Synthetic or Reconstructed Biometric Sample Detection for Real-Time Systems:Application to Face Recognition

Preeti R Dubey, Manikamma

Abstract-This paper covers, a novel scheme of software-based fake detection method that can be used in multiple biometric system to detect different types of fraudulent access attempts. To ensure the actual presence of real legitimate trait in contrast to a fake self-manufactured synthetic sample is a significant problem in biometric authentication, which requires the development of new protection measures. The objective of this method is to enhance the security of biometric recognition system by adding liveness assessment in a fast, user friendly, and non intrusive manner, through the use of image quality assessment. This method 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 to distinguish between legitimate and imposter samples.

Keywords- Image quality assessment, biometric, security, attacks, countermeasures.

INTRODUCTION

Biometric based personal identification techniques that use physiological or behavioral characteristics are becoming increasingly popular compared to traditional token-based or knowledge based techniques such as identification cards, passwords, etc. One of the main reasons for this popularity is the ability of the biometric technology to differentiate between an authorized person and an imposter who fraudulently acquires the access privilege of an authorized person. Among various commercially available biometric techniques such as face, voice, fingerprint, iris, etc, the biometric techniques offer a reliable method for personal identification, the problem of security and integrity of the biometric data poses new issues. In order to promote the wide spread utilization of biometric techniques, an increased level of security of biometric data is necessary.

Biometric is defined as the technology for automatically identifying individuals based on their distinct physical or behavioral characteristics [1], such as fingerprint, face, voice, iris, etc. However, with the widely used verification based on biometrics, it creates a demand for ensuring the security and integrity of biometric data. In our method we are making use of image quality assessment for liveness detection. The use of image quality assessment for liveness detection is motivated by the supposition that: "It is expected that a fake image captured in an attack attempt will have different quality than a real sample acquired in the normal operation scenario for which the sensor was designed". Predictable quality differences between real and fake samples may contain: color and luminance levels, general artifacts, quantity of information, and quantity of sharpness, found in both type of images, structural distortions or natural appearance. For example, iris image captured from a printed paper are more likely to be unclear or out of focus due to trembling, this fake sample will most likely lack some of the properties found in natural images.

The potential of general image quality assessment as a protection method against different biometric attacks (with special attention to spoofing). Different quality measures present diverse sensitivity to image artifacts and distortions. For example, measures like the mean square error respond additive to noise, while others such as the spectral phase error are extra sensitive to blur; while gradient-related features respond to distortions concentrated around edges and textures. Therefore, using a large range of IQMs exploiting complementary image quality properties should allow detecting the aforementioned quality differences between real and fake samples expected to be found in many attack attempts (i.e., given that the technique with multi attack protection capabilities). So consider that there is sound proof for the "quality-difference" theory and that image quality measures have the possible to achieve success in biometric protection tasks.

EXISTING SYSTEM

Image quality has been successfully used in previous works for image manipulation detection [14] and steganalysis in the forensic field. To a certain extent, many spoofing attacks, especially those which involve taking a picture of a facial image displayed in a 2D device (e.g., spoofing attacks with printed iris or face images), may be regarded as a type of image manipulation which can be effectively detected by the use of different quality features.

In addition to the previous studies in the forensic area, different features measuring trait-specific quality properties have already been used in fingerprint and iris applications. However, even though these two works give a solid basis to the use of image quality as a protection method in biometric systems, none of them is general. For instance, measuring the ridge and valley frequency may be a good parameter to detect certain fingerprint spoofs, but it cannot be used in iris. On the other hand, the amount of occlusion of the eye is valid as an

Manuscript received May, 2015.

Ms Preeti R Dubey, *Computer Science and Engineering, Godutai Engineering College for Women, Gulbarga, India, 9620370208*
Prof. Manikamma Malipatil*, Computer Science and Engineering, Godutai Engineering College for Women, Gulbarga, India, 9945941988.*

iris anti-spoofing mechanism, but will have little use in fake fingerprint detection.

Although all of them represent very valuable works which bring insight into the difficult problem of spoofing detection, they fail to generalize to different problems as they are usually designed to work on one specific modality and, in many cases, also to detect one specific type of spoofing attack. Human observers very often refer to the "different appearance" of real and fake samples to distinguish between them.

