A REVIEW ON FACE IDENTIFICATIONS SYSTEM USING FUSION METHOD

Bhagya Arora*, Er. Sushil Kamboj
SUSGOI, Tangori
susbhagyaarora@gmail.com*, er.kamboj@gmail.com

ABSTRACT

Biometrics is used in the process of authentication of a person by verifying or identifying that a user requesting a network resource is who he, she, or it claims to be, and vice versa. It uses the property that a human trait associated with a person itself like structure of finger, face details etc. By comparing the existing data with the incoming data we can verify the identity of a particular person. There are many types of biometric system like fingerprint recognition, face detection and recognition, iris recognition etc., these traits are used for human identification in surveillance system, criminal identification. Face is a complex multidimensional structure and needs good computing techniques for recognition. The face is our primary and first focus of attention in social life playing an important role in identity of individual. In this paper, we are proposing the fusion techniques for face identification system and compare it with Gaussian model and 2D Histogram. Also analyze the performance of the system using various performance parameters such as recognition rate, accuracy, true positive rate, and false negative rate.

Keywords: Gaussian model, Accuracy, Fusion method, Histogram, Face Detection

I. INTRODUCTION

Face recognition is a task so common to humans, that the individual does not even notice the extensive number of times it is performed every day. Although research in automated face recognition has been conducted since the 1960’s, it has only recently caught the attention of the scientific community. Many face analysis and face modeling techniques have progressed significantly in the last decade [3]. However, face recognition is still an area of active research since a completely successful approach or model has not been proposed to solve the face recognition problem. The inadequacy of automated face recognition systems is especially apparent when compared to our own innate face recognition ability. We perform face recognition, an extremely complex visual task, almost instantaneously and our own recognition ability is far more robust than any computer’s can hope to be. We can recognize a familiar individual under very adverse lighting conditions, from varying angles or view points. Scaling differences (a face being near or far away), different backgrounds do not affect our ability to recognize faces and we can even recognize individuals with just a
fraction of their face visible or even after several years have passed. Furthermore, we are able to recognize the faces of several thousand individuals whom we have met during our lifetime.

1.1 Face detection

The problem of face recognition is all about face detection. This is a fact that seems quite bizarre to new researchers in this area. However, before face recognition is possible, one must be able to reliably find a face and its landmarks. This is essentially a segmentation problem and in practical systems, most of the effort goes into solving this task. In fact the actual recognition based on features extracted from these facial landmarks is only a minor last step. Face is a complex multidimensional structure and needs good computing techniques for recognition. The face is our primary and first focus of attention in social life playing an important role in identity of individual. We can recognize a number of faces learned throughout our lifespan and identify that faces at a glance even after years. There may be variations in faces due to aging and distractions

There are two types of face detection problems:

1) Face detection in images and
2) Real-time face detection

In general, face recognition techniques can be divided into two groups based on the face representation they use appearance-based, which uses holistic texture features and is applied to either whole-face or specific regions in a face image and feature-based, which uses geometric facial features (mouth, eyes, brows, cheeks etc), and geometric relationships between them.

Most of the current face recognition systems presume that faces are readily available for processing. However in reality we do not get images with just faces. So there is a need of a system, which will detect, locate and segregate faces in cluttered images, so that these segregated Faces can be given as input to face recognition systems. The general face detection system consists of three steps. The first step is to classify each pixel in the given image as a skin pixel or a non-skin pixel. The second step is to identify different skin Regions in the skin detected image by using connectivity analysis. The last step is to decide whether each of the skin regions identified is a face or not. This is done using two parameters. They are the height to width ratio of the skin region and the percentage of skin in the rectangle defined by the height and width.

1.2 Face Recognition Tasks

The three primary face recognition tasks are:

- Verification (authentication) - Am I who I say I am? (one to one search)
- Identification (recognition) - Who am I? (one to many search)
- Watch list - Are you looking for me? (one to few search)
Different schemes are to be applied to test the three tasks described above. Which scheme to use depends on the nature of the application?

