International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 04 Issue: 12 | Dec-2017 www.irjet.net p-ISSN: 2395-0072

3D Face Recognition Technology in Network Security Applications

Meena D. Murumkar[1], Rachit Vijan[2], Aakar Kale[3]

[1]Student, Electronics and Communication Engineering, Usha Mittal Institute of Technology (SNDT University),
[23] Students, Information Technology Engineering, Fr. Conceicao Rodrigues College of Engineering (University of Mumbai), Mumbai, India.

Abstract - *In Data Communications, latest research inclination is towards the security of network information. When classical and modern encryption fails because of lack of uniqueness, biometric information can be used to attain authentication and for the security of confidential data. In this paper, the exploration of relatively new and highly implemented 3D face recognition technology is being analyzed. Several face recognition software uses 3D model, which provides higher accuracies. Some distinctive features of the face are being utilized in the 3D system like depth, curves of nose, chin and eye socket, skin complexion, and many others are extracted, which is usually ignored in the 2D system. 2D face recognition system provides better security if the input is frontal face image. Pitfalls of 2D face recognition system, challenges to 3D face recognition systems, types of face recognition algorithms, Network and other applications will be studied majorly. Some approaches to challenges faced in the 2D system are also discussed in the paper.*

We will discuss merits of the 3D face recognition technology, the relevant work will be reviewed and different recognition algorithms are compared. This includes PCA, DCT, LDA(FLDA) and SVM

***Key Words*: Recognition , Feature Extraction, Detection, Principal Component Analysis (PCA), Linear Discriminant Analysis (LDA),Fisher's LDA (FLDA), Discrete Cosine Transform(DCT), Support Vector Machine (SVM).**

1. INTRODUCTION

Today's network world is securing confidential data requires a strong key. This key should be unaffected by brute force or other kinds of attacks. Thus, biometrics can be a solution for generating secure passwords which can help us combat network and cyber security problems.

Humans often recognize other individuals using their distinctive faces and advancements in the areas of computing capability, image processing, and artificial intelligence has made it possible to enable such recognitions automatically. Thus face recognition is the most implemented biometric technology used for detection and identification of any individual whose face features and other details are already stored in the database. Face recognition is an application of image analysis and it's a challenge to build such system which is capable of recognizing faces just like humans, though humans are quite good in identifying a face they aren't very skilled to deal with large numbers of unknown faces. Thus computers with almost limitless storage and computational speed could overcome human limitations. In brief, face recognition system is a computer which uses the image acquired by any camera, extracts features and recognizes the pattern, lastly matches these characters with the database to determine individual identity.

In face recognition, it is desirable to identify different instances of a face and it should be independent of external factors like illumination conditions, angle, use of cosmetic products, etc and internal factors for eg. facial expressions. The ultimate aim of Face Recognition technology is to find an invariant representation of face insensitive to all these changes. 2D face image can be altered significantly as a result of above factors. Moreover, unlike 2D face image, 3D data carries all the information related to the geometry of the face.[5]

1.1 Biometrics for Network Security

With the internet, comes interconnection and sharing, thus network information security has become essential in past years especially in the field of computer and communication networks. The classical encryption algorithms and other techniques proved a boom in this field, but with time they lost the glory because of being highly suspicious for attacks, also the accuracy of such algorithms is very low. Current encryption techniques, be it public key or private key cryptosystem involves a password or pin which the users are required to store their keys. This methods brings inconvenience to the user and also the pin or passwords recovery involves a lot of time. Also deciphering of user passwords is not a difficult task for hackers, brute force or simple guess works most of the time. Hence a powerful tool is required which can be used as a unique parameter for every individual for his identification. This is done by using biometrics.

Thus, combining biometrics with cryptography for secure communication of confidential data takes place in two steps:

1. Biometric-key release
2. Biometric-key binding

Biometric-key release: When a legitimate user wants to access any digital content, she will offer biometric sample to the system. If it matches successfully then that user's biometric sample with her template will be then used as a unique key.

This key is later used to decrypt the desired content and thus allows the user to access it.

If any illegitimate person attempts to access the same data, his match won't functions as cryptographic key and thus an access would not be granted.