A different quality measure presents different sensitivity to image artifacts and distortions. For instance, measures like the mean squared error respond more to additive noise, whereas others such as the spectral phase error are more sensitive to blur; while gradient-related features react to distortions concentrated around edges and textures. Therefore, using a wide range of IQMs exploiting complementary image quality properties, should permit to detect the aforementioned quality differences between real and fake samples expected to be found in many attack attempts.

PROPOSED SYSTEM

The problem of fake biometric detection can be seen as a two-class classification problem where an input biometric sample has to be assigned to one of two classes: real or fake. The key point of the process is to find a set of discriminant features which permits to build an appropriate classifier which gives the probability of the image "realism" given the extracted set of features. In the present work we propose a novel parameterization using general image quality measures. A general diagram of the protection approach proposed in this work is shown in Fig. 1. In order to keep its generality and simplicity, the system needs only one input: the biometric sample to be classified as real or fake.

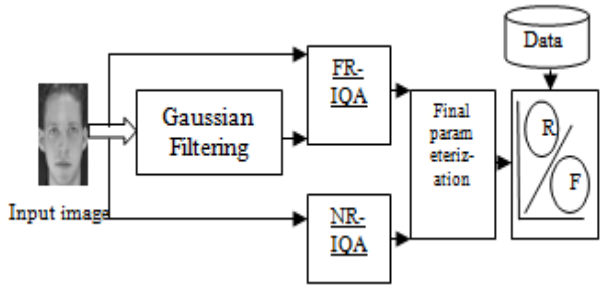

Fig.1 General diagram of the biometric protection method based on Image Quality Assessment (IQA) proposed in the present work.

A). Full reference IQ measures

Full-reference (FR) IQA methods rely on the availability of a clean undistorted reference image to estimate the quality of the test sample. In the problem of fake detection addressed in this work such a reference image is unknown, as the detection system only has access to the input sample.

This approach assumes that the loss of quality produced by Gaussian filtering differs between real and fake biometric samples.

- Error Sensitivity Measures: Traditional perceptual image quality assessment approaches are based on measuring the errors (i.e., signal differences) between the distorted and the reference images, and attempt to quantify these errors in a way that simulates human visual error sensitivity features.
- Pixel Difference measures : These features compute the distortion between two images on the basis of their pixel wise differences. Here we include: Mean Squared Error (MSE), Peak Signal to Noise Ratio (PSNR), Signal to Noise Ratio (SNR), Structural Content (SC), Maximum Difference (MD), Average Difference (AD), Normalized Absolute Error (NAE), R-Averaged Maximum Difference (RAMD) and Laplacian Mean Squared Error (LMSE).
- Correlation-based measures: The similarity between two digital images can also be quantified in globally: IQA FOR FAKE BIOMETRIC DETECTION terms of the correlation function. A variant of correlation based measures can be obtained by considering the statistics of the angles between the pixel vectors of the original and distorted images.
  These features include: Normalized Cross-Correlation (NXC), Mean Angle Similarity (MAS) and Mean Angle- Magnitude Similarity (MAMS).
- Edge-based measures: Edges and other two-dimensional features such as corners, are some of the most informative parts of an image, which play a key role in the human visual system and in many computer vision algorithms including quality assessment applications. Since the structural distortion of an image is tightly linked with its edge degradation, here we have considered two edge-related quality measures: Total Edge Difference (TED) and Total Corner Difference (TCD).
- Spectral distance measures: In this work we will consider as IQ spectral-related features: the Spectral Magnitude Error (SME) and the Spectral Phase Error (SPE).
- Gradient-based measures: Gradients convey important visual information which can be of great use for quality assessment. Many of the distortions that can affect an image are reflected by a change in its gradient. Therefore, using such information, structural and contrast changes can be effectively captured .Two simple gradient-based features are included in the biometric protection system proposed : Gradient Magnitude Error (GME) and Gradient Phase Error (GPE)
- Information Theoretic Measures: The quality assessment problem may also be understood, from an information theory perspective, as an information-fidelity problem (rather than a signal-fidelity problem. In the present work we consider two of these information theoretic features: the Visual Information Fidelity (VIF) and the Reduced Reference Entropic Difference index (RRED).

B). No reference IQ measures

- Distortion-specific approaches: These techniques rely on previously acquired knowledge about the type of visual quality loss caused by a specific distortion. The final quality measure is computed according to a model trained on clean images and on images affected by this particular distortion. Two of these measures have been included in the biometric protection method proposed in the present work. The JPEG Quality Index (JQI), which evaluates the quality in images.
- Training-based approaches: Similarly to the previous class of NR-IQA methods, in this type of techniques a model is trained using clean and distorted images. Then, the quality score is computed based on a number of features extracted from the test image and related to the general model.