**Verification:** The verification task is aimed at applications requiring user interaction in the form of an identity claim, i.e. access applications. The verification test is conducted by dividing persons into two groups:

- Clients, people trying to gain access using their own identity.
- Imposters, people trying to gain access using a false identity, i.e. an identity known to the system but not belonging to them.
- The percentage of imposters gaining access is reported as the False Acceptance

**Identification:** The identification task is mostly aimed at applications not requiring user interaction, i.e. surveillance applications. The identification test works from the assumption that all faces in the test are of known persons. The percentage of correct identifications is then reported as the Correct Identification Rate (CIR) or the percentage of false identifications is reported as the False Identification Rate (FIR).

**Watch List:** The watch list task is a generalization of the identification task which includes unknown people. The watch list test is like the identification test reported in CIR or FIR, but can have FAR and FRR associated with it to describe the sensitivity of the watch list, meaning how often is an unknown classified as a person in the watch list (FAR).

### 1.3 Applications of Face Recognition System

It has become one of the most active research areas especially in recent years as it has a variety of wide applications in the areas:

- Public security
- Law enforcement and commerce
- Credit card verification
- Criminal identification
- Access control
- Human-computer intelligent interaction
- Digital libraries and information security.

Face recognition is applied as **access control point**, to obtain the permission for the particular services like entering into a building, strong rooms/bank lockers etc. In this kind of a system, the image of a person is taken by the camera positioned appropriately at a place called the access point and the captured image is matched against the stored face database of the same person. If a match is found, only then the access is permitted i.e. the door is opened. Now days, face recognition is being applied in a number of **surveillance** tasks like voter identity, issuance of driving licenses, security measure in military areas, government offices,
entry to examinations, ATM’s etc. Properly designed systems installed at airports, multiplexes, and other public places, can detect the presence of criminals in the crowd. Other biometrics like fingerprints, iris, and speech recognition cannot perform this kind of mass scanning. To allow **secure transactions on internet**, instead of using passwords or PIN numbers the face verification may be used. Through this tool the secure transactions can be formulated in e-commerce or m-commerce, online banking, access to networks and other personal facilities such as e-health or e-learning. This concept can also be applied to personal computers by using a webcam to capture a digital image of the individual. The captured face image could replace the password as a means to **log-in**.

Face recognition technology is also useful for a number of commercial applications like day-care facilities for picking up the children, search for missing children or runaways, card counters in gaming industry, residential security, benefit payments, recording of students attendance etc. Face recognition systems are no longer limited to the identity verification and surveillance tasks alone. Several tools have started utilizing the face recognition technology to realize the human intentions, actions and behavior for designing future smart environments. For example, a smart home is able to recognize its owner, his family, friends and guests and also able to remember the preferences of the owner and his family. It may be able even to understand what are they asking and looking for. Different gestures and expressions may also be interpreted by it and as such this system is likely to be able to facilitate them. The face recognition technology has become an essential tool in the development of these kinds of intelligent applications.

![Block Diagram of Face Recognition System](image_url)

**Figure 1.1: Block Diagram of Face Recognition System**

Face recognition is one of the few biometric methods that possess the merits of both high accuracy and low intrusiveness. It has the accuracy of a physiological approach without being intrusive. For this reason, since
the early 70’s, face recognition has drawn the attention of researchers in fields from security, psychology, and image processing, to computer vision. Numerous algorithms have been proposed for face recognition; while network security and access control are the most widely discussed applications, face recognition has also proven useful in other multimedia information processing areas. Face recognition [1] techniques can be used to browse video database to find out shots of particular people. Also for face images with a compact parameterized facial model for low bandwidth communication applications such as videophone and teleconferencing. Recently, as the technology has matured, commercial products have appeared on the market. Despite the commercial success of those face recognition products, a few research issues remain to be explored.

1.4 Challenges in the Field of Face Recognition

The challenges associated with face recognition can be attributed to the following factors:

- Presence or absence of structural components: Facial features such as beards, mustaches, and glasses may or may not be present and there is a great deal of variability among these components including shape, color and size.
- Pose: The images of a face vary due to the relative camera-face pose (frontal, tilted, profile, upside down).
- Facial expression and emotions: The appearance of faces is directly affected by a person’s facial expression and emotions.
- Occlusion: Faces may be partially occluded by other objects. For an example, in an image with a group of people, some faces may partially occlude other faces (face identification).
- Image orientation: Face images directly vary for different rotations about the camera’s optical axis.
- Imaging conditions: When the image is formed, factors such as lightning and camera characteristics affect the appearance of a face.
- Age: Images taken after one or two year’s gap may not match with the images in database.

Size of the database: Number of images in the database will affect the performance of the system

1.5 Why Use the Face for Recognition

Biometric-based techniques have emerged as the most promising option for recognizing individuals in recent years since, instead of authenticating people and granting them access to physical and virtual domains based on passwords, PINs, smart cards, plastic cards, tokens, keys and so forth, these methods examine an individual’s physiological and/or behavioral characteristics in order to determine and/or ascertain his identity. Passwords and PINs are hard to remember and can be stolen or guessed; cards, tokens, keys and the like can be misplaced, forgotten, purloined or duplicated; magnetic cards can become corrupted and
unreadable. However, an individual’s biological traits cannot be misplaced, forgotten, stolen or forged. Biometric-based technologies include identification based on physiological characteristics (such as face, fingerprints, finger geometry, hand geometry, hand veins, palm, iris, retina, ear and voice) and behavioral traits (such as gait, signature and keystroke dynamics) [1].

1.6 Problems that may occur during Face Recognition

Due to the dynamic nature of face images, a face recognition system encounters various problems during the recognition process. It is possible to classify a face recognition system as either "robust" or "weak" based on its recognition performances under these circumstances. The objectives of a robust face recognition system are given below:

- **Scale invariance**: The same face can be presented to the system at different scales as shown in Figure 1.5-b. This may happen due to the focal distance between the face and the camera. As this distance gets closer, the face image gets bigger.

- **Shift invariance**: The same face can be presented to the system at different perspectives and orientations as shown in Figure 1.5-c. For instance, face images of the same person could be taken from frontal and profile views. Besides, head orientation may change due to translations and rotations.

- **Illumination invariance**: Face images of the same person can be taken under different illumination conditions such as, the position and the strength of the light source can be modified like the ones shown in Figure 1.7.

- **Emotional expression and detail invariance**: Face images of the same person can differ in expressions when smiling or laughing. Also, like the ones shown in Figure 1.5-e, some details such as dark glasses, beards or moustaches can be present.

A robust face recognition system should be capable of classifying a face image as "known" even under above conditions, if it has already been stored in the face database.
2. LITERATURE REVIEW

There is much research work in the field of human face detection and analysis of different countries people face using segmentation over the past decades. Some of the work done has been discussed one by one below:

**Tan et al. (2014)** suggested a new face detection algorithm to build fully automated systems that analyzed the information contained in face images, robust and efficient. Automatic face detection has been intensively studied for human-related recognition systems. On the one hand is based on the segmentation of the color image to skin regions using a new approach to detect the pixels of the skin and the water shed segmentation method. On the other hand, using Gabor filters, combined with a proposed model of face, skin regions are classified into two classes: face and non-face. The integration of these tools in our algorithm permits to develop a face detector with very reasonable and efficient performances. Experimental results show that the method mentioned in this paper can achieved high detection rates and low false positives. To evaluate the detection speed of proposed algorithm, a comparison with a recent known algorithm is made too.

**Vezhnevets et al. (2014)** used segmentation to localize and identify homogeneous regions in a picture by perceptual attributes which include the size, the shape and the texture and/or color information. The probability of each RGB color space of skin and non-skin database is important to detect skin pixels. Skin-color modeling is a crucial task for several applications of computer vision. Problems such as face detection in video are more likely to be solved if an efficient skin-color model is constructed. Most potential applications of skin-color model required robustness to significant variations in races, differing lighting conditions, textures and other factors. Given the fact that a skin surface reflected the light in a different way as compared to other surfaces. As the color of human skin is created by the combination of blood (red) and melanin (brown, yellow) which gives it a restricted range of hues. A skin region can be classified by comparing large image content of skin database and non-skin database. The RGB color space is widely used and most effective to detect skin region from an image.
Hajraoui, et al.(2015) proposed a detailed experimental study of face detection algorithms based on “Skin Color” has been made. Three color spaces, RGB, YCbCr and HSI are of main concern. He has compared the algorithms based on these color spaces and have combined them to get a new skin color based face detection algorithm which gives higher accuracy. Experimental results show that the proposed algorithm is good enough to localize a human face in an image with an accuracy of 95.18%.

Tabassum et al. (2015) proposed a novel human skin detection approach, an eye detector is used to refine the skin model for aseptic person. The proposed approach reduces computational costs as no training is required, and it improved the accuracy of skin detection despite wide variation in ethnicity and illumination. This is the first method to employ fusion strategy for this purpose. Qualitative and quantitative results on three standard public datasets and a comparison with state-of-the-art methods have shown the effectiveness and robustness of the proposed approach. A reliable human skin detection method that is adaptable to different human skin colors and illumination conditions is essential for better human skin segmentation. Even though different human skin-color detection solutions have been successfully applied, they are prone to false skin detection and are not able to cope with the variety of human skin colors across different ethnic. Moreover, existed methods require high computational cost.

3. PROBLEM FORMULATION

Human face detection and recognition play important roles in many applications such as video surveillance and face image database management. Computational models of face recognition are interesting because they can contribute not only to theoretical knowledge but also to practical applications. A face recognition system would allow user to be identified by simply walking past a surveillance camera. Human beings often recognize one another by unique facial characteristics. One of the newest biometric technologies, automatic facial recognition, is based on this phenomenon. Facial recognition is the most successful form of human surveillance.

The various gaps of the existing algorithms are:-

— Existing algorithm such as Gaussian model and 2D Histogram have high in processing time and also difficulty of detecting occluded objects, there is a necessity of huge data for machine learning.
— Another drawback of the previous approach is that its success relies on eye detector algorithms.
— In previous algorithms there have been found that YCbcR and Histogram color space are more efficient in comparison to RGB to classify the skin region. But still both are not able to give very good results.

So, there is a need to develop a new technique for human face detection which can overcome the entire research gaps.
3.1 Research Objectives

Objectives of the research work includes

- To study the existing techniques of human skin detection from digital image.
- To propose and implement the fusion approach for human skin detection.
- To compare the existing and proposed technique on the basis of Color Space, Accuracy, true Positive rate, false Negative Rate.

4. RESEARCH METHODOLOGY

Steps of system are given below:

Step 1: Take the image and get the image into RGB color space and process it.

Step 2: Apply the skin color segmentation algorithm of different color models and convert it into the binary image.

Step 3: After this the noisy image may apply the morphological operations on the image and for further refined image may apply the filter.

Step4: Calculate required skin area and also calculate feature points.

Step5. Classify the calculated features.

Step6: Result analysis qualitatively as well as quantitatively.

Figure 1.3: Steps to perform Face recognition
5. FUTURE WORK

Human faces contain a lot of important biometric information. The information can be used in a variety of civilian and law enforcement applications. For example, identity verification for physical access control in buildings or security areas is one of the most common face recognition applications. Recently, face recognition has become one of the most popular research areas in the fields of image processing, pattern recognition, computer vision, and machine learning, because it spans numerous applications. A number of possible improvements for future work have been identified through this research. In the future, we will implement the fusion method to detect the face identification system and check the performance of the system using various performance parameters.

REFERENCES


