

FACE RECOGNITION USING PRINCIPAL COMPONENT ANALYSIS AND NEURAL NETWORKS

A. S. SYED NAVAZ¹, T. DHEVI SRI² & PRATAP MAZUMDER³

¹Assitant Professor, Department of Computer Applicatons, Muthayammal College of Arts & Science, Namakkal, India

^{2,3}Muthayammal College of Arts & Science, Namakkal, India

ABSTRACT

Security and authentication of a person is a crucial part of any industry. There are many techniques used for this purpose. One of them is *face recognition*. Face recognition is an effective means of authenticating a person. The advantage of this approach is that, it enables us to detect changes in the face pattern of an individual to an appreciable extent. The recognition system can tolerate local variations in the face expression of an individual. Hence face recognition can be used as a key factor in crime detection mainly to identify criminals. There are several approaches to face recognition of which Principal Component Analysis (PCA) and Neural Networks have been incorporated in our project. The system consists of a database of a set of facial patterns for each individual. The characteristic features called 'eigenfaces' are extracted from the stored images using which the system is trained for subsequent recognition of new images.

KEYWORDS: Neural Networks, Biometrics, Principal Component Analysis, Eigen Values, Eigen Vector

INTRODUCTION

Security and authentication of a person is a crucial part of any industry. There are many techniques used for these purpose one of them is face recognition. Face recognition is an effective means of authenticating a person the advantage of this approach is that, it enables us to detect changes in the face pattern of an individual to an appreciable extent the recognition system can tolerate local variations in the face expressions of an individual. Hence face recognition can be used as a key factor in crime detection mainly to identify criminals there are several approaches to face recognition of which principal component(PCA) and neural networks have been incorporated in our project face recognition as many applicable areas. Moreover it can be categories into face recognition, face classification, one, or sex determination. The system consist of a database of a set of facial patterns for each individual. The characteristic features called 'eigen faces' are extracted form the storage images using which the system is trained for subsequent recognition of new images.

EXISTING SYSTEM

- Face recognition biometrics is the science of programming a computer to recognize a human face. When a person is enrolled in a face recognition system, a video camera takes a series of snapshots of the face and then represents it by a unique holistic code.
- When someone has their face verified by the computer, it captures their current appearance and compares it with the facial codes already stored in the system.
- the faces match, the person receives authorization; otherwise, the person will not be identified. The existing face recognition system identifies only static face images that almost exactly match with one of the images stored in the database.

- When the current image captured almost exactly matches with one of the images stored then the person is identified and granted access.
- When the current image of a person is considerably different, say, in terms of facial expression from the images of that person which are already stored in the database the system does not recognize the person and hence access will be denied

LIMITATIONS OF THE EXISTING SYSTEM

The existing or traditional face recognition system has some limitations which can be overcome by adopting new methods of face recognition :

- The existing system cannot tolerate variations in the new face image. It requires the new image to be almost exactly matching with one of the images in the database which will otherwise result in denial of access for the individual.
- The performance level of the existing system is not appreciable.

PROPOSED SYSTEM AND ITS ADVANTAGES

The proposed face recognition system overcomes certain limitations of the existing face recognition system. It is based on extracting the dominating features of a set of human faces stored in the database and performing mathematical operations on the values corresponding to them. Hence when a new image is fed into the system for recognition the main features are extracted and computed to find the distance between the input image and the stored images. Thus, some variations in the new face image to be recognized can be tolerated. When the new image of a person differs from the images of that person stored in the database, the system will be able to recognize the new face and identify who the person is.

The proposed system is better mainly due to the use of facial features rather than the entire face. Its advantages are in terms of:

- Recognition accuracy and better discriminatory power Computational cost because smaller images (main features) require less processing to train the PCA.
- because of the use of dominant features and hence can be used as an effective means of authentication

TYPES OF MODULES

The modules are of three types

- Biometrics
- Face Recognition Using Principal Component Analysis (PCA)
- Face Recognition Using Neural Networks

BIOMETRICS

Biometrics refers to the automatic identification of a person based on his/her physiological or behavioral characteristics. This method of identification is preferred over traditional methods involving passwords and PIN numbers for various reasons:

- The person to be identified is required to be physically present at the point-of-identification
- Identification based on biometric techniques obviates the need to remember a password or carry a token.

With the increased use of computers as vehicles of information technology, it is necessary to restrict access to sensitive/personal data. By replacing PINs, biometric techniques can potentially prevent unauthorized access to or fraudulent use of ATMs, cellular phones, smart cards, desktop PCs, workstations, and computer networks. PINs and passwords may be forgotten, and token based methods of identification like passports and driver's licenses may be forged, stolen, or lost. Thus biometric based systems of identification are receiving considerable interest. Various types of biometric systems are being used for real-time identification; the most popular are based on face, iris and fingerprint matching. However, there are other biometric systems that utilize retinal scan, speech, signatures and hand geometry.

A biometric system is essentially a pattern recognition system which makes a personal identification by determining the authenticity of a specific physiological or behavioral characteristic possessed by the user. It is a means of identifying a person by measuring a particular physical or behavioral characteristic and later comparing it to a library of characteristics belonging to many people. An important issue in designing a practical system is to determine how an individual is identified. Depending on the context, a biometric system can be either a verification (authentication) system or an identification system.

Verification vs Identification

There are two different ways to resolve a person's identity: verification and identification. Verification (*Am I whom I claim I am?*) involves confirming or denying a person's *claimed identity*. In identification, one has to establish a person's identity (*Who am I?*). Each one of these approaches has its own complexities and could probably be solved best by a certain biometric system.

Operation and Performance

In a typical IT biometric system, a person registers with the system when one or more of his physical and behavioral characteristics are obtained. This information is then processed by a numerical algorithm, and entered into a database. The algorithm creates a digital representation of the obtained biometric.

If the user is new to the system, he or she enrolls, which means that the digital template of the biometric is entered into the database. Each subsequent attempt to use the system, or authenticate, requires the biometric of the user to be captured again, and processed into a digital template and is known as "live data". That template is then compared to those existing in the database to determine a match. The process of converting the acquired biometric into a digital template for comparison is completed each time the user attempts to authenticate to the system. The comparison process involves the use of a Hamming distance. This is a measurement of how similar two bit strings are. For example, two identical bit strings have a Hamming Distance of zero, while two totally dissimilar ones have a Hamming Distance of one. Thus, the Hamming distance measures the percentage of dissimilar bits out of the number of comparisons made. Ideally, when a user logs in, nearly all of his features match; then when someone else tries to log in, who does not fully match, and the system will not allow the new person to log in. Current technologies have widely varying Equal Error Rates, varying from as low as 60% and as high as 99.9%.

Thus the working of biometric systems can be classified into two stages:

Enrollment Acquiring, encoding and storing the biometric samples (e.g., fingerprints, hand or iris) as reference templates to be used for future comparisons.

Verification or Identification

Comparing the live data and the reference templates forming the database to authenticate the individual.

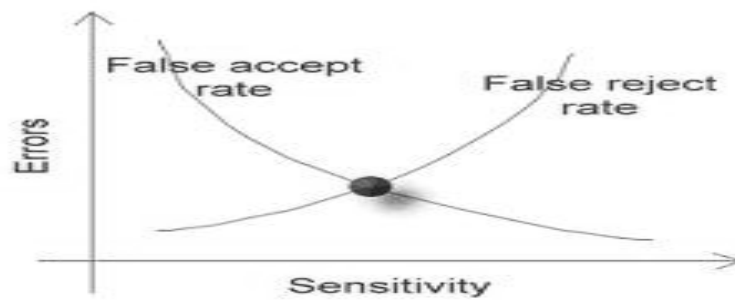


Figure 1 : Performance Metrics of a Biometric System

Performance of a biometric measure as depicted in Figure 1 is usually referred to in terms of the false accept rate (FAR), the false non match or reject rate (FRR), and the failure to enroll rate (FTE or FER). The FAR measures the percent of invalid users who are incorrectly accepted as genuine users, while the FRR measures the percent of valid users who are rejected as impostors. In real-world biometric systems the FAR and FRR can typically be traded off against each other by changing some parameter. One of the most common measures of real-world biometric systems is the rate at which both accept and reject errors are equal: the equal error rate (EER), also known as the cross-over error rate (CER). The lower the EER or CER, the more accurate the system is considered to be.