This is the case of the Blind Image Quality Index (**BIQI**), which is part of the feature set used in the present work.

METHODOLOGY

In our method initially the input is given as biometric image. By using that image enhancing can be done by Gaussian filter. It contains IQM parameters (FULL REFERENCE IQMS, NO REFERENCE IQMS). Image feature extraction can be done by "IMAGE QUALITY ASSESSMENT". After that feature extraction is performed. Then by comparing the image with stored image data to identify the image is real/fake. Finally if the output is not matching with data it is fake biometric image. If the output matches with data it is real biometric image.
For face biometric image if the image is real then it proceed for recognition. Here we provide a new framework in the face recognition System by the use of (ASM) Active Shape model. Initially we detect the face from the image. After that we extract the LBP feature. It is used to find the texture feature for the face image. Active shape models (ASMs) are statistical model of the shape of objects which iteratively deform to fit to an example of the object in a new image. The modules used for face recognition are:

A) Preprocessing
B) Normalization
C) Active shape model
D) Feature Extraction And Recognition

A) Preprocessing:

- In noise removal process, Initially we convert the image in gray. And then we filter the noise from the image. In Filtering we are applying Gaussian filtering to our input image.
- Gaussian filtering is often used to remove the noise from the image.
- Gaussian filter is windowed filter of linear class, by its nature is weighted mean.
- Named after famous scientist Carl Gauss because weights in the filter calculated according to Gaussian distribution.

B) Normalization:

- Normalization is a process that changes the range of pixel intensity values. Illumination changes caused by light sources at arbitrary positions and intensities contribute to a significant amount of variability.
- To address this issue, we present a new method for performing image normalization.
- The method used to remove shadows and specularities from images. All the shadowed regions are grayed out to a uniform color, eliminating soft shadows and specularities and hence creating an illumination invariant signature of the original image.

C) Active Shape model:

- Active shape models (ASMs) are statistical models of the shape of objects which iteratively deform to fit to an example of the object in a new image.
- The shapes are constrained by the PDM (point distribution model) Statistical shape model to vary only in ways seen in a training set of labeled examples. The shape of an object is represented by a set of points (controlled by the shape model).
- The ASM algorithm aims to match the model to a new image. It works by alternating the following steps:
- Look in the image around each point for a better position for that point.
- Update the model parameters to best match to these new found positions.

D) Feature Extraction:

- Initially we separate the image as patches. For each patch of image we apply the LBP (Local Binary Pattern).
- The LBP operator assigned a label to every pixel of a gray level image. The label mapping to a pixel is affected by the relationship between this pixel and its eight neighbors of the pixel. If we set the gray level image is I, and Z0 is one pixel in this image. So we can define the operator as a function of Z0 and its neighbors, Z1, … , Z8. And it can be written as:

$$T = t(Z0, Z0\text{-}Z1, Z0\text{-}Z2, \dots, Z0\text{-}Z8).$$

However, the LBP operator is not directly affected by the gray value of Z0, so we can redefine the function as following:

$$T \fallingdotseq t(Z0\text{-}Z1, Z0\text{-}Z2, \dots, Z0\text{-}Z8).$$

To simplify the function and ignore the scaling of grey level, we use only the sign of each element instead of the exact value. So the operator function will become:

$$T \fallingdotseq t(s(Z0\text{-}Z1), s(Z0\text{-}Z2), \dots, s(Z0\text{-}Z8)).$$

Where the s (.) is a binary function, defined as $s(x) = 1$, $x>=0$; $S(x) = 0$, otherwise.

- And finally recognition process is identify by the weighted matching. similarity is identified between the features. Finally identified image is displayed.

System Architecture: Following fig.2 shows the architecture of face recognition system

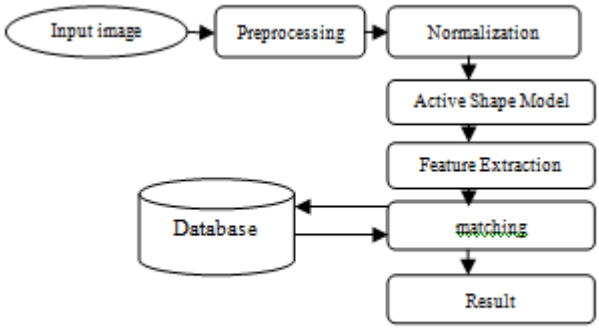

Fig.2 Diagram shows face recognition system architecture

EXPERIMENTS AND RESULTS

The evaluation experimental protocol has been designed with a two-fold objective: First, it evaluates the- multi biometric dimension of the protection method. And second, evaluate the- multi-attack dimension of the protection method. Following section shows the results produced by the system.

Results: Iris

The database used in this scenario is the ATVS-Fir DB which may be obtained from the Biometric Recognition Group-ATVS. The database comprises real and fake iris images (printed on paper). The results obtained for real and fake iris images are shown below.

Following figures Fig.3 and Fig.4 shows the progress of training process on feature set of iris database and completion of training.

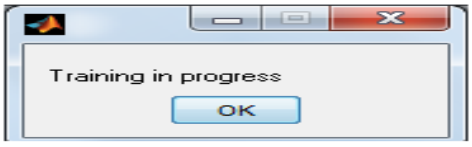

Fig.3 Diagram shows training process

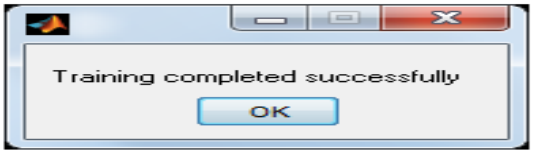

Fig.4 shows the completion of training process

After completion of training we select recognition feature, and proceed with an application provided in the menu box. Here we have selected an iris feature by taking corresponding iris database, if the image selected is fake it will identify as fake and if the image is real it will show as real and abort the execution. This is shown in the following two figures, Fig.5 and Fig.6.

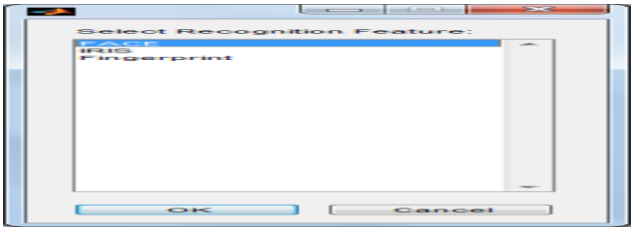

Fig.5 shows the menu with three features: Face, Iris and Fingerprint

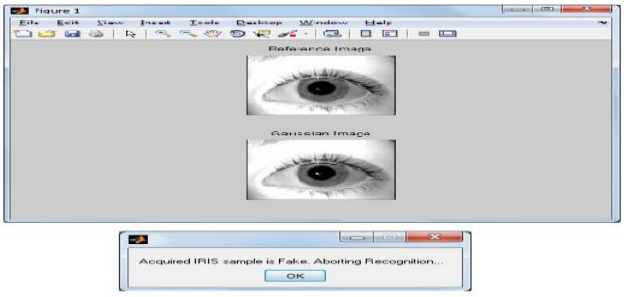

Fig.6 Recognized iris image is fake aborting recognition

Results: Fingerprint

For the fingerprint modality, the performance of the proposed protection method is evaluated comprising real and fake samples. As in the iris experiments the database is divided into a: train set, used to train the classifier; and test set, used to evaluate the performance of the protection method.

Similarly as we have done for iris, for fingerprint also we initially select the feature. And fingerprint image is selected from corresponding database. If selected image is fake, system identifies it as fake or if it is real then system identifies it as real image and abort the execution. This is shown in the following two figures, Fig.7 and Fig.8.

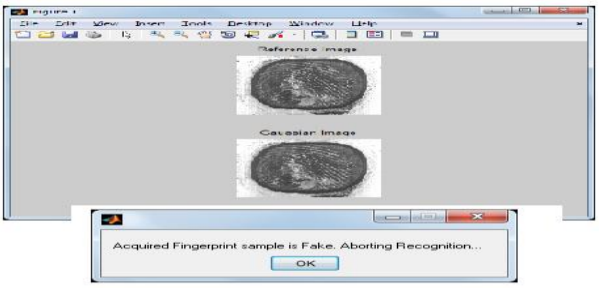

Fig.7 Fingerprint image showing as fake after analysis

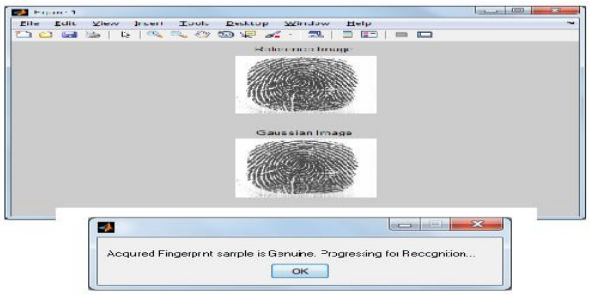

Fig.8 Fingerprint image showing as Genuine after analysis

Results: Face

For the face modality, the performance of the proposed protection method is evaluated comprising real and fake samples. As in the iris and fingerprint experiment the database is divided into a: train set, used to train the classifier; and test

set, used to evaluate the performance of the protection method. Once face image is identified as real it will proceed for further recognition. If the face image is fake, then it will abort the recognition.

This process proceeds by loading the pixel values of the given image, for the given original image Gaussian filter is applied then the filtered image is obtained with removal of noise contents. Following figures show the process of loading the input image and filtering image.

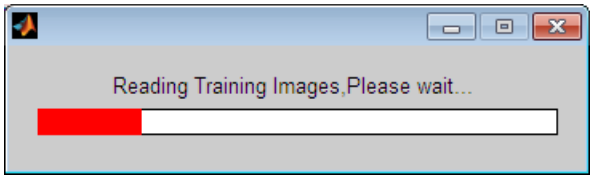

Fig.9 Diagram shows reading process of input image

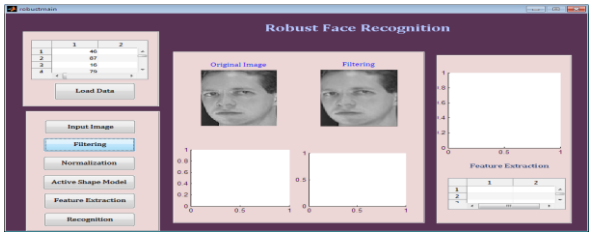

Fig.10 Diagram showing face analysis with filtered input image

Image normalization is performed after filtering the input image. This method is used to remove shadows and specularities from image. All the shadowed regions are grayed out to a uniform color, eliminating soft shadows and specularities and hence creating an illumination invariant signature of the original image.

Active shape model is used to extract features that represent best parameters. It will ask for the region from which the feature extraction is done. If we are satisfied with asked region we say yes and proceed for feature extraction. All the feature extraction is shown in the execution process.

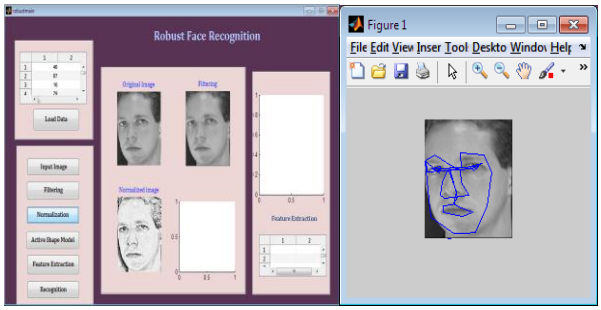

Fig.11 Diagram shows the normalization and the region which we select for feature extraction

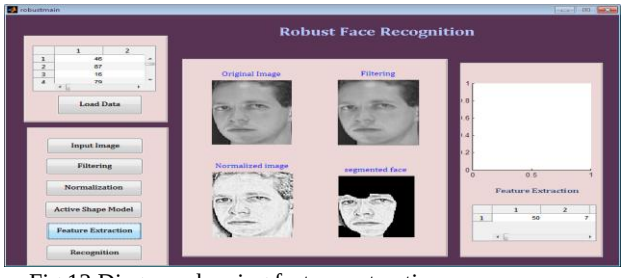

Fig.12 Diagram showing feature extraction process

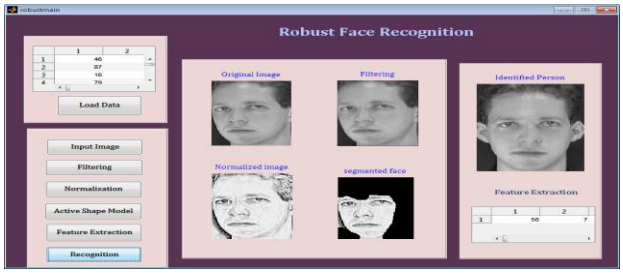

Fig.13 This diagram shows the final step where face sample is identified

CONCLUSION

The study of the vulnerabilities of biometric systems against different types of attacks has been a very active field of research in recent years. This hobby has lead to huge advances in the field of security-improving advancements for Biometric based applications.

For this reason we have considered a highlight space of 25 integral picture quality measures which we have joined with basic classifiers to distinguish genuine and fake access attempts.

The proposed method is able to consistently perform at a high level for different biometric traits ("multi-biometric") and the proposed method is able to adapt to different types of attacks providing for all of them a high level of protection ("multi-attack").

REFERENCES

[1] Anil K. Jain, Fellow, IEEE, Arun Ross, Member, IEEE, "An Introduction to Biometric Recognition", Salil Prabhakar, Member, IEEE.

[2] Khattab M. Ali Alheeti, "Biometric Iris Recognition Based on Hybrid Technique".

[3] Javier Galbally, Arun Ross, Marta Gomez-Barrero, Julian Fierrez, Javier Ortega-Garcia, "Iris image reconstruction from binary templates: An efficient probabilistic approach based on genetic algorithms".

[4] Anil K. Jain, Karthik Nandakumar, and Abhishek Nagar, "Biometric Template Security".

[5] J. Galbally, F. Alonso-Fernandez, J. Fierrez, and J. Ortega-Garcia, "A high performance fingerprint liveness detection method based on quality related features," Future Generat. Comput. Syst., vol. 28, no. 1, pp. 311–321, 2012".

[6] Javier Galbally, Sara Carballo, Julian Fierrez, and Javier Ortega-Garcia, "Vulnerability Assessment of Fingerprint Matching Based on Time Analysis".

[7] Housam Khalifa Bashier, Lau Siong Hoe, Pang Ying Han, Liew Yee Ping and Chiang Mee Li, " Face Spoofing Detection Using Local Graph Structure".

[8] U.L.Sindhu, A.Asha, S.Suganya, M.Vinodha, Karpagam Institute of Technology, " Face Recognition in Online Using Image Processing".

[9] "Face liveness detection using dynamic texture",Tiago de Freitas Pereira1, Jukka Komulainen2, Andre Anjos, Jose Mario De Martino, Abdenour Hadid2, Matti Pietikainen2 and Sebastien Marce.

[10] Battista Biggio, Zahid Akhtar, Giorgio Fumera, Gian Luca Marcialis, and Fabio Roli Department of Electrical and Electronic Engineering, University of Cagliari Piazza d'Armi, 09123 Cagliari, Italy, "Security Evaluation of Biometric Authentication Systems Under Real Spoofing Attacks".

[11] S. Prabhakar, S. Pankanti, and A. K. Jain, "Biometric recognition: Security and privacy concerns," IEEE Security Privacy, vol. 1, no. 2, pp. 33–42, Mar./Apr. 2003.

[12] Pedro Tome, Ruben Vera-Rodriguez, Julian Fierrez, and Javier Ortega-Garcia, "Fusion of Facial Regions using Color Information in a Forensic Scenario".

[13] Biometrics Institute, London, U.K. (2011).Biometric Vulnerability Assessment Expert Group [Online]. Available:http://www.biometricsinstitute.org/pages/biometric-vulnerability-assessment-expertgroup-bvaeg.html

[14] J.Galbally, J. Ortiz-Lopez, J. Fierrez, and J. Ortega-Garcia, "Iris liveness detection based on quality related features," in Proc. 5th IAPR ICB, Mar./Apr. 2012, pp. 271–276.

Preeti R Dubey received the B.E degree in Information Science and Engineering from Visvesvaraya university, Belgaum, Karnataka, India in 2013, now pursuing M. Tech (4^{th} sem) degree in Computer Science and Engineering from Visvesvaraya university, Belgaum, Godutai Engineering College for Women, Gulbarga, Karnataka, India in 2015. 9482337974

Manikamma Malipatil received the B.E degree in Computer Science from Poojya Doddappa appa college of engineering Gulbarga, India in 2010 and M.tech degree in Computer Science from Visvesvaraya university, Poojya Doddappa appa college of engineering Gulbarga, Karnataka, India in 2012.And Working as Asst. Prof in Godutai Engineering College for Women, Gulbarga.