Biometric-key binding: Here only hash of template of any biometric data is stored in the database. This is very similar to the concept of cancellable data. When the hash function is chosen, it is not possible to use biometric template's hash value to extract the original biometric sample. So this doesn't require any template hash database. A secret and trusted bit replacement algorithm can be implemented to hide the cryptographic key of the user's biometric template. Basically no extra storage is required.

Because of the integration of matching and key extraction, it is not an easy procedure for an attacker to release the cryptographic key. But if the biometric smart card is stolen, the person with the card can get an access to the data.

With this key generation protocol mutual authentication is achieved resulting to better network security.

1.2 Two-Dimensional Face Recognition Technology

2D face recognition techniques were very popular in the last decade, is the most advanced biometric parameter during those times. It gives best results when the subject looks towards the camera and a frontal image is captured. Illumination affected the accuracy of this system. If the image of the subject is rotated even for 20 degrees the accuracy of recognition falls lower the threshold value. The depth of face features is an important parameter which is mostly concerned with eye socket, nose inclination, etc for face detection and recognition. We cannot realize depth information and it is simply ignored in a two-dimensional view.

Before recognizing subject's face, the face has to be detected properly in a given image. Face detection is foreclosed by constraining the user. As this system lacks accuracy, most systems use a combination of skin texture and face texture to locate face features and use the image pyramid as a parameter for detecting faces of various sizes. Moreover, systems are developed for improved face detection and are not fully- frontal.

As the past facial recognition programs were fully dependent on two dimension picture to compare it with an image sorted in the database, but this system functions properly only when the subject looks just to the camera. Besides this, 2D face recognition technology is also affected by environmental surrounding the subject like light may change image's view making it difficult for the computer to extract features and match it with corresponding images in the memory. Also, recognition of identity between identical twins was near to impossible with this system. Factors like changes in hairstyle or cosmetic used by the same results in the system failure in face recognition

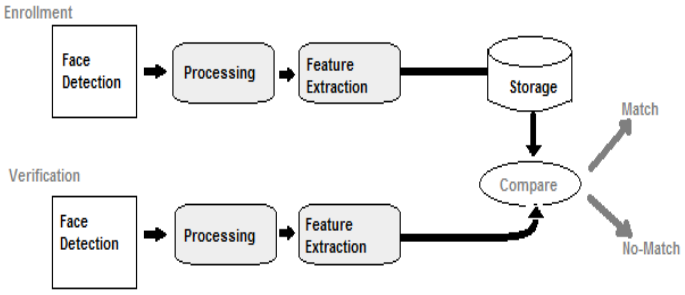

Fig -1: Face Recognition Process

Some of the factors that affect 2D face recognition technology are mentioned below:

1. Pose change
2. Occlusion due to mask, scarf and other kinds of obstacles
3. Illumination change
4. Changes in facial expressions
5. Aging
6. Size of the image
7. Beard or use of accessories like spectacles, etc.
8. Frontal profile of the subject

Many researchers dealt with great diversity in a position of the head, light changes, light intensities which led to failure or lower accuracies of these systems in spite of several improvements in 2D face recognition algorithms. 3D models whereas holds surface information that is used for face detection and subject discrimination.

3D face recognition, unlike this technology, poses invariant. But facial expressions are still a major barrier to recognizing a subject. 2D face recognition technology seems to outperform 3D technology, as it is expected to increase its accuracies by introducing point signatures to describe 3D landmark. Point signatures are used to describe nose, eyes, and forehead. This method has reached a cent percent accuracies when tested on a dataset with six subjects, conducted by Wang et al.

1.3. Three-Dimensional Face Recognition Technology

The new and advanced face recognition technologies are based on 3D patterns, where the images are captured using special cameras. The captures images define three-dimensional views of any subject, by extracting special facial features that remain invariant for example nose shape, the distance between eyes, etc. As these features are invariant that is lighting, make-up etc cannot change the measurements, they are an essential source for any 3D face recognition system. [6]

Three-dimensional face recognition technology has successfully achieved unseen accuracies of the past two-dimensional face recognition technology. The information from the captured face is used to extract distinctive features present on its surface like contour, nose, eye sockets, etc. Hence detection of the face is the primary and very important stage of 3D face recognition technology. Recognition of one face in a crowd is a painstaking procedure. [1]

So one of the important application of image processing is face detection of one particular subject amongst an uncontrolled and complex crowd. Application of this purpose will help us on detection of a particular subject like any individual or any criminal from a crowd, detection of an audience, Robotics, etc. This is where Multiple Face Detection is implemented.

1.4 From 2D to 3D

From two dimensional to three-dimensional recognition technology we have experienced a lot of positive developments. Image processing and artificial intelligence have improved identification. Additional information is now collected on a sub-millimeter basis and depth of curves around nose, chin and eye sockets. Because of these information building of face structure becomes easier which also results in better recognition accuracy.

As three-dimensional modeling is more unaffected by angles or lighting. 3D to 2D conversion is done easily wherever required without any identifiers or key data.
Face recognition along with skin biometrics can increase identification accuracies. In this technique, a patch of the skin is broken into blocks which are measured, then the system distinguishes any pores or lines in the original skin texture. Using this technique, the identification between identical twins becomes possible, where the face recognition technology fails.

2. WORKING OF 3D FACE RECOGNITION SYSTEM

The use of depth and focus of the face that does not affect the change in lighting is known as three-dimensional face recognition system. The software system that relay on three-dimensional technique with a series of steps to eventually be able to perform a face recognition procedure. We can divide the whole process by the following steps. Figure 5.1 also shows these steps:

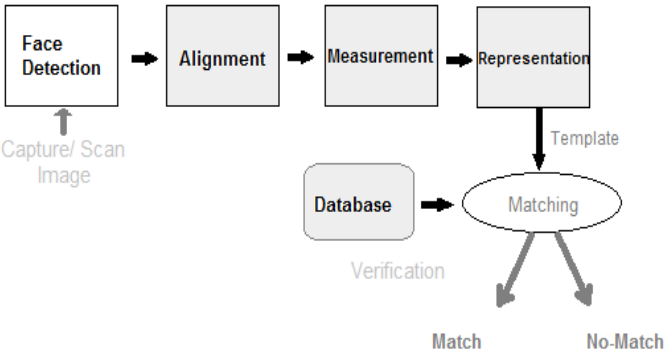

Fig -2: A 3-D Face Recognition system

2.1 Detection

An existing image can be digitally scanned (2D) or a live picture can be acquired by using a video image (3D).
The digital image is captured by a digital camera or any video camera. 3D image is preferably better input to any face recognition technology because they help you determine the depth as this is not provided by the 2D image.

2.2 Alignment

After face detection, this technology determines the position of the head, its size and position angle. Any subject can be recognized up to 90 degrees, but the problem comes with 2D where the subject needs to be turned 35 degrees towards the camera.

2.3 Measurement

Facial curves, eye socket, nose area inclination, face features depth is measured on a sub-millimeter scale, a model or a template is generated.

2.4 Representation

3D face recognition system will translate this model or the generated template into a unique code. This type of coding gives a set of numbers to represent the features on a subject's face.

2.5 Matching

If the picture is three dimensional, the corresponding three-dimensional images present in the database are compared. This comparison is direct and immediate. But the problem arises when the image is two dimensional, as most of the images present in the database are two

dimensional. So the comparison of this image with millions of two-dimensional images in the database is a complicated task. A new technology is used which supports the use of different points called as nodal points to get to know any face in the database.

2.6 Verification

The programs will compare the images in the process of recognition and match them with pictures presented in the database.

With the aim of verifying the result of the matching stage, the 3D face recognition system compares the subject's face with all images presented in the database and then results are displayed mostly in percentages.

3. STUDY OF DIFFERENT ALGORITHMS FOR FACE RECOGNITION

Data compression is very important for computer signal processing. Linear transformation is an important part in signal and image processing areas.

A mathematical operation called transform is applied to a signal that is processed converting in different domain and they are converted back into the original domain [3]

3.1 Principal Component Analysis

The Principal Component Analysis is a highly implemented mathematical procedure in which dimensionality is reduced by extracting the principal components of the multi-dimensional information. The principal component is the linear combination of original dimensions with the highest variability. The nth principal component is the linear combination with max variability since it is orthogonal to n-1 principal components. The highest variance is recorded in the first co-ordinate.

It's advantages are because of its easy implementation, insensitivity for small changes and speed The PCA method which is used the most in face recognition is the "eigenface" approach. This approach transforms faces into "small faces", i.e small sets of characteristics, eigenfaces, which are the main components of the initial set of learning images (training set). Face Recognition is mainly done by projecting the new acquired image in the eigenface subspace, after which the person is classified by comparing its position in eigenface space with the position of known individuals. The advantage of this approach over other face recognition systems is in its simplicity, speed and insensitivity to small or gradual changes on the face. The problem is limited to files that can be used to recognize the face. Namely, the images must be vertical frontal views of human faces. The whole recognition process involves just two steps:. Initialization process and Recognition process.

3.2 Discrete Cosine Transform

The Discrete Cosine Transform produces a sequence of data points in terms of sum of cosine functions which are oscillated at different frequencies. Strong energy compaction properties are possessed by such technique. They are used for data compression. It allows effective reduction in dimensionality, thus the images are transformed by compacting the variations. The DCT uses only real numbers and it is based on Fourier Discrete Transform.[3]

Discrete cosine transform is a powerful transform to extract proper features for face recognition. After applying DCT to the entire face images, some of the coefficients are selected to construct feature vectors. In some cases, the low-frequency coefficients are discarded in order to compensate illumination variations. Since the discrimination power of all the coefficients is not the same and some of them are discriminant than others, so we can achieve a higher true recognition rate by using discriminant coefficients (DCs) as feature vectors. Discrimination power analysis (DPA) is a statistical analysis based on the DCT coefficients properties and discrimination concept. It searches for the coefficients which have more power to discriminate different classes better than others. The proposed approach, against the conventional approaches, is data-dependent and is able to find DCs on each database.

3.3 Linear Discriminant Analysis

Linear Discriminant Analysis preserves class separability. It is used to find linear combination of features. It is highly implemented because it doesn't demands for class differences. It requires data points for different classes to be placed far away from each other. Consequently, LDA results in a differences projection vectors for every individual classes.

Fisher's LDA is used as pattern recognition and machine learning algorithm. Here linear combination are characterized that means the classes are seperated. The result of this combination is used as linear classifier, or for dimensionality reduction.

Linear discriminant analysis (LDA) is a generalization of Fisher's linear discriminant, a method used in statistical, pattern recognition and machine learning to find a linear combination of features that characterizes or separates two or more classes of objects or events. The resulting combination may be used as a linear classifier, or, more commonly, for dimensionality reduction before later classification. [2]

LDA is closely related to analysis of variance (ANOVA) and regression analysis, which also attempt to express one dependent variable as a linear combination of other

features or measurements. However, ANOVA uses categorical independent variables and a continuous dependent variable, whereas discriminant analysis has continuous independent variables and a categorical dependent variable (i.e. the class label). Logistic regression and probit regression are more similar to LDA than ANOVA is, as they also explain a categorical variable by the values of continuous independent variables. These other methods are preferable in applications where it is not reasonable to assume that the independent variables are normally distributed, which is a fundamental assumption of the LDA method.[2]

3.4 Support Vector Machine

Support Vector Machine as a face recognition algorithm is formulated considering the difference space which represents the dissimilarities between facial images of the same person.

The interpretation criteria of the selected surface is modified by SVM. A similarity metric can thus be generated to check for similar features on the face.

SVM uses binary classification system. It is basically the reformulation and reinterpretation of the output of SVM classifier.

4. APPLICATIONS

4.1 Network Security

The application of face recognition for network information security is major to solve a number of shortcomings of the information security password system. With the internet expanding, sharing and interconnection increasing, the network information security has become an important direction in the field of computer networks and telecommunications networks in current domestic and foreign regions. [4]

Till now, encryption methods are mostly employed to solve the issue of information security. But however, the current encryption systems, whether the private key system or public key systems require the user to securely store their keys and the general key to protecting it's user's passwords. There are two main disadvantages of using this type of encryption system:-

It is difficult to remember such passwords and will bring a lot of inconvenience and trouble when forgotten.
Passwords are easily deciphered by hackers through various methods. Thus a lot of resources are wasted to secure such passwords from these attacks by hackers.

Face recognition technology is used ubiquitously, the fusion of facial distinctiveness, stability etc. The original images are segmented into four different regions, which are also called sub-images. Then the famous FLDA method is directly used for the sub-images obtained from the previous step, which the new criterion evaluated the quality of an image by encouraging inner region smoothness and inter-region contrast.

4.2 Business Intelligence

3D face recognition systems for security applications is a mainstream, it can play an important role when applied for performing business intelligence. If a person who is a frequent user of some service approaches the front desk, where the cameras placed on it recognizes him and displays his usual preferences, this will reflect that business knows how to customize the experience for that user. Matching faces after recognition of customers to a known database will allow hotels, banks, retailers, and casinos will allow customer identification to check for their eligibility for VIP treatment, or to know their past records may help these businesses to keep a track from their service.

3D face recognition technology being an automated system can be a powerful business intelligence tool, by collecting and tracking customer behavioral patterns and customer demographics, for eg. Analyzing sales record according to female or male purchases, by age groups or by regions. Thus artificial intelligence adds the additional feature to 3D face recognition system.

This is how facial recognition technology can be used in marketing and business intelligence. Anyone can use the efficiency of this system and thus can bring face recognition system in any type of environments and not only for super high-security applications.

4.3 Security-critical environments

3D face recognition technology because of its highly efficient qualities can be used in such environments where high security is must like for eg. Airports, Government Access control, Border control areas and others. Fast and accurate 3D face recognition systems can be used to determine illegal aliens, to determine known criminals and many other implementations thus making management of any city easier.

It can be implemented in a hospital for keeping proper health records of every patient thus maintaining the confidentiality because of no human involvement. It can serve as an effective tool for predicting consequences of any particular medication by tracking past medical history, thus being more advanced and accurate with fewer errors because of less human interaction.

4.4 Social or e-commerce websites

Automatic login, auto-tagging, preferred services, recommendations and other interesting features can be added to any social platform if 3D face recognition is implemented. Thus recognition of valid user can be acquired, using a web cam or any other image capturing device. Users or the authority behind such websites will also be able to view images of fake users or any unauthorized attempts of access by anyone.

5. CONCLUSION

The paper presented here features biometric as a network security element. Face recognition along with skin analysis provides better accuracy as illumination and other environmental effects don't affect skin analysis technique.

2-D face recognition system was recently improvised and emerged to be the more accurate 3-D face recognition system. 3-D face scans can prove to be an eminent parameter for providing access to confidential data, thus contributing to network and cyber security. Different approaches and algorithms are discussed, different algorithms are used depending on specific applications. Fisher's LDA is more suited for Network security applications. PCA is less affected to illumination and pose, so by the consideration of all pixel value of an image as a feature vector, better representation of the image is seen but the complexity of this technique is higher compared to others. Along with the accuracy, the complexities associated with 3D face recognition technology are also increased.

Many areas other than just security can witness the power of this system when Artificial Intelligence is introduced along with image processing.

REFERENCES

[1] Rashmi S Nair, Preeja Priji, "A Survey on Multiple Face Detection and Tracking in Crowds", International Journal of Innovations in Engineering and Technology (IJIET), Volume 7 Issue 4 December 2016

[2] http://trymachinelearning.com/machine-learning-algorithms/dimensionality-reduction/linear-discriminant-analysis/

[3] N. Ahmed, T. Natarajan, and K. R. Rao." Discrete cosine transform", IEEE Transactions on Computers, 23:90–93, 1974

[4] Liying Lang, Yue Hong, "The application of face recognition", Internal Conference on Computational Intelligence and Security, 978-0-7695-3508-1/08©IEEE

[5] Abhijit Bhandari "3D Face Recognition" Department of Electronics Engineering Sardar Patel Institute of Technology

[6] Bayan Ali Saad Al-Ghamdi & Sumayyah Redhwan Allaam "Recognition of Human Face by "Face Recognition System using 3D" Journal of Information & Communication Technology Vol. 4, No. 2, 27-34

BIOGRAPHIES

Meena Murumkar
B.Tech (Electronics and Communication Engineering)
Usha Mittal Institute of Tech.

Rachit Vijan
B.E. (Information Technology),
Fr.Conceicao Rodrigues College of Engineering

Aakar Kale
B.E. (Information Technology),
Fr.Conceicao Rodrigues College of Engineering