Quest Journals
Journal of Electronics and Communication Engineering Research
Volume 7 ~ Issue 1 (2021) pp: 05-13
ISSN(Online) : 2321-5941
www.questjournals.org

Research Paper

Face Recognition Technology

Nwogu. U. O.[1], Madu Hilary C.[2], and Kikanme Ronald E.[3]
[1](Department of Electrical Electronics Engineering, Federal Polytechnic Nekede, Owerri Nigeria)
[2](Department of Electrical Electronics Engineering, Federal Polytechnic Nekede, Owerri Nigeria)
[3](Department of Electrical Electronics Engineering, Federal Polytechnic Nekede, Owerri Nigeria)

ABSTRACT: *Face recognition presents a challenging problem in the field of image analysis and computer vision. The security of information is becoming very significant and difficult. Security cameras are presently common in airports, Offices, University, ATM, Bank and in any locations with a security system. Face recognition is a biometric system used to identify or verify a person from a digital image. Face Recognition system is used in security. Face recognition system should be able to automatically detect a face in an image. This involves extracts its features and then recognize it, regardless of lighting, expression, illumination, ageing, transformations (translate, rotate and scale image) and pose, which is a difficult task. This presentation describes the common methods of face recognition technology, its applications with examples and future research directions of face recognition.*

KEYWORDS: Face Recognition, Holistic Matching Methods, Feature-based (structural) Methods, Hybrid Methods

Received 23 Jan, 2021; Revised:04 Feb, 2021; Accepted 07 Feb, 2021 © The author(s) 2021.
Published with open access at www.questjournals.org

I. INTRODUCTION

Face recognition is an important research problem spanning numerous fields and disciplines. This because face recognition, in additional to having numerous practical applications such as bankcard identification, access control, Mug shots searching, security monitoring, and surveillance system, is a fundamental human behavior that is essential for effective communications and interactions among people.

Face recognition technology is used to automatically identify a person through a digital image. Facial recognition is a category of biometric software that maps an individual's facial features mathematically and stores the data as a face print in the database.

A formal method of classifying faces was first proposed, the author proposed collecting facial profiles as curves, finding their norm, and then classifying other profiles by their deviations from the norm. This classification is multi-modal, i.e. resulting in a vector of independent measures that could be compared with other vectors in a database. Progress has advanced to the point that face recognition systems are being demonstrated in real-world settings [2]. The rapid development of face recognition is due to a combination of factors: active development of algorithms, the availability of a large databases of facial images, and a method for evaluating the performance of face recognition algorithms. In the literatures, face recognition problem can be formulated as: given static (still) or video images of a scene, identify or verify one or more persons in the scene by comparing with faces stored in a database. When comparing person verification to face recognition, there are several aspects which differ. First, a client – an authorized user of a personal identification system is assumed to be co-operative and makes an identity claim.

Face recognition is a biometric approach that employs automated methods to verify or recognize the identity of a living person based on his/her physiological characteristics. In general, a biometric identification system makes use of either physiological characteristics (such as a fingerprint, iris pattern, or face) or behavior patterns (such as hand-writing, voice, or key-stroke pattern) to identify a person. Because of human inherent protectiveness of his/her eyes, some people are reluctant to use eye identification systems. Face recognition has the benefit of being a passive, no intrusive system to verify personal identity in a "natural" and friendly way.

*Corresponding Author: Abdalftah Elbori
MODES Department Atilim University Turkey

II. OBJECTIVES

The main objective of this work is to present an overview of face recognition and biometrics technology and their applications in various fields. Face recognition technology is a broad field of study which is applied in so many fields today, as such, this work is limited to the general overview and application of the technology and its modern trends.

III. REVIEW OF RELATED WORKS

In Divyarajsinh, et al., (2013) presented the common methods of face recognition like holistic matching method, feature extraction method and hybrid methods and the applications with examples in their paper titled "Face Recognition Methods & Applications".

Lucas and Helen (2010) in their report titled "Facial Recognition Technology A Survey of Policy and Implementation Issues" developed a socio-political analysis that bridges the technical and social-scientific literatures on Face Recognition Technology and addresses the unique challenges and concerns that attend its development, evaluation, and specific operational uses, contexts, and goals. The report highlighted the potential and limitations of the technology, noting those tasks for which it seems ready for deployment, those areas where performance obstacles may be overcome by future technological developments or sound operating procedures, and still other issues which appear intractable. Its concern with efficacy extends to ethical considerations.

IV. STEPS IN BIOMETRIC PROCEDURE

In general, biometric devices can be explained with a three-step procedure

(1) A sensor takes an observation. The type of sensor and its observation depend on the type of biometric devices used. This observation gives us a "Biometric Signature" of the individual.

(2) A computer algorithm "normalizes" the biometric signature so that it is in the same format (size, resolution, view, etc.) as the signatures on the system's database. The normalization of the biometric signature gives us a "Normalized Signature" of the individual.

(3) a matcher compares the normalized signature with the set(or sub-set) of normalized signatures on the system's data base and provides a "similarity score" that compares the individual's normalized signature with each signature in the database set (or sub-set).

What is then done with the similarity scores depends on the biometric system's application? Face recognition starts with the detection of face patterns in sometimes cluttered scenes, proceeds by normalizing the face images to account for geometrical and illumination changes, possibly using information about the location and appearance of facial landmarks, identifies the faces using appropriate classification algorithms, and post processes the results using model-based schemes and logistic feedback.

V. APPLICATIONS OF FACE RECOGNITION SYSTEM

Law enforcement and justice solutions: Today's law enforcement agencies are looking for innovative technologies to help them stay one step ahead of the world's ever-advancing criminals.

As such, FRS is committed to developing technologies that can make the jobs of the law enforcement officer easier. This includes acclaimed CABS-computerized arrest and booking system and the child base protection, a software solution for global law enforcement agencies to help protect and recover missing and sexually exploited children, particularly as it relates to child pornography.

Child base protection: Child Base is an application that helps protect and recover missing and sexually-exploited children, particularly those children victimized through child abuse images.

Identification solutions: With regards to primary identification documents, (Passports, Driver's licenses, and ID Cards), the use of face recognition for identification programs has several advantages over other biometric technologies. Leverage your existing identification infrastructure. This includes, using existing photo databases and the existing enrollment technology (e.g. cameras and capture stations); and Increase the public's cooperation by using a process (taking a picture of one's face) that is already accepted and expected;

Integrate with terrorist watch lists, including regional, national, and international "most-wanted" databases.

Airport security: Airport and other transportation terminal security is not a new thing. People have long had to pass through metal detectors before they boarded a plane, been subject to questioning by security personnel, and restricted from entering "secure" areas. What has changed, is the vigilance in which these security efforts are being applied.

The use of biometric identification, can enhance security efforts already underway at most airports and other major transportation hubs (seaports, train stations, etc.).
This includes the identification of known terrorists before they get onto an airplane or into a secure location.

Immigration: Most countries do not want to be perceived as being a "weak link" when it comes to accepting immigrants and refugees, particularly if that individual uses the new country as a staging ground for multi-national criminal and terrorist activities. Consequently, governments around the world are examining their immigration policies and procedures.
Biometric technology, particularly face recognition software, can enhance the effectiveness of immigration and customs personnel. After all, to the human eye it is often difficult to determine a person's identity by looking at a photo, especially if the person has aged, is of a different ethnic background, has altered their hair style, shaved their beard, etc. FRS does not have this difficulty.

Financial services: The financial services industry revolves around the concept of security. Yet for the most part, security within the industry is limited to a simple personal identification number (PIN) or password.
Biometrics, particularly face recognition software, can improve the security of the financial services industry, saving the institution time and money both through a reduction of fraud cases and the administration expenses of dealing with forgotten passwords.

Furthermore, biometric-based access control units can safeguard vaults, teller areas, and safety deposit boxes to protect against theft.
The use of biometrics can also ensure that confidential information remains confidential while deterring identity theft, particularly as it relates to ATM terminals and card-not-present e-commerce transactions.

VI. LIMITATIONS OF FACIAL RECOGNITION TECHNOLOGY

Image quality: Image quality affects how well facial-recognition algorithms work. The image quality of scanning video is quite low compared with that of a digital camera. Even high-definition video is, at best, 1080p (progressive scan); usually, it is 720p. These values are equivalent to about 2MP and 0.9MP, respectively, while an inexpensive digital camera attains 15MP. The difference is quite noticeable.

Image size: When a face-detection algorithm finds a face in an image or in a still from a video capture, the relative size of that face compared with the enrolled image size affects how well the face will be recognized. An already small image size, coupled with a target distant from the camera, means that the detected face is only 100 to 200 pixels on a side. Further, having to scan an image for varying face sizes is a processor-intensive activity. Most algorithms allow specification of a face-size range to help eliminate false positives on detection and speed up image processing.

Face angle: The relative angle of the target's face influences the recognition score profoundly. When a face is enrolled in the recognition software, usually multiple angles are used (profile, frontal and 45-degree are common). Anything less than a frontal view affects the algorithm's capability to generate a template for the face. The more direct the image (both enrolled and probe image) and the higher its resolution, the higher the score of any resulting matches.

Processing and storage: Even though high-definition video is quite low in resolution when compared with digital camera images, it still occupies significant amounts of disk space. Processing every frame of video is an enormous undertaking, so usually only a fraction (10 percent to 25 percent) is actually run through a recognition system. To minimize total processing time, agencies can use clusters of computers. However, adding computers involves considerable data transfer over a network, which can be bound by input-output restrictions, further limiting processing speed.

Ironically, humans are vastly superior to technology when it comes to facial recognition. But humans can only look for a few individuals at a time when watching a source video. A computer can compare many individuals against a database of thousands.

As technology improves, higher-definition cameras will become available. Computer networks will be able to move more data, and processors will work faster. Facial-recognition algorithms will be better able to pick out faces from an image and recognize them in a database of enrolled individuals. The simple mechanisms that defeat today's algorithms, such as obscuring parts of the face with sunglasses and masks or changing one's hairstyle, will be easily overcome.

An immediate way to overcome many of these limitations is to change how images are captured. Using checkpoints, for example, requires subjects to line up and funnel through a single point. Cameras can then focus

on each person closely, yielding far more useful frontal, higher-resolution probe images. However, wide-scale implementation increases the number of cameras required.

Evolving biometrics applications are promising. They include not only facial recognition but also gestures, expressions, gait and vascular patterns, as well as iris, retina, palm print, ear print, voice recognition and scent signatures. A combination of modalities is superior because it improves a system's capacity to produce results with a higher degree of confidence. Associated efforts focus on improving capabilities to collect information from a distance where the target is passive and often unknowing.

Clearly, privacy concerns surround this technology and its use. Finding a balance between national security and individuals' privacy rights will be the subject of increasing discussion, especially as technology progresses.

ADVANTAGES AND DISADVANTAGES OF FACIAL RECOGNITION TECHNOLOGY

Facial recognition technology is a fairly new way of identify people who could be dangerous or need to be located. It works by picking faces out of a crowd, obtaining the measurements necessary and comparing it to the images already in its database.

Advantages:

- Can prevent card counters, etc. from entering casinos –Can identify terrorists, criminals, etc. –Can find missing children –Prevents voter fraud –Targets shoppers

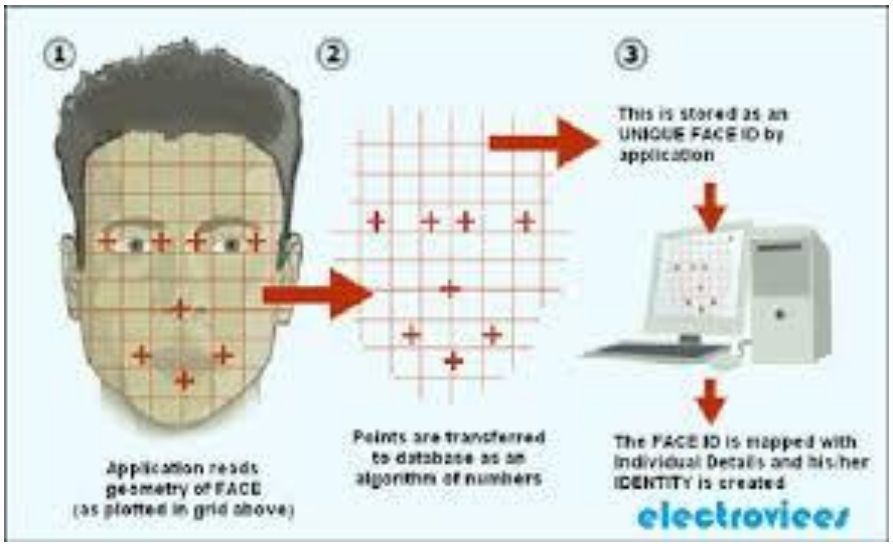
Disadvantages:

-Isn't always accurate –Hindered by glasses, masks, long hair etc. –Must ask users to have a neutral face when pictures are being taken –Considered an invasion of privacy to be watched?

HOW FACE RECOGNITION SYSTEMS WORK

The face recognition system locates the head and finally the eyes of the individual. A matrix is then developed based on the characteristics of the

Individual's face. The method of defining the matrix varies according to the algorithm (the mathematical process used by the computer to perform the comparison). This matrix is then compared to matrices that are in a database and a similarity score is generated for each comparison.



A facial recognition system is a technology capable of identifying or verifying a person from a digital image or a video frame from a video source. There are multiples methods in which facial recognition systems work, but in general, they work by comparing selected facial features from given image with faces within a database.

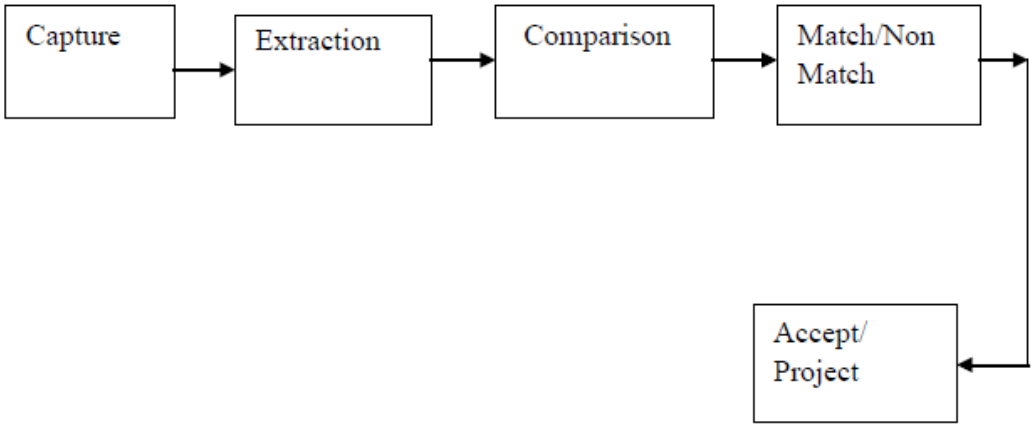
While initially a form of computer application, it has seen wider uses in recent times on mobile platforms and in other forms of technology, such as robotics, Facebook

Artificial intelligence is used to simulate human interpretation of faces. In order to increase the accuracy and adaptability, some kind of machine learning has to be implemented.

There are essentially two methods of capture. One is video imaging and the other is thermal imaging. Video imaging is more common as standard video cameras can be used.