Claimed error rates sometimes involve idiosyncratic or subjective elements. For example, one biometrics vendor set the acceptance threshold high, to minimize false accepts. In the trial, three attempts were allowed, and so a false reject was counted only if all three attempts failed. At the same time, when measuring performance biometrics (e.g. writing, speech etc.), opinions may differ on what constitutes a false reject. If a signature verification system is trained with an initial and a surname, can a false reject be legitimately claimed when it then rejects the signature incorporating a full first name? Despite these misgivings, biometric systems have the potential to identify individuals with a very high degree of certainty. Forensic DNA evidence enjoys a particularly high degree of public trust at present (ca. 2004) and substantial claims are being made in respect of iris recognition technology, which has the capacity to discriminate between individuals with identical DNA, such as monozygotic twins.

FACE RECOGNITION SYSTEM

A face recognition system has to associate an identity or name for each face it comes across by matching it to a large database of individuals. Automatic face detection and recognition has been a difficult problem in the field of computer vision for several years. Although humans perform the task in an effortless manner, the underlying computations within the human visual system are of tremendous complexity. Furthermore, the ability to find faces visually in a scene and recognize them is critical for humans in their everyday activities. Consequently, the automation of this task would be useful for many applications including security, surveillance, gaze-based control, affective computing, speech recognition assistance, video compression and animation.

Robust face recognition requires the ability to recognize identity despite many variations in appearance that the face can have in a scene. The face is a 3D object which is illuminated from a variety of light sources and surrounded by arbitrary background data (including other faces). Therefore, the appearance a face has when projected onto a 2D image can vary tremendously. A system capable of performing non-contrived recognition need to find and recognize faces despite

these variations. Additionally, face detection and recognition scheme must be capable of tolerating variations in the faces themselves. The human face is not a unique rigid object. There are billions of different faces and each of them can assume a variety of deformations. Inter-personal variations can be due to race, identity, or genetics while intra-personal variations can be due to deformations, expression, aging, facial hair, cosmetics and facial paraphernalia. Furthermore, the output of the detection and recognition system has to be accurate and robust.

The applications of facial recognition range from a static, controlled “mug-shot” verification to a dynamic, uncontrolled face identification in a cluttered background (e.g., airport). The most popular approaches to face recognition are based on either (i) the location and shape of facial attributes, such as the eyes, eyebrows, nose, lips, and chin and their spatial relationships, or (ii) the overall (global) analysis of the face image that represents a face as a weighted combination of a number of canonical faces. While the verification performance of the face recognition systems that are commercially available is reasonable, they impose a number of restrictions on how the facial images are obtained, sometimes requiring a fixed and simple background or special illumination. These systems also have difficulty in recognizing a face from images captured from two drastically different views and under different illumination conditions. The face itself, without any contextual information, is a sufficient basis for recognizing a person from a large number of identities with a high level of confidence. In order that a facial recognition system works well, it should automatically:

- detect and locate the face in the image
- recognize the face from a general viewpoint (i.e., from any pose).

Popular recognition algorithms include Eigenface, Fisher face, the Hidden Markov model and the neuronal motivated Dynamic Link Matching.

The two approaches concentrated on to face recognition are as follows:

Eigenface-Based Face Recognition

In this method the main features of the face are extracted and eigenvectors are formed. The images forming the training set (database) are projected onto the major eigenvectors and the projection values are computed. In the recognition stage the projection value of the input image is also found and the distance from the known projection values is calculated to identify who the individual is.

Neural Network Based Face Recognition

The same procedure is followed for forming the eigenvectors as in the Eigenface approach, which are then fed into the Neural Network Unit to train it on those vectors and the knowledge gained from the training phase is subsequently used for recognizing new input images. The training and recognition phases can be implemented using several neural network models and algorithms.

Uses of Face Recognition System

Face recognition system can be used for:

- Eliminating duplicate IDs
- Verifying identity
- Criminal investigations

Benefits of Face Recognition:

The following are the benefits of using face recognition system:

- Accurate
- Cost-effective
- Non-invasive
- Uses legacy data
- Often is the only suitable biometric
- Built in human back up mechanism

FACE RECOGNITION USING PRINCIPAL COMPONENT ANALYSIS (PCA)

In statistics, **principal components analysis (PCA)** is a technique that can be used to simplify a dataset. It is a linear transformation that chooses a new coordinate system for the data set such that the greatest variance by any projection of the data set comes to lie on the first axis (called the first principal component), the second greatest variance on the second axis, and so on. PCA can be used for reducing dimensionality in a dataset while retaining those characteristics of the dataset that contribute most to its variance, by keeping lower-order principal components and ignoring higher-order ones. The idea is that such low-order components often contain the "most important" aspects of the data.

The task of facial recognition is discriminating input signals (image data) into several classes (persons). The input signals are highly noisy (e.g. the noise is caused by differing lighting conditions, pose etc.), yet the input images are not completely random and in spite of their differences there are patterns which occur in any input signal. Such patterns, which can be observed in all signals could be - in the domain of facial recognition - the presence of some objects (eyes, nose, mouth) in any face as well as relative distances between these objects. These characteristic features are called **eigenfaces** in the facial recognition domain (or **principal components** generally). They can be extracted out of original image data by means of the mathematical tool called *Principal Component Analysis (PCA)*.

By means of PCA one can transform each original image of the training set into a corresponding eigenface. original image. If one uses all the eigenfaces extracted from original images, one can reconstruct the original images from the eigenfaces *exactly*. But one can also use only a part of the eigenfaces. Then the reconstructed image is an approximation of the original image. However, losses due to omitting some of the eigenfaces can be minimized. This happens by choosing only the most important features (eigenfaces). Omission of eigenfaces is necessary due to scarcity of computational resources. Thus the purpose of PCA is to reduce the large dimensionality of the face space (observed variables) to the smaller intrinsic dimensionality of feature space (independent variables), which are needed to describe the data economically. This is the case when there is a strong correlation between observed variables.

To generate a **set of eigenfaces**, a large set of digitized images of human faces, taken under the same lighting conditions, are normalized to line up the eyes and mouths. They are then all resample at the same pixel resolution (say $m \times n$), and then treated as mn -dimensional vectors whose components are the values of their pixels. The eigenvectors of the covariance matrix of the statistical distribution of face image vectors are then extracted. Since the eigenvectors belong to the same vector space as face images, they can be viewed as if they were $m \times n$ pixel face images: hence the name *eigenfaces*. Viewed in this way, the principal eigenface looks like a bland androgynous average human face. Some subsequent eigenfaces can be seen to correspond to generalized features such as left-right and top-bottom asymmetry, or

the presence or lack of a beard. Other eigenfaces are hard to categorize, and look rather strange. When properly weighted, eigenfaces can be summed together to create an approximate gray-scale rendering of a human face. Remarkably few eigenvector terms are needed to give a fair likeness of most people's faces, so eigenfaces provide a means of applying data compression to faces for identification purposes.

It is possible not only to extract the face from eigenfaces given a set of weights, but also to go the opposite way. This opposite way would be to extract the weights from eigenfaces and the face to be recognized. These weights tell nothing less, as the amount by which the face in question differs from "typical" faces represented by the eigenfaces.

Therefore, using this weights one can determine two important things:

- Determine if the image in question is a face at all. In the case the weights of the image differ too much from the weights of face images (i.e. images, from which we know for sure that they are faces) the image probably is not a face.
- Similar faces (images) possess similar features (eigenfaces) to similar degrees (weights). If one extracts weights from all the images available, the images could be grouped to clusters. That is, all images having similar weights are likely to be similar faces.

EIGENVALUES AND EIGENVECTORS

Large matrices can be costly, in terms of computational time, to use. Large matrices may have to be iterated hundreds or thousands of times for a calculation. Additionally, the behavior of matrices would be hard to explore without important mathematical tools. One mathematical tool, which has applications not only for Linear Algebra but for differential equations, calculus, and many other areas, is the concept of *eigenvalues* and *eigenvectors*. The words eigenvalue and eigenvector are derived from the German word "eigen" which means "proper" or "characteristic." An eigenvalue of a square matrix is a scalar that is usually represented by the Greek letter λ and an eigenvector is a non-zero vector denoted by the small letter x . For a given square matrix, A , all eigenvalues and eigenvectors satisfy the equation

$$Ax = \lambda x$$

In other words, an eigenvector of a matrix is a vector such that, if multiplied with the matrix, the result is always an integer multiple of that vector. This integer value is the corresponding eigenvalue of the eigenvector. Let's consider an example.

Let

$$A = \begin{pmatrix} 1 & 2 \\ 0 & -2 \end{pmatrix}$$

and

$$x = \begin{pmatrix} -2 \\ 3 \end{pmatrix}.$$

When x is transformed by A ,

$$Ax = \begin{pmatrix} 4 \\ -6 \end{pmatrix}$$

But what is remarkable is that,

$$A\mathbf{x} = (-2)\begin{pmatrix} -2 \\ 3 \end{pmatrix} = -2\mathbf{x}$$

So when vector \mathbf{x} is operated with matrix A , instead of getting a different vector we get the *same* vector \mathbf{x} multiplied by some constant. The value -2 of the matrix A is its *eigenvalue*, and the vector \mathbf{x} is called the *eigenvector* for the matrix A .

Eigenvectors possess following properties

- They can be determined only for square matrices
- There are n eigenvectors (and corresponding eigenvalues) in a $n \times n$ matrix.
- All eigenvectors are perpendicular, i.e. at right angle with each other.

Since each eigenvector is associated with an eigenvalue, we often refer to an x and λ that correspond to one another as an **eigenpair**. An **eigenspace** is a space consisting of all eigenvectors which have the same eigenvalue. These eigenvectors are derived from the covariance matrix of the probability distribution of the high-dimensional vector space of possible faces of human beings and hence eigenfaces are a set of eigenvectors.

STEPS FOR RECOGNITION USING PCA

The step by step instructions along with the formulas for the recognition of faces using Principal Component Analysis (PCA) are as follows:

STEP 1: Prepare the Data

The first step is to obtain a set S with M face images. Each image is transformed into a vector of size N and placed into the set.

$$S = \{ \Gamma_1, \Gamma_2, \Gamma_3, \dots, \Gamma_M \}$$

STEP 2: Obtain the Mean

After obtaining the set, the mean image Ψ has to be obtained as,

$$\Psi = \frac{1}{M} \sum_{n=1}^M \Gamma_n$$

STEP 3: Subtract the Mean from Original Image

The difference between the input image and the mean image has to be calculated and the result is stored in Φ .

$$\Phi_i = \Gamma_i - \Psi$$

STEP 4: Calculate the Covariance Matrix

The covariance matrix C is calculated in the following manner

$$C = \frac{1}{M} \sum_{n=1}^M \Phi_n \Phi_n^T$$

$$= AA^T$$

$$A = \{ \Phi_1, \Phi_2, \Phi_3, \dots, \Phi_n \}$$

STEP 5: Calculate the Eigenvectors and Eigenvalues of the Covariance Matrix and Select the Principal Components

In this step, the eigenvectors (eigenfaces) u_i and the corresponding eigenvalues λ_i should be calculated. From M eigenvectors, u , only M' should be chosen, which have the highest eigenvalues. The higher the eigenvalue, the more characteristic features of a face does the particular eigenvector describe. Eigenfaces with low eigenvalues can be omitted, as they explain only a small part of the characteristic features of the faces. After M' eigenfaces are determined, the “training” phase of the algorithm is finished. Once the training set has been prepared the next phase is the classification of new input faces. The recognition procedure consists of two major steps:

STEP 1: Transform the New Face

The new face is transformed into its eigenface components and the resulting weights form the weight vectors.

$$\omega_k = \mu_k^T (\Gamma - \Psi)$$

where ω = weight, μ = eigenvector, Γ = new input image, Ψ = mean face

The weight vector Ω^T is given by,

$$\Omega^T = [\omega_1, \omega_2, \dots, \omega_M]$$

FACE RECOGNITION USING NEURAL NETWORKS

An artificial neural network (ANN), also called as simulated neural network (SNN) or commonly just neural network (NN) is an interconnected group of artificial neurons that uses a mathematical or computational model for information processing based on connectionist approach to computation. In most cases an ANN is an adaptive system that changes its structure based on external or internal information that flows through the network. In more practical terms neural networks are non-linear statistical data modeling tools. They can be used to model complex relationships between inputs and outputs or to find patterns in data. The original inspiration of the technique was from the examination of the central nervous system and the neurons. In a neural network model, simple nodes (called variously “neurons”, “neuroses”, “processing elements”, or units) are connected together to form a network of nodes- hence the term neural network. While a neural network does not have to be adaptive, its practical use comes with algorithms designed to alter the strengths (weights) of the connections in the network to produce a desired signal flow. These networks are also similar to the biological neural networks in the sense that the functions are performed collectively and in parallel by the units, rather than there being a clear delineation of sub-tasks to which various units are assigned.

Neural network models in artificial intelligence are usually referred to as artificial neural networks (ANNs); these are essentially simple mathematical models defining a function $f: X \rightarrow Y$. Each type of ANN model corresponds to a *class*

of such functions. The word *network* in the term 'artificial neural network' arises because the function $f(x)$ is defined as a composition of other functions $g_i(x)$, which can further be defined as a composition of other functions. This can be conveniently represented as a network structure, with arrows depicting the dependencies between variables. A widely used type of composition is the *nonlinear weighted sum*, where $f(x) = K(\sum w_i g_i(x))$, where K is some predefined function, such as the hyperbolic tangent. convenient for the following to refer to a collection of functions g_i as simply a vector $g = (g_1, g_2, \dots, g_n)$. Two views can be put in the form of graphs, the functional view and probabilistic view.

However interesting such functions may be in themselves, what has attracted the most interest in neural networks is the possibility of *learning*, which in practice means the following:

Given a specific *task* to solve, and a *class* of functions F , learning means using a set of *observations*, in order to find $f^* \in F$ which solves the task in an *optimal sense*. This entails defining a cost function such that, for the optimal solution f^* ,

$$C(f^*) \leq C(f) \forall f \in F$$

The cost function C is an important concept in learning, as it is a measure of how far away we are from an optimal solution to the problem that we want to solve. Learning algorithms search through the solution space in order to find a function that has the smallest possible cost. For applications where the solution is dependent on some data, the cost must necessarily be a *function of the observations*, otherwise we would not be modeling anything related to the data. It is frequently defined as a statistic to which only approximations can be made. As a simple example consider the problem of finding the model f which minimizes $C = E[|f(x) - y|^2]$, for data pairs (x, y) drawn from some distribution D . In practical situations we would only have N samples from D and thus, for the above example, we would only minimize C . Thus, the cost is minimized over a sample of the data rather than the true data distribution.

CONCLUSIONS

Thus the proposed face recognition system based on PCA has been implemented. It accurately identifies input face images of an individual which differ from the set of images of that person already stored in the database thus serving as an effective method of recognizing new face images. The base code for training face images using Back Propagation Neural Network has also been completed. Hence when a new image is fed into the system for recognition the main features are extracted and computed to find the distance between the input image and the stored images.

Thus, some variations in the new face image to be recognized can be tolerated. When the new image of a person differs from the images of that person stored in the database, the system will be able to recognize the new face and identify who the person is. Recognition accuracy and better discriminatory power Computational cost because smaller images (main features) require less processing to train the PCA. Because of the use of dominant features and hence can be used as an effective means of authentication.

REFERENCES

1. Limun Fu, 'Neural Networks in Computer Intelligence', Tata McGraw Hill, 2003
2. Rafael C Gonzalez, Richard E Woods and Steven L Eddins, 'Digital Image Processing Using Matlab', Prentice Hall, 2004
3. http://www.hrsLtd.com/identification_technology/biometrics.htm
4. <http://cnx.org/content/m12534/latest/>

5. http://dapissarenko.com/resources/2003_02_06_eigenfacesDocHtml/html/index.html
6. <http://www.dacs.dtic.mil/techs/neural/neural2.html>
7. http://en.wikipedia.org/wiki/Artificial_neural_network
8. http://www.mathworks.com/company/events/archived_webinars.html?sec=imageprocessing
9. "Principal component analysis" submitted by . J. Hightower, and G. Borriello, IEEE Computer, August 2007 (also in IEEE Special Report "Trends Technologies & Applications in Mobile Computing").
10. James A. Senn, "The information technology digest", IEEE Computer Magazine, Vol. 33, No 12, December 2007.

AUTHOR'S DETAILS



A.S.Syed Navaz received BBA from Annamalai University, Chidambaram 2006, M.Sc Information Technology from KSR College of Technology, Anna University Coimbatore 2009, M.Phil in Computer Science from Prist University, Thanjavur 2010 and M.C.A from Periyar University, Salem 2010. Currently he is working as an Asst.Professor in the Department of Computer Applications, Muthayammal College of Arts & Science, Namakkal. His area of interests are Wireless Communications, Computer Networks and Mobile Communications.



T.Dhevi Sri, Pursuing her Bachelor's in Computer Applications, Muthayammal College of Arts & Science, Periyar University, Namakkal, India. Her area of interests are Computer Networks.



Pratap Mazumder, Pursuing his Bachelor's in Computer Applications, Muthayammal College of Arts & Science, Periyar University, Namakkal, India. His area of interests are Computer Networks.

