IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Face Recognition System

Surya Mohan Kumar [A], Dr Raghavendra Prasad [B*]

[A, B] Amity University Chhattisgarh

Abstract

Computer programs that can recognize, track, identify, or validate human faces in pictures or videos are known as face recognition programs(Yang & Han, 2020a) .This biometric security system recognizes a person by their face traits.(Yang & Han, 2020). People can be recognized in images, films, or in real time using facial recognition technology. Systems for recognizing faces employ distinct mathematical patterns to store biometric information. They are among the safest and most reliable identifying techniques available in biometric technology as a result(Grudin, 2000). To lower the possibility of unwanted access, facial data can be privatized and anonymized. The technique of recognizing or verifying a person's identification using technology based on images, videos, or in-the-moment surveillance of their face is known as facial recognition.(Kortli et al., 2020) . Facial recognition systems may generally be utilized for two kinds of tasks: identification and verification. The background of facial recognition technology. Woody Bledsoe, Helen Chan Wolf, and Charles Bisson were the pioneers of automated facial recognition in the 1960s, with their work centered on teaching computers to recognize human faces. In addition to lowering crime rates, enhancing safety and security, and minimizing human contact, facial recognition technology has benefits for society(Annual IEEE Computer Conference et al., n.d.). The following are a few benefits of facial recognition: aids in the recovery of missing persons. Safeguards companies from theft. It varies according to the kind of facial recognition we're discussing(Yang & Han, 2020b). Among the safest in the business is Apple's 3D facial recognition system. However, 2D facial recognition, which is present in the majority of phones, is not very safe. Its lack of security implies that it won't open for someone else's face, but it might still open for a photographer, while you're asleep, or when you wear makeup or sunglasses and it can't identify your presence(Zhang & Institute of Electrical and Electronics Engineers, n.d.). It will be simpler for the recognition system to discover and identify faces in clear, well-focused photographs with decent illumination. Encourage your subjects to keep their postures and facial expressions consistent when the camera is focused on them. This can improve the system's ability to match faces between various photos. Crucial elements encompass the separation between your eyes, the profundity of your eye sockets, the arc from your forehead to your chin, the form of your cheekbones, and the outline of your lips, ears, and chin(Phillips et al., 2005). Finding the facial landmarks that are essential to differentiating your face is the goal. Low image quality or inadequate lighting can affect facial recognition systems(Lu et al., n.d.). Because of obstructed camera angles, the data might not match the person's nodal points; this results in an error when matching faceprints cannot be confirmed in the database.

Keywords: - Students live Behavior Monitoring, Criminal Investigation Tracker, Attendance System

Introduction

A biometric technology called face recognition uses a person's face to identify or verify their identification. It functions by recognizing and quantifying face features in a picture(Lu et al., n.d.). The three processes involved in face recognition are usually detection, analysis, and recognition(Hassaballah & Aly, 2016a). During the detection phase, computers employ computer vision to recognize objects, persons, and locations in photos with levels of accuracy comparable to or higher than those of humans, as well as increased speed and efficiency(Hassaballah & Aly, 2015b) .In the analysis stage, valuable information is automatically extracted, analyzed, classified, and understood from visual data using sophisticated artificial intelligence(Chingovska et al., 2016) .To sum up, facial recognition is one of the safest and most reliable identification techniques in biometric technology since it stores biometric data using distinct mathematical patterns during the recognition step(Chen, Liao, Ko, et al., n.d.) Facet data Modern technology called face recognition allows computers to recognize and verify people by analyzing their facial characteristics. This type of biometric identification uses specific facial features such the separation between the eyes, nose shape, and facial contouring(Chen, Liao, Lin, et al., n.d.-a) Usually, the procedure entails taking a picture or a video of a person's face, identifying its salient characteristics, and comparing those characteristics to a database of recognized faces in order to find a match(Chen, Liao, Lin, et al., n.d.-b) .For these jobs, sophisticated algorithms—often built on deep learning and neural networks—are utilized with impressive accuracy(Bruce & Young, 1986).Using an analysis of facial traits, face recognition is a revolutionary biometric technique that is revolutionizing the way people can be identified and authenticated(Bah & Ming, 2020a) Face recognition systems can precisely match faces acquired in photos or videos against a database of known faces by utilizing complex algorithms and machine learning approaches(Çarıkçı & Özen, 2012).With its wide range of uses, this technology can improve security protocols in financial institutions and airports as well as provide smooth user interfaces for smartphones and social media sites (Szakál et al., n.d.).Its quick acceptance, meanwhile, also brings up important questions about data security, privacy, and ethical issues(Computer Vision and Pattern Recognition, 2009, CVPR 2009, IEEE Conference on : Dates: 20-25 June 2009., 2009). Maintaining individual rights while promoting innovation in face recognition technology is crucial as it develops.