The precise position and the angle of the head and the surrounding lighting conditions may affect the system performance. The complete facial image is usually captured and a number of points on the face can then be mapped, position of the eyes, mouth and the nostrils as a example.

More advanced technologies make 3-D map of the face which multiplies the possible measurements that can be made. Thermal imaging has better accuracy as it uses facial temperature variations caused by vein structure as the distinguishing traits. As the heat pattern is emitted from the face itself without source of external radiation these systems can capture images despite the lighting condition, even in the dark. The drawback is high cost. They are more expensive than standard video cameras.

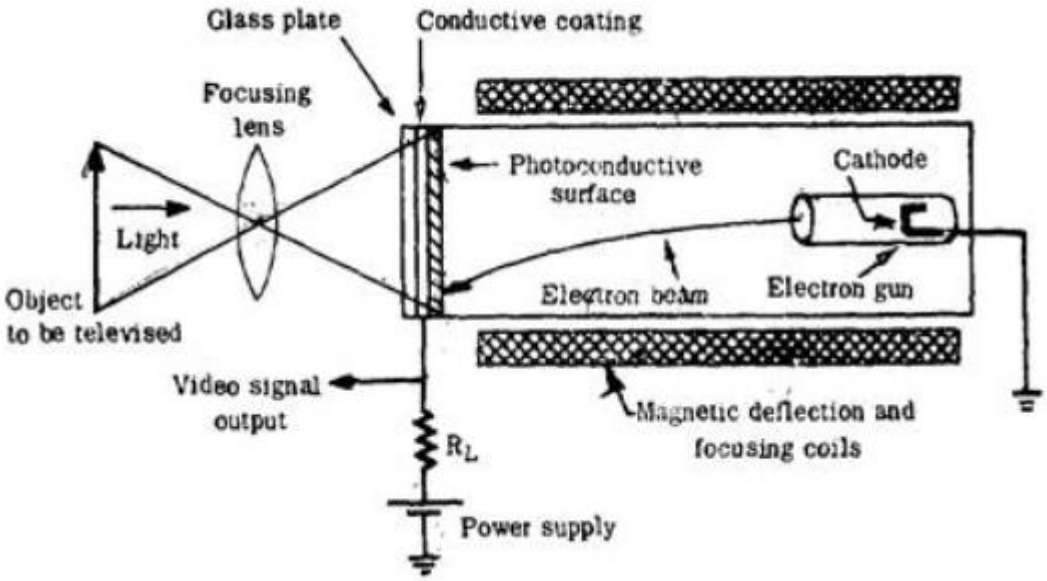


CAPTURING OF IMAGE BY STANDARD VIDEO CAMERAS

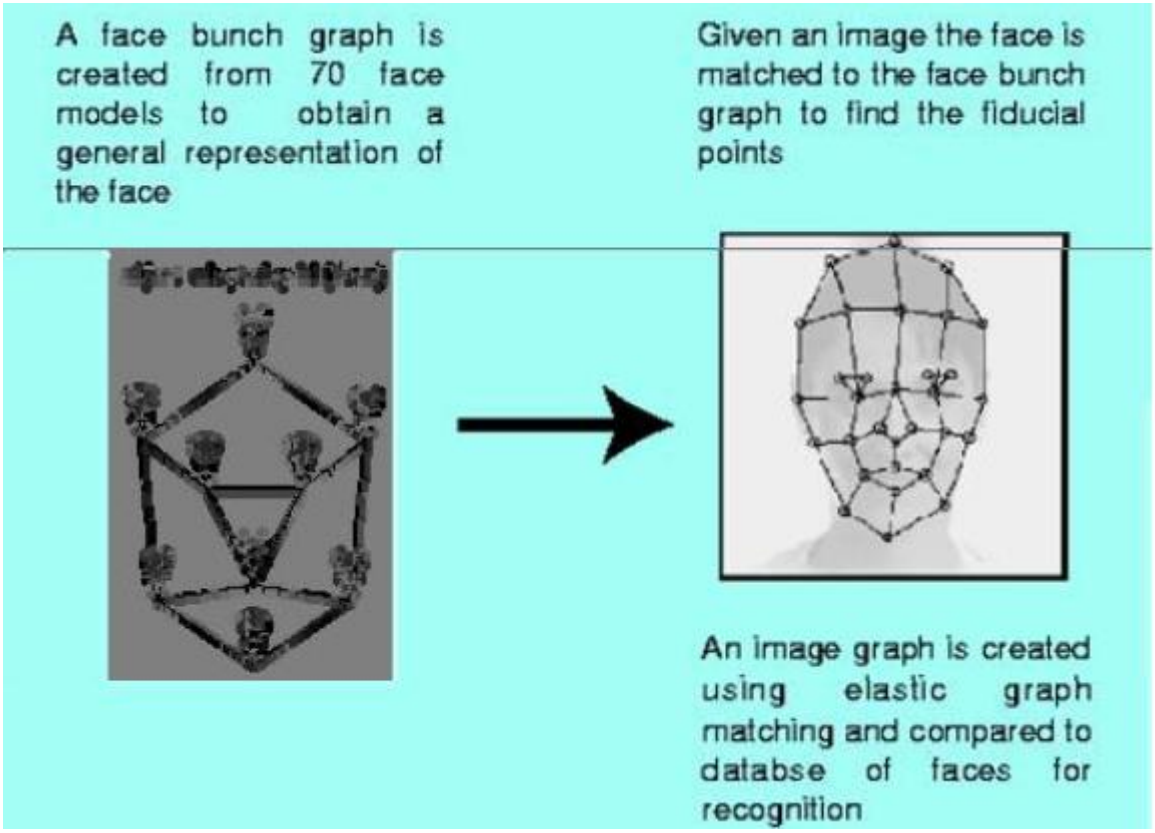
The image is optical in characteristics and may be thought of as a collection of a large number of bright and dark areas representing the picture details. At an instant there will be large number of picture details existing simultaneously each representing the level of brightness of the scene to be reproduced. In other words the picture information is a function of two variables: time and space. Therefore it would require infinite number of channels to transmit optical information corresponding to picture elements simultaneously. There is practical difficulty in transmitting all information simultaneously so we use a method called scanning.

Here the conversion of optical information to electrical form and its transmission is carried out element by element one at a time in a sequential manner to cover the entire image. A TV camera converts optical information into electrical information, the amplitude of which varies in accordance with variation of brightness. An optical image of the scene to be transmitted is focused by lenses assembly on the rectangular glass plate of the camera tube. The inner side of this has a transparent coating on which is laid a very thin layer of photoconductive material. The photo layer has very high resistance when no light is falling on it but decreases depending on the intensity of light falling on it. An electron beam is formed by an electron gun in the TV camera tube. This beam is used to pick up the picture information now available on the target plate of varying resistance at each point.

The electron beam is deflected by a pair of deflecting coils mounted on the glass envelope and kept mutually perpendicular to each other to achieve scanning of the entire target area. The deflecting coils are fed separately from two sweep oscillators, each operating at different frequencies. The magnetic deflection caused by current in one coil gives horizontal motion to the beam from left to right at a uniform rate and brings it back to the left side to commence the trace of the next line. The other coil is used to deflect the beam from top to bottom.



As the beam moves from element to element it encounters different resistance across the target plate depending on the resistance of the photoconductive coating. The result is flow of current which varies in magnitude as elements are scanned. The current passes through the load resistance Rl connected to conductive coating on one side of the DC supply source on the other. Depending on the magnitude of current a varying voltage appears across the resistance Rl and this corresponds to the optical information of the picture.



These nodal points are measured to create a numerical code, a string of numbers that represents a face in the database. This code is called face print. Only 14 to 22 nodal points are needed for faceit software to complete the recognition process.

SOFTWARE

Facial recognition software falls into a larger group of technologies known as biometrics. Facial recognition methods may vary, but they generally involve a series of steps that serve to capture, analyze and compare your face to a database of stored images. Here is the basic process that is used by the Faceit system to capture and compare images:

Detection

When the system is attached to a video surveillance system, the recognition software searches the field of view of a video camera for faces. If there is a face in the view, it is detected within a fraction of a second. A multi-scale algorithm is used to search for faces in low resolution. (An algorithm is a program that provides a set of instructions to accomplish a specific task). The system switches to a high-resolution search only after a head-like shape is detected.

Alignment

Once a face is detected, the system determines the head's position, size and pose. A face needs to be turned at least 35 degrees toward the camera for the system to register it.

Normalization

The image of the head is scaled and rotated so that it can be registered and mapped into an appropriate size and pose. Normalization is performed regardless of the head's location and distance from the camera. Light does not impact the normalization process.

Representation

The system translates the facial data into a unique code. This coding process allows for easier comparison of the newly acquired facial data to stored facial data.

Matching

The newly acquired facial data is compared to the stored data and (ideally) linked to at least one stored facial representation. The heart of the FaceIt facial recognition system is the Local Feature Analysis (LFA) algorithm. This is the mathematical technique the system uses to encode faces. The system maps the face and creates a face print, a unique numerical code for that face. Once the system has stored a face print, it can compare it to the thousands or millions of face prints stored in a database. Each face print is stored as an 84-byte file. Using facial recognition software, police can zoom in with cameras and take a snapshot of a face.

The system can match multiple face prints at a rate of 60 million per minute from memory or 15 million per minute from hard disk. As comparisons are made, the system assigns a value to the comparison using a scale of one to 10. If a score is above a

Predetermined threshold, a match is declared. The operator then views the two photos that have been declared a match to be certain that the computer is accurate.

VII. CONCLUSION

Face recognition technologies have been associated generally with very costly top secure applications. Today the core technologies have evolved and the cost of equipments is going down dramatically due to the intergration and the increasing processing power. Certain applications of face recognition technology are now cost effective, reliable and highly accurate. As a result there are no technological or financial barriers for stepping from the pilot project to widespread deployment.

.

REFERENCES

[1]. A. Nigam, P. Gupta, "A New Distance Measure for Face Recognition System", 2009 Fifth International Conference on Image and Graphics

[2]. C. A. Hansen, "Face Recognition", Institute for Computer Science University of Tromso, Norway.

[3]. C. Gonzalez, R. E. Woods, S. liddins, "Digital Image processing Using MATLAB".

[4]. E. A. Abusham, A. T. B. Jin, W. E. Kiong, "Face Recognition Based on Nonlinear Feature Approach", American Journal of Applied Sciences, 2008.

[5]. M. A. Turk and A. P. Pentland, "Face Recognition Using Eigenfaces", 1991.

[6]. M. D. Kelly. Visual identification of people by computer. PhD thesis, Stanford University, Stanford, CA, USA, 1971.

[7]. R. Jafri, H. R. Arabnia, "A Survey of Face Recognition Techniques", Journal of Information Processing Systems, Vol.5, No.2, June 2009.

[8]. S. Asadi, Dr. D. V. Subba R. V. Saikrishna, "A Comparative study of Face Recognition with PCA and Cross-Correlation Technique", IJCA(0975-8887), Volume 10- No.8, November 2010.

[9]. S. Suhas, A. Kurhe, Dr.P. Khanale, "Face Recognition Using Principal Component Analysis and Linear Discriminant Analysis on Holistic Approach in Facial Images Database", IOSR Journal of Engineering e-ISSN: 2250-3021, p-ISSN: 2278-8719, Vol. 2, Issue 12 (Dec. 2012), ||V4|| PP 15-23

[10]. T. Kanade. Computer Recognition of Human Faces, 47, 1977.

[11]. W. Zhao, R. Chellappa, P. J. Phillips & A. Rosenfeld, "Face recognitions literature survey", ACM Computing Surveys, Vol. 35, No. 4, December 2003, pp. 399–458.