness, and their higher flexibility. They try to detect liveness by analyzing synthetic image features that are peculiar of vital biometric traits and not easily reproduced on fakes. Liveness detection methods are generally classified into two types : (i) Softwarebased techniques, in this type the fake trait is Detected once the sample has been acquired with a normal sensor (i.e., features used to differentiate between real and fake traits are extracted from the biometric sample, and not from the trait itself); (ii) Hardware-based techniques, which add some particular device to the sensor in order to detect Exacting properties of a living trait (e.g., fingerprint sweat, blood pressure, or specific reflection properties of the eye)[1]. liveness detection techniques, which use different physiological properties to differentiate between real and fake character.

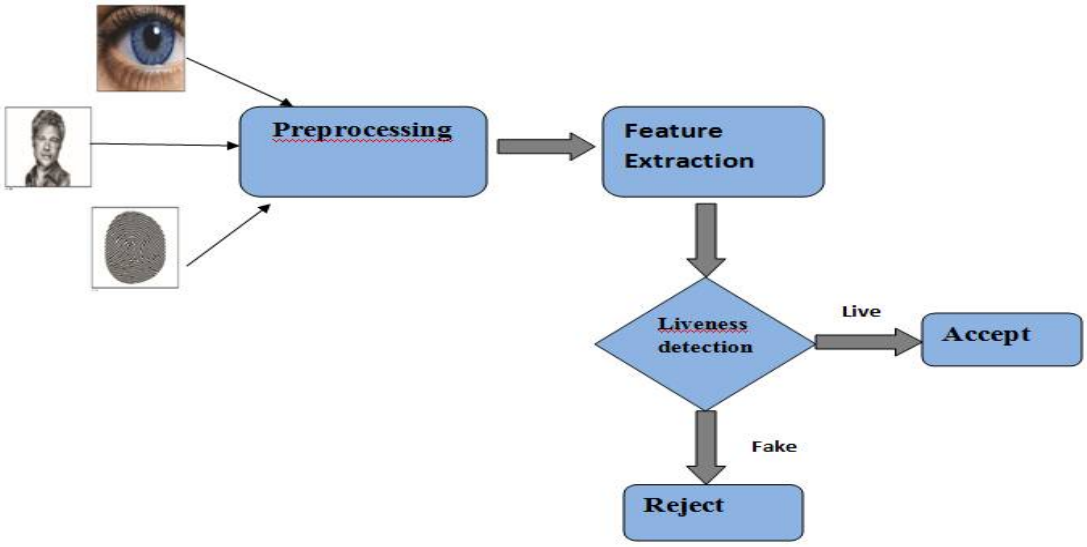

Fig.1 overview of liveness detection system

Once the biometric trait has been acquired a feature extraction process followed by a classification step labels the image as fake or live. Only in this last case the image is considered for the recognition phase. In the following we will review the literature on liveness detection for nger print, iris and face images. The majority of techniques follow the paradigm shown in Fig.1., differing mainly in the type of features extracted.Besides other anti-spoong approaches such as the use of multi biometrics or challenge-response methods, special attention has been paid by researchers and industry to the liveness detection techniques, which use different physiological properties to distinguish between real and fake traits. Liveness assessment methods represent a challenging engineering problem as they have to satisfy certain demanding requirements:

- non-invasive, the technique should in no case be harmful for the individual or require an excessive contact with the user;
- user friendly, people should not be reluctant to use it;

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

- fast, results have to be produced in a very reduced interval as the user cannot be asked to interact with the sensor for a long period of time;
- low cost, a wide use cannot be expected if the cost is excessively high;
- performance, in addition to having a good fake detection rate, the protection scheme should not degrade the recognition performance (i.e., false rejection) of the biometric system.

This paper targets the countermeasures for the biometric spoofing attacks and also suggests technical measures for implementing the biometric liveness detection systems. Inorder to overcome the shortcomings of alredy existing liveness detection tools,in this work we propose two different feature extraction techniques for software-based liveness detection: Convolutional Networks and Local Binary Patterns. Both techniques were used in conjunction with a Support Vector Machine (SVM) classifier.

II RELATED WORKS

Different fingerprint liveness detection algorithms have been proposed and they can be broadly divided into two approaches: hardware and software.[1] In the hardware approach, a specific device is added to the sensor in order to detect particular properties of a living trait such as blood pressure [2], skin distortion[3],or odor[4].

A large number of methods have been proposed in recent years to combat spoofing . Some of them rely on the detection of vitality signs at the acquisition stage[5]. Hence they require additional hardware embedded in the sensor which verifies vitality by measuring particular intrinsic properties of a living trait, such as temperature, odor, sweat, blood pressure, or reflection properties of the eye sometimes also in response to specific stimuli .

[6] Biometric systems based on face recognition have been shown unreliable under the presence of face-spoofing images. Hence, automatic solutions for spoofing detection became necessary. In this paper, face-spoofing detection is proposedby searching for Moiré patterns due to the overlap of the digital grids. The conditions under which these patterns arise are first described, and their detection is proposed which is based on peak detection in the frequency domain. Experimental results for the algorithm are presented for an image database of facial shots under several conditions. In this paper, a face-spoofing detection algorithm was proposed based on the detection of Moiré patterns due to the overlap of digital grids. The conditions under which these patterns arise were described and experimentally verified. The effectiveness of the proposed algorithm was also verified by running tests on a database of face images shot under several conditions. Results show that, under the right conditions, face-spoofing detection can be performed with great accuracy.

[7] To ensure the actual presence of a real legitimate trait in contrast to a fake self-manufactured synthetic or reconstructed sample is a significant problem in biometric authentication, which requires the development of new and efficient protection measures. In this paper, we present a novel software-based fake detection method thatcan beused inmultiple biometric systems to detect different types of fraudulent access attempts. The objective of the proposed system is to enhance the security of biometric recognition frameworks, by adding liveness assessment in a fast, user-friendly, and non-intrusive manner, through the use of image quality assessment. The proposed approach presents a very low degree of complexity, which makes it suitable for real-time applications, using 25 general image quality features extracted from one image (i.e., the same acquired for authentication purposes) to distinguish between legitimate and impostor samples. The experimental results, obtained on publicly available data sets of fingerprint, iris, and 2D face, show that the proposed method is highly competitive compared with other state-of-the-art approaches and that the analysis of the general image quality of real biometric samples reveals highly valuable information that may be very efficiently used to discriminate them from fake traits.

[8] In this paper, address the problem of face spoof detection, particularly in a cross-database scenario. While most of the published methods use motion or texture based features, They propose an efficient and rather robust face spoof detection algorithm based on image distortion analysis (IDA). Four different features (specular reflection, blurriness, chromatic moment, and color diversity) are extracted to form the IDA feature vector. An ensemble classifier, consisting of multiple SVM classifiers trained for different face spoof attacks (e.g., printed photo and replayed video), is used to

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

distinguish between genuine (live) and spoof faces. The proposed approach is extended to multiframe face spoof detection in videos using a voting-based scheme.

[9] In this work, we investigated two deep representation research approaches for detecting spoofing in different biometric modalities. On one hand, we approached the problem by learning representations directly from the data through architecture optimization with a final decision-making step atop the representations. On the other, we sought to learn filter weights for a given architecture using the well-known backpropagation algorithm. As the two approaches might seem naturally connected, we also examined their interplay when taken together. In addition, we incorporated our experience with architecture optimization as well as with training filter weight for a given architecture into a more interesting and adapted network, spoofnet. Experiments showed that these approaches achieved outstanding classification results for all problems and modalities outperforming the state-of-the-art results in eight out of nine benchmarks.

[10] In this paper, a novel fingerprint liveness descriptor named "BSIF" is described, which, similarly to Local Binary Pattern and Local Phase Quantization-based representations, encodes the local fingerprint texture on a feature vector. Experimental results on LivDet 2011 data sets appear to be encouraging and make this descriptor worth of further investigations. The BSIF descriptor has two parameters: the filter size and the number of features extracted. These algorithms extract from a fingertip image a certain number of features that will be used to classify the fingerprint as either live or fake. This algorithm clearly outperformed the LBP and LPQ methods.

[11] This paper aims at assessing the potential of these descriptors for the liveness detection task in authentication systems based on various biometric traits: fingerprint, iris, and face. Besides compact descriptors based on the independent quantization of features, already considered for some liveness detection tasks, we will study promising descriptors based on the joint quantization of rich local features. The experimental analysis, conducted on publicly available data sets and in fully reproducible modality, confirms the potential of these tools for biometric applications, and points out possible lines of development toward further improvements.

[12] In this paper, we use convolutional neural networks (CNNs) for fingerprint liveness detection. Our system is evaluated on the data sets used in the liveness detection competition of the years 2009, 2011, and 2013, which comprises almost 50000 real and fake fingerprints images. We compare four different models: two CNNs pretrained on natural images and fine-tuned with the fingerprint images, CNN with random weights, and a classical local binary pattern approach. We show that pretrained CNNs can yield the state-of-theart results with no need for architecture or hyperparameter selection. Data set augmentation is used to increase the classifiers performance, not only for deep architectures but also for shallow ones. This model won the first prize in the fingerprint liveness detection competition 2015 with an overall accuracy of 95.5%.

III. LIVENESS DETECTION TECHNIQUES

. Liveness detection methods are generally classified into two types : (i) Softwarebased techniques, in this type the fake trait is Detected once the sample has been acquired with a normal sensor (i.e., features used to differentiate between real and fake traits are extracted from the biometric sample, and not from the trait itself); (ii) Hardware-based techniques, which add some particular device to the sensor in order to detect Exacting properties of a living trait (e.g., fingerprint sweat, blood pressure, or specific reflection properties of the eye)[1]. liveness detection techniques, which use different physiological properties to differentiate between real and fake character.

Table 1 shows the comparative study of the various liveness detection techniques .based the liveness assement parameter.mainly the study is based on the multi biometric and multi attack characteristics.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

Method	Strength	Limitations
Hardware-based techniques, (challenge-response methods, intrinsic properties)	higher fake detection rate, increase the robustness to direct attacks, Very high accuracy, very good reliability	lack of generality, Higher level of user cooperation required, Expensive, usually slower, rigid solution
Face-Spoofing 2D-Detection Based on Moiré-Pattern Analysis	Results show that, under the right conditions, face-spoofing detection can be performed with great accuracy, Very effective against photo based attack, implementation is transparent to the user.	Reliable only for face spoof detection, Poor generalization ability, Performance degrade wih light intensity variation
Image Quality Analysis Based Method(IQA)	"multi-biometric" and "multi-attack" characteristics, Good generalization ability, Fast response, simple, non-intrusive, user-friendly and cheap Low computational complexity	Different classifiers are needed for different spoof attack, not used video quality measures for video attacks
Face Spoof Detection With Image Distortion Analysis	the proposed approach outperforms the state-of-the-art methods in face spoof detection, very effective against video based attack	lack of generality, Reliable only for face spoof detection, trait specific(not multi-biometric)
Deep Representations for Iris, Face, and Fingerprint Spoofing Detection	Experiments showed that these approaches achieved outstanding classification results for all problems and modalities outperforming the state-of-the-art results in eight out of nine benchmarks	High computational complexity, requirement of greater number of training samples.
Local Descriptors for Biometric Spoofing Detection	excellent performance and flexibility.	All descriptor-based classifiers, in fact, require training on a large set of images describing the source. data augmentation not considered here for uniformity
Fingerprint Liveness Detection Using Convolutional Neural Networks	Data set augmentation is used to increase the classifiers performance, not only for deep architectures but also for shallow ones. good accuracy	Lack of generality, not multi-biometric

Table 1: Comparative Study

IV. PROBLEM STATEMENT

Biometrics already form a significant component of current and emerging identification technologies. Biometrics systems aim to determine or verify the identity of an individual from their behavioural and/or biological characteristics. Despite their many advantages, biometric systems, like any other security application, are vulnerable to a range of attacks. To keep a good level of security, reliable spoofing detection tools are necessary, preferably implemented as software modules. The aim of this work is to provide an efficient liveness detection of fingerprint, face, iris using convolutional networks and local binary patterns.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

V.PROPOSED SYSTEM MODEL

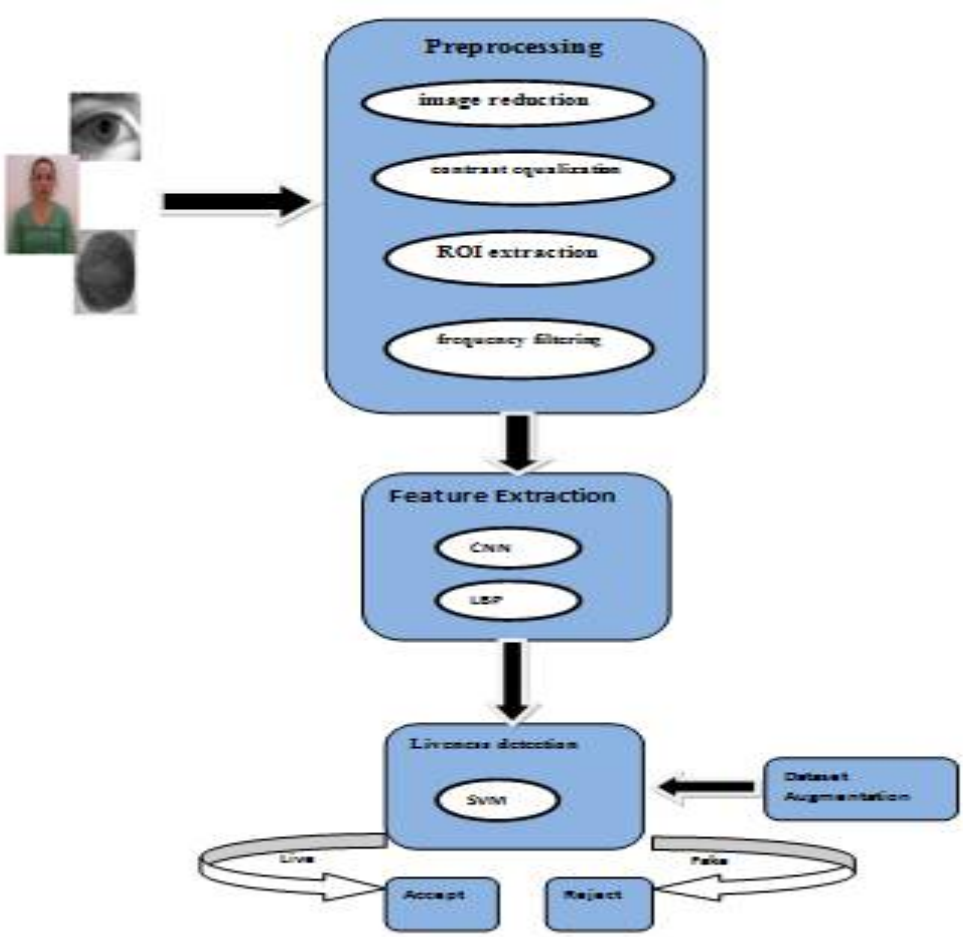

Fig.2 System model

Inorder to overcome the shortcomings of already existing liveness detection tools,in this work we propose two different feature extraction techniques for software-based liveness detection(Fig .2): Convolutional Networks and Local Binary Patterns. Both techniques were used in conjunction with a Support Vector Machine (SVM) classifier. Dataset Augmentation is used to increase classifier's performance and a variety of preprocessing operations are tested, such as frequency filtering, contrast equalization, and region of interest filtering.

A. DESIGN GOALS:

- Deep networks designed and trained for the task of object recognition can be used to achieve state-of-the-art accuracy in liveness detection. No specific hand engineered technique for the task oft liveness detection was used. Thus, we provide another success case of transfer learning for deep learning techniques..
- Pre-trained Deep networks require less labeled data to achieve good accuracy in a new task
- Dataset augmentation helps to increase accuracy not only for deep architectures but also for shallow techniques such as LBP

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

- Achieving invariance to changes in position or lighting conditions, robustness to clutter, and compactness of representation

VI. CONCLUSION

biometric authentication systems are quite vulnerable to sophisticated spoofing attacks. to keep a good level of security, reliable spoofing detection tools are necessary, preferably implemented as software modules. .all the main techniques and functions in this liveness detection area are included in this paper. as shown in this paper, there are several different methods and techniques working against current presentation attack scenarios efficiently. here it must be mentioned that none of these techniques provide an entire protection to biometric systems. especially, the detection of video attacks is a particular challenge . as a consequence, a combination of different liveness detection techniques is strongly recommended. moreover, there are several other detection techniques that should be used for detecting presentation attacks and protecting against manipulations of biometric systems to increase the overall security .a very good performing liveness detection system is not only capable of operating under different biometric systems (multibiometric) and for diverse spoong scenarios, but it also provides a very good level of protection against certain non-spoofing attacks (multi-attack). inorder to overcome the shortcomings of already existing liveness detection tools,in this work we propose two different feature extraction techniques for software-based liveness detection: convolutional networks and local binary patterns. both techniques were used in conjunction with a support vector machine (svm) classifier.

REFERENCES

1. Maximilian Krieg,Nils Rogmann," Liveness Detection in Biometrics", BIOSIG international conference, November 2015.
2. P. D. Lapsley, J. A. Lee, D. F. Pare, Jr., and N. Hoffman, "Anti-fraud biometric scanner that accurately detects blood flow," U.S. Patent 5737439, Apr. 7, 1998.
3. A. Antonelli, R. Cappelli, D. Maio, and D. Maltoni, "Fake finger detection by skin distortion analysis," IEEE Trans. Inf. Forensics Security, vol. 1, no. 3, pp. 360–373, Sep. 2006.
4. D. Baldisserra, A. Franco, D. Maio, and D. Maltoni, "Fake fingerprint detection by odor analysis," in Advances in Biometrics. Heidelberg, Germany: Springer, 2005, pp. 265–272.
5. Y. N. Singh and S. K. Singh, "Vitality detection from biometrics: State-of-the-art," in Proc. World Congr. Inf. Commun. Technol., Dec. 2011, pp. 106–111.
6. Diogo Caetano Garcia,Ricardo L. de Queiroz, " Face-Spoofing 2D-Detection Based on Moiré-Pattern Analysis", IEEE transactions on information forensics and security, vol. 10, no. 4, April 2015.
7. J. Galbally, S. Marcel, and J. Fierrez, "Image quality assessment for fake biometric detection: Application to iris, fingerprint, and face recognition," IEEE Trans. Image Process., vol. 23, no. 2, pp. 710–724, Feb. 2014.
8. Di Wen, Hu Han,Anil K. Jain, "Face Spoof Detection With Image Distortion Analysis", IEEE transactions on information forensics and security, vol. 10, no. 4, April 2015
9. David Menotti, Giovani Chiachia, Allan Pinto, "Deep Representations for Iris, Face, and Fingerprint Spoofing Detection", IEEE transactions on information forensics and security, vol. 10, no. 4, April 2015.
10. Luca Ghiani, Abdenour Hadid, Gian Luca Marcialis, Fabio Roli" Fingerprint liveness detection using Binarized Statistical Image Features",IEEE 6 th International conference, Oct 2013.
11. Diego Gragnaniello, Giovanni Poggi, Carlo Sansone, Luisa Verdoliva," An Investigation of Local Descriptors for Biometric Spoofing Detection", IEEE transactions on information forensics and security, vol. 10, no. 4, April 2015
12. Rodrigo Frassetto Nogueira, Roberto de Alencar Lotufo, and Rubens Campos Machado," Fingerprint Liveness Detection Using Convolutional Neural Networks", IEEE transactions on information forensics and security, vol. 11, no. 6, June 2016

BIOGRAPHY

Mrs.Anita Babu is currently doing her M.Tech in Computer Science & Engineering from Sahrdaya College of Engineering & Technology, Kodakara, Thrissur. She completed her B.Tech in CSE from Sahrdaya College of Engineering & Technology, Thrissur. Her area of interest is security, image processing.