What are biometrics?

Biometrics are distinct physical traits that can be utilized for automatic recognition, like fingerprints(Grudin, 2000).They may also consist of quantifiable behavioral and biological aspects, such as anatomical and physiological features, that can be utilized to determine an individual's identity(Computer Vision and Pattern Recognition, 2009, CVPR 2009, IEEE Conference on : Dates: 20-25 June 2009., 2009b). A biometric system consists of several parts, such as sensors, databases, processing units, and output interfaces. The biometric sample, like a fingerprint or face image, is picked up by the sensors and digitally transformed (Yang & Han, 2020a).After extracting the salient characteristics from the sample, the processing unit compares it to other samples that are kept in the database(Phillips et al., 2005). The biometric system gives the user access to the resources if the input sample matches one of the samples in the database. Biometric modalities come in many forms: physiological modalities, like fingerprint and iris recognition, and behavioral modalities, like voice and signature recognition. Every modality has advantages and disadvantages of its own, and the best option is determined by the particular application and desired level of security(Lu et al., n.d.).Numerous applications, including border control, access control, and identity establishment, use biometric technologies. They also serve as a practical and safe method of verification in consumer goods like laptops and cellphones. Generally speaking, biometric technologies are safer and more dependable than conventional identification techniques like ID cards and passwords. (Hassaballah & Aly, 2015b).They are not impenetrable, though, and mistakes and weaknesses can occur(Chingovska et al., 2016).So, when applying biometric systems in different applications, it's critical to take into account their drawbacks and possible hazards.

❖ **Type of Biometrics :-**

- Finger-Scan
- Facial Recognition
- Iris-Scan
- Retina-Scan
- Hand-Scan

Why we choose Face Recognition over other biometric?

- Because facial recognition technology doesn't involve physical contact, it is more convenient and hygienic than other biometric techniques.

- As livens detection and anti-spoofing technologies have been included, facial recognition technology has become more dependable and secure than previous biometric techniques(Kortli et al., 2020).

  Generally speaking, facial recognition is thought to be less invasive than other biometric techniques like fingerprint or iris recognition (Yang & Han, 2020a).

- Comparatively speaking, facial recognition is more adaptable than other biometric techniques because it may be utilized both remotely and in different lighting situations(Kortli et al., 2020).

- Facial recognition is a well-known and reliable biometric technique that is utilized in many different applications, including mobile device unlocking, border control, and access control(Annual IEEE Computer Conference et al., n.d.).

- Facial recognition is a trustworthy method of verification since it can identify people with a high degree of accuracy(Yang & Han, 2020b).

- To create a complete security solution, facial recognition technology can be used with additional security measures like CCTV systems(Zhang & Institute of Electrical and Electronics Engineers, n.d.).

- Personalization is made possible via facial recognition in a number of contexts, including driver monitoring and hospitality(Phillips et al., 2005).

- With advancements in facial recognition technology, it is now feasible to reliably identify people in public settings during medical emergencies, even when they are donning masks(Lu et al., n.d.).

Face Recognition

A biometric technology called face recognition makes use of a person's facial traits to confirm or identify them(Hassaballah & Aly, 2015b). It operates by identifying and evaluating facial traits in a picture or video, then cross-referencing those features with a database of recognized faces (Chingovska et al., 2016). Applications for face recognition include marketing, law enforcement, and access control. Since it is a non-contact biometric, there is no need for direct physical touch with the subject of the identification (Chen, Liao, Ko, et al., n.d.). Because it eliminates the need for users to carry physical tokens or remember passwords, face recognition technology may be more convenient than other biometric technologies.(Chen, Liao, Lin, et al., n.d.-a).But since facial photos can be taken and stored without a person's knowledge or consent, it also poses privacy problems.

- **Verification –**

The System compares the given individual with who they say they are and gives a yes or no decision (Chen, Liao, Lin, et al., n.d.-b) . Machine learning techniques are generally used by face verification systems to evaluate facial features and spot distinctive patterns(Chen, Liao, Lin, et al., n.d.-c) . After that, a biometric template is made using these patterns, kept safely, and utilized for upcoming comparisons. The fact that face verification is non-contact is one of its advantages; this makes it a convenient and hygienic choice for consumers(Bruce & Young, 1986).Additionally, compared to other biometric techniques like fingerprint or iris scanning, it is usually thought to be easier to use. Facial verification systems are susceptible to assaults, wherein an impersonator's phony photo or video is presented(Kortli et al., 2020). Such attacks can be avoided by using liveness detection algorithms, which confirm that the individual presenting their face is a real human being.

- **Identification –**

A biometric technology called face recognition can be used to identify a person by identifying their face and comparing it to a database image that is known to exist(Bruce & Young, 1986). Access control, law enforcement, and airport security are just a few of the uses for this technology A facial recognition system measures and examines facial characteristics including the space between an individual's eyes, the breadth of their nose, and the contour of their jawline as it scans a person's face (Bah & Ming, 2020).After that, the image is transformed into a face print—a numerical code—which is then compared to the faceprints stored in the database.

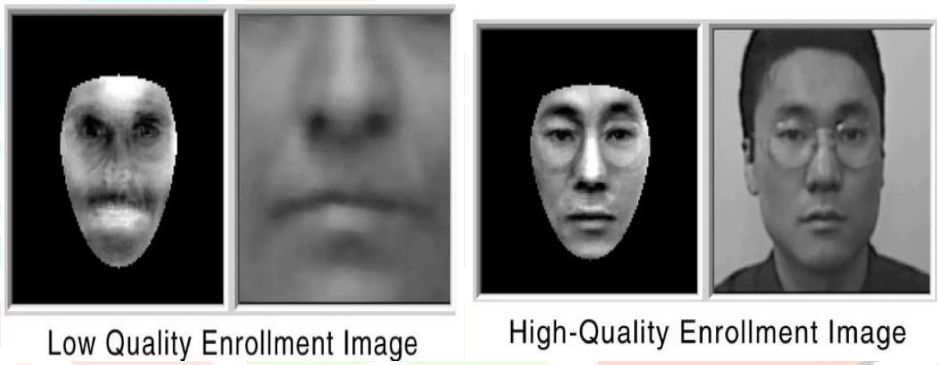
Implementation

Recognizing faces in photos or videos, identifying if two faces are of the same person, or finding a face in a vast library of previously taken photos are all possible with facial recognition software(Çarıkçı & Özen, 2012).

The implementation of face recognition Technology includes the following four stages:

- **Image Acquisition –**

The process of taking a picture and transforming it into a digital format so that a computer system can interpret and analyze it is known as image acquisition(Szakál et al., n.d.). Image acquisition in face recognition usually entails taking a picture of a person's face with a camera or other imaging device. When taking pictures of faces, it's critical to make sure the face is visible and that the quality of the shots is good(Computer Vision and Pattern Recognition, 2009, CVPR 2009, IEEE Conference on : Dates: 20-25 June 2009., 2009a). Aspects like lighting, distance, and angle might have an impact on the image's quality and may need to be adjusted when taking the picture. Following acquisition, the face photos can be subjected to a variety of image processing techniques, including feature extraction, normalization, and filtering (Grudin, 2000). By using these methods, one can improve the image quality and extract pertinent information for face identification.



- **Image Processing-**

Especially for image-based biometrics like faces, fingerprints, and irises, image processing is an essential component in the biometric process(Grudin, 2000). Improving the quality of the biometric image and extracting pertinent features for recognition are the two main objectives of image processing. Three functional categories can be used to organize image processing methods: feature extraction, image enhancement, and picture restoration(Computer Vision and Pattern Recognition, 2009, CVPR 2009, IEEE Conference on : Dates: 20-25 June 2009., 2009b). Noise reduction and filtering are two image restoration techniques that are used to lower noise and enhance image quality.(Kortli et al., 2020). Techniques for enhancing images, such sharpening and brightness, are applied to make specific characteristics more visible. Relevant features from the image that can be utilized for recognition are extracted using feature extraction techniques like B-Splines and Gabor filters(Yang & Han, 2020a) After the features are retrieved, the feature vectors of the candidate image and the image stored in the database are compared using an appropriate classifier(Annual IEEE Computer Conference et al., n.d.). The Nearest Neighbor classifier is the most commonly used classifier.

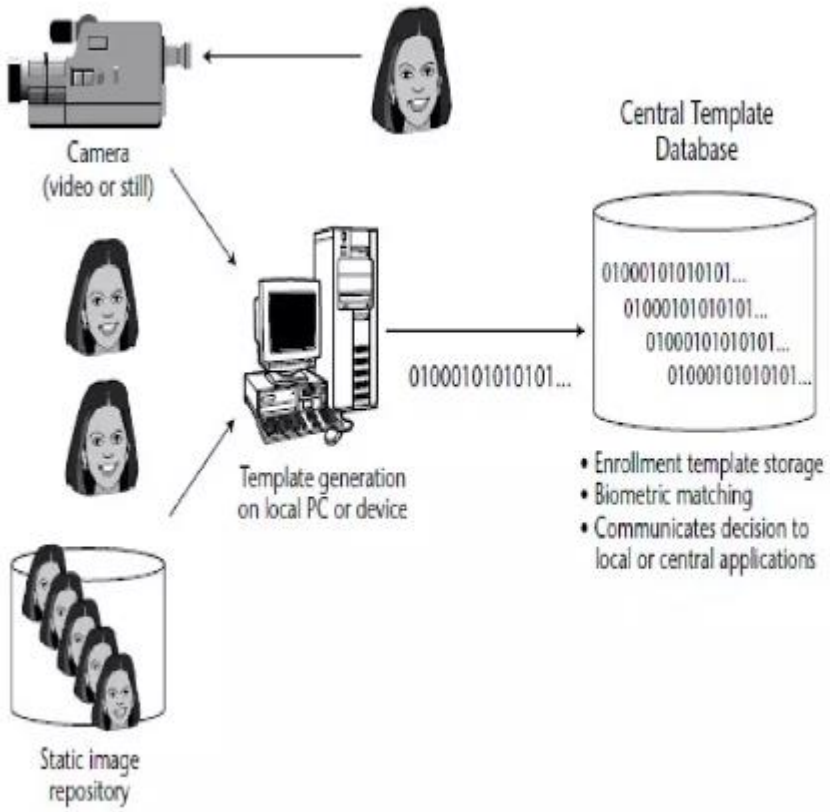
❖ **Distinctive characteristic location-**

A crucial stage in biometric recognition is determining the position of a distinctive trait, especially for image-based biometrics like faces, fingerprints, and irises(Yang & Han, 2020b). Finding and identifying the distinctive qualities or elements of the biometric image that can be utilized for recognition is the aim of this stage(Yang & Han, 2020b). In facial recognition, the eyes, nose, and mouth are usually the distinguishing features. By aligning and normalizing the face image, these features contribute to an increase in recognition accuracy. Within the domain of trademark law, a brand's distinctive character is defined as the feature that enables customers to recognize that it represents a distinct place of origin for products or services(Zhang & Institute of Electrical and Electronics Engineers, n.d.). Due to its decreased likelihood of causing misunderstanding among customers, a brand with distinctive character has a higher chance of being registered and protected under trademark law(Phillips et al., 2005) Locations, attributes, and character that are distinctive are key ideas in linguistics, trademark law, logistics, and other disciplines(Grudin, 2000). They help distinguish and classify things, sounds, and brands according to their special qualities. A stimulus set whose dimensions or properties can be controlled is necessary for the development of formal models of human categorization and recognition.

were a popular stimulus set in the 1970s and early 1980s that were used to construct these models (e.g., Goldman & Homa, 1977; Medin & Schaffer, 1978; Reed, 1972; Solso & McCarthy, 1981). The stimulus sets were created in a style reminiscent of the "Identikit" and "Photofit" facial composite systems of the time (for an illustration, view Figure 1) (*Computer Vision and Pattern Recognition, 2009, CVPR 2009, IEEE Conference on : Dates: 20-25 June 2009.*, 2009b)Studies investigating cue saliency in face recognition (e.g., Davies, Ellis, & Shepherd, 1977) also used a similar methodology. Exemplar models, such as Palmer (1975), posed a challenge to prototype models of idea representation by arguing against the extraction of a prototype or central tendency. Exemplar theorists (e.g., Nosofsky, 1986) show that more flexible exemplar models could account for empirical results that were previously viewed as proof of prototype extraction (Kortli et al., 2020). However, the idea represented literature was getting more and further removed from our comprehension of how faces are recognized in daily life. Knowing how stimuli such as those in Figure 1 can be portrayed didn't help much with our understanding of how the pertinent aspects or dimensions are taken out of real face photographs so that we can identify and classify real faces(Annual IEEE Computer Conference et al., n.d.) .The goal of face-space was to escape the theoretical dead end of cue saliency by finding a level of explanation appropriate to both familiar and unfamiliar face processing(Bah & Ming, 2020b).

In order to gather training data for our probabilistic algorithm, we first computed the intensity differences for a training subset of 74 intrapersonal differences (by matching each person's two views in the gallery) and a random subset of 296 extrapersonal differences (by matching images of different people). Lastly, we observe that simple linear discriminant techniques (such employing hyperplanes) cannot be applied with any degree of reliability because these classes are not linearly separable. Under the Gaussian assumption, the appropriate decision surface is naturally nonlinear (quadratic, in fact), and it is best defined in terms of the a posteriori probabilities, that is, by the equality P (I j}) = P (Ej~). Thankfully, when a MAP classification rule is called, the optimal discriminant After examining the two distributions' geometries, we used the PCA-based approach described to get the likelihood estimates P (j I) and P (j E). For I and E, we chose primary subspace dimensions of MI = 10 and ME = 30, respectively. These approximations of density

❖ **Template Creation-**



After the features have been retrieved, you may utilize them to create a template for every face image.(Yang & Han, 2020b). A template is a condensed version of the face image that highlights its main characteristics. For example, Principal Component Analysis (PCA), Linear Discriminant Analysis (LDA), and Local Linear Embedding (LLE) are a few of the algorithms and methods available for template construction(Phillips et al., 2005). These templates can be used to identify faces in new photographs once they have been generated. In this step, the templates of the new photos are compared to the templates of the recognized faces in order to determine which template is the closest match(Lu et al., n.d.). Template matching can be accomplished with a variety of methods and algorithms, including Euclidean distance, Cosine similarity, and Dynamic Time Warping (DTW)(Hassaballah & Aly, 2015a).

How facial Recognition System work...?

An image's facial features are detected and measured by a facial recognition system, which then compares the features to a database of recognized faces to determine whether they match(Chingovska et al., 2016). The three

primary steps of the system are usually detection, analysis, and recognition. The system detects whether a face is present in an image or video stream during the detection step(Kortli et al., 2020). Usually, computer vision algorithms that are highly accurate at detecting and locating faces are used for this. The technology searches a database of recognized faces for a match between the face print and the one being recognized(Yang & Han, 2020b). Usually, machine learning algorithms that have a high degree of accuracy in analyzing and comparing facial traits are used for this. Applications for facial recognition systems include recognizing people for security reasons, confirming identities for online accounts, and enhancing the in-store experience for customers(Phillips et al., 2005). It's crucial to remember, though, that bias and mistakes can occur with facial recognition software. It's crucial to use this technology sensibly and to put the necessary safeguards in place as a result.

Face Recognition in Software: -

Algorithms in face recognition software are used to recognize and validate people based on the characteristics of their faces(Lu et al., n.d.). It can be applied to many different things, including personalization, identity verification, and security(Hassaballah & Aly, 2015b).

- **Detection: -**

In detection systems, face recognition refers to determining whether a face is present in an image or video stream(Hassaballah & Aly, 2015a) .Usually, computer vision algorithms that are highly accurate at detecting and locating faces are used for this. The system can use facial recognition technology to evaluate and identify a face once it has been spotted(Chingovska et al., 2016) .There are several uses for facial recognition in detecting systems, including identity verification, security, and customization (Chen, Liao, Ko, et al., n.d.). For instance, it can be used to detect and monitor suspicious activities in public areas or to instantly identify people for access control purposes (Chen, Liao, Lin, et al., n.d.-a).Facial recognition technology has several advantages over other biometric technologies, such as faster and more effective verification, higher accuracy, and interoperability with a wide range of security applications(Chen, Liao, Lin, et al., n.d.-b) To preserve people's privacy and security, it's crucial to utilize technology sensibly and with the right security measures in place(Chen, Liao, Lin, et al., n.d.-c) .You can use a variety of tools and libraries, including OpenCV, Dlib, and Tensor Flow, to implement facial recognition in detecting systems. In order to assist you in developing your own detection system, these tools offer pre-built functions and algorithms for face detection and recognition(Bruce & Young, 1986).

- **Alignment :-**

Aligning facial pictures to a consistent size and orientation before to face recognition is known as face recognition in alignment(Çarıkçı & Özen, 2012). Usually, this is accomplished by first identifying facial landmarks like the mouth, nose, and eyes, and then aligning the face to a canonical orientation via an affine transformation(Szakál et al., n.d.). By guaranteeing that the facial characteristics remain in the same place and orientation in many photos, this can help to increase the accuracy of face recognition algorithms (*Computer Vision and Pattern Recognition, 2009, CVPR 2009, IEEE Conference on : Dates: 20-25 June 2009.*, 2009a). The FaceAligner class, which uses an affine transformation to align faces based on the location of the eyes, is used to demonstrate face alignment in the context of the PyImageSearch documentation. A facial landmark predictor, which is used to identify facial landmarks, and a set of desired face dimensions, which specify the dimensions and orientation of the aligned face, are inputs that the FaceAligner class uses(Grudin, 2000). A facial landmark predictor and the intended face dimensions are used to initialize the FaceAligner class. Next, the image and the bounding box of the face are fed into the align method, which is used to align the face in the image(Computer Vision and Pattern Recognition, 2009, CVPR 2009, IEEE Conference on : Dates: 20-25 June 2009., 2009b). The aligned face is returned as a numpy array by the align method. Normalization, when used to increase face

recognition algorithm accuracy, is the act of converting facial photographs into a standard format. Techniques like contrast stretching, photometric normalizing, and histogram equalization can be a part of this. Using a technique called contrast stretching, one can modify an image's contrast by scaling its intensity values within a predetermined range(Kortli et al., 2020) .This can help make facial characteristics more visible, especially in photos with limited contrast or intensity range. The process of photometric normalization modifies an image's color balance to eliminate fluctuations in illumination and lighting(Annual IEEE Computer Conference et al., n.d.). By ensuring that facial features maintain a consistent color and brightness across several photos, this can help to increase the accuracy of face recognition systems.

- **Representation:-**

In representation, face recognition is the process of transforming facial images into numerical representations for matching and recognition. Typically, deep learning algorithms trained on massive datasets of facial photographs are used to build these representations, also called face embedding. The most pertinent and discriminative aspects, such as the contours of the lips, nose, and eyes, as well as their separation, should be extracted from face photos to accomplish face recognition in representation(Yang & Han, 2020b). After that, these characteristics are merged into a single numerical representation known as an embedding, which is useful for matching and comparing faces. For any face recognition system, face recognition in representation is an essential phase since it establishes the system's correctness and dependability(Zhang & Institute of Electrical and Electronics Engineers, n.d.). Even in the face of changes in illumination, posture, and expression, a skilled face recognition system should be able to provide precise and discriminative embedding's that are useful for differentiating between people. Typically, convolutional neural networks (CNNs) trained on large datasets of facial photos are used by deep learning models to produce accurate face embeddings. These models are designed to identify and match faces by selecting the most pertinent aspects from the photos and combining them into a single embedding.(Lu et al., n.d.).

- **Matching: -**

In face recognition matching, the individual in the picture is identified by comparing the features of the given face image to a database of recognized faces. Usually, machine learning algorithms trained on massive facial picture datasets are used for this. This is how the remainder of the paper is structured(Computer Vision and Pattern Recognition, 2009, CVPR 2009, IEEE Conference on : Dates: 20-25 June 2009., 2009a). We examine the current local matching face recognition techniques in Section II. The overall architecture of the local matching method is broken down into three parts in Section III: classification and combination, local feature extraction, and alignment and division. In each phase, we enumerate and go over many options. Additionally, several theories are put out. In Section V, they are justified empirically. We provide a brief description of the The comprehensive comparative experimental research in Section V provides answers to the queries posed in Section III. Section VI consists of the discussion and conclusions. Much like with holistic approaches, aligning the face pictures is the first step in most local matching algorithms(Grudin, 2000). After that, the aligned faces are divided into local blocks. Since the steps for alignment and partitioning are typically connected, we address them together(*Computer Vision and Pattern Recognition, 2009, CVPR 2009, IEEE Conference on : Dates: 20-25 June 2009.*, 2009b) .Three categories can be used to group the alignment and partitioning techniques. The first category's approaches identify a few local face features, like the mouth, nose, and eyes(Yang & Han, 2020a). These facial components are separated from the face, and the matching facial components are compared in the ensuing recognition process. This class of techniques forgoes shape information, or the geometric arrangement of facial features. and merely examines how the matching components appear (photometric cues). We think that a key component of automatic face recognition should be the configuration The misalignment of local patches typically indicates that the two faces have distinct global shapes, as will be covered in the next few paragraphs. As a result, misalignment can be used to aid in recognition(Kortli et al., 2020).

Additionally, warping deforms the local facial components in addition to the global face, even if its intended outcome is to make the face more like a "standard" face. Because these local features—like the corners of the lips, the nose, the eyebrows, and the eyes—carry significant discriminating information, we believe that altering them is unproductive(Yang & Han, 2020b).

rather than matching facial components, the corresponding local regions (centered at the same coordinates). We highlight the distinction between local regions and local components(Zhang & Institute of Electrical and Electronics Engineers, n.d.) .The regions that the face components—such as the eyes, noses, and mouths—occupy and that are independently centered at the component centers are referred to as local components(Lu et al., n.d.) Local regions are windows that are focused on specific coordinates inside a shared coordinate system.

Raspberry Pi 3 Model B+: -

When compared to other single-board computers, the Raspberry Pi 3 Model B+ offers a special benefit because of its PoE (Power over Ethernet) functionality.(Hassaballah & Aly, 2015b)Its dedicated PoE interface makes circuit design simpler and increases circuit dependability by directly powering the Raspberry Pi 3 B+(Chen, Liao, Ko, et al., n.d.). Not many other single-board computers have this feature. The MxL7704 power management model from MaxLinear, which can supply 5 outputs and enhance the board's overall power management, is used by the Raspberry Pi 3 Model B+(Chen, Liao, Lin, et al., n.d.-a) This improves the PoE feature's dependability and effectiveness even more. It's important to remember that certain additional single-board PCs might also include add-on modules or external adapters that enable PoE. For instance, the Beagle Bone Black features a PoE-capable connector, but in order to utilize this capability, another PoE module is needed(Chen, Liao, Lin, et al., n.d.-b) .Compared to many other single-board computers, the Raspberry Pi 3 Model B+ features a more integrated and dependable PoE functionality, which might be a big advantage for some applications(Chen, Liao, Lin, et al., n.d.-c) .A 64-bit quad-core processor operating at 1.4GHz, dual-band wireless LAN operating at 2.4GHz and 5GHz, Bluetooth 4.2/BLE, faster Ethernet, and PoE functionality through the use of an additional PoE HAT are all features of the Raspberry Pi 3 Model B+ single-board computer.(Bah & Ming, 2020a)It keeps the same physical footprint as the Model B Raspberry Pi 2 and Model B Raspberry Pi 3. With its modular compliance certification, the dual-band wireless LAN board may be integrated into final products with a great reduction in wireless LAN compliance testing, which lowers costs and accelerates time to market(Çarıkçı & Özen, 2012) Along with Microsoft

Windows 10 IoT version, it can run the entire line of ARM GNU/Linux distributions, including Snappy Ubuntu Core(Szakál et al., n.d.).

Reference: -

Annual IEEE Computer Conference, IEEE Conference on Computer Vision and Pattern Recognition 25 2012.06.16-21 Providence, R., CVPR 25 2012.06.16-21 Providence, R., & IEEE Computer Society Conference on Computer Vision and Pattern Recognition 25 2012.06.16-21 Providence, R. (n.d.). *IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2012 16 - 21 June 2012, Providence, RI, USA*.

Bah, S. M., & Ming, F. (2020a). An improved face recognition algorithm and its application in attendance management system. *Array*, *5*, 100014. https://doi.org/10.1016/j.array.2019.100014

Bah, S. M., & Ming, F. (2020b). An improved face recognition algorithm and its application in attendance management system. *Array*, *5*, 100014. https://doi.org/10.1016/j.array.2019.100014

Bruce, V., & Young, A. (1986). Understanding face recognition. *British Journal of Psychology*, *77*(3), 305–327. https://doi.org/10.1111/j.2044-8295.1986.tb02199.x

Çarıkçı, M. üge, & Özen, F. (2012). A Face Recognition System Based on Eigenfaces Method. *Procedia Technology*, *1*, 118–123. https://doi.org/10.1016/j.protcy.2012.02.023

Chen, L.-F., Liao, H.-Y. M., Ko, M.-T., Lin, J.-C., & Yu, G.-J. (n.d.). *A new LDA-based face recognition system which can solve the small sample size problem*.

Chen, L.-F., Liao, H.-Y. M., Lin, J.-C., & Han, C.-C. (n.d.-a). *Why recognition in a statistics-based face recognition system should be based on the pure face portion: a probabilistic decision-based proof*.

Chen, L.-F., Liao, H.-Y. M., Lin, J.-C., & Han, C.-C. (n.d.-b). *Why recognition in a statistics-based face recognition system should be based on the pure face portion: a probabilistic decision-based proof*.

Chen, L.-F., Liao, H.-Y. M., Lin, J.-C., & Han, C.-C. (n.d.-c). *Why recognition in a statistics-based face recognition system should be based on the pure face portion: a probabilistic decision-based proof*.

Chingovska, I., Erdogmus, N., Anjos, A., & Marcel, S. (2016). Face recognition systems under spoofing attacks. In *Face Recognition Across the Imaging Spectrum* (pp. 165–194). Springer International Publishing. https://doi.org/10.1007/978-3-319-28501-6_8

Computer Vision and Pattern Recognition, 2009, CVPR 2009, IEEE Conference on : dates: 20-25 June 2009. (2009a). IEEE.

Computer Vision and Pattern Recognition, 2009, CVPR 2009, IEEE Conference on : dates: 20-25 June 2009. (2009b). IEEE.

Grudin, M. A. (2000). On internal representations in face recognition systems. In *Pattern Recognition* (Vol. 33).

Hassaballah, M., & Aly, S. (2015a). Face recognition: Challenges, achievements and future directions. In *IET Computer Vision* (Vol. 9, Issue 4, pp. 614–626). Institution of Engineering and Technology. https://doi.org/10.1049/iet-cvi.2014.0084

Hassaballah, M., & Aly, S. (2015b). Face recognition: Challenges, achievements and future directions. In *IET Computer Vision* (Vol. 9, Issue 4, pp. 614–626). Institution of Engineering and Technology. https://doi.org/10.1049/iet-cvi.2014.0084

Kortli, Y., Jridi, M., Al Falou, A., & Atri, M. (2020). Face recognition systems: A survey. In *Sensors (Switzerland)* (Vol. 20, Issue 2). MDPI AG. https://doi.org/10.3390/s20020342

Lu, X., Colbry, D., & Jain, A. K. (n.d.). *Three-Dimensional Model Based Face Recognition **.

Phillips, P. J., Flynn, P. J., Scruggs, T., Bowyer, K. W., Chang, J., Hoffman, K., Marques, J., Min, J., & Worek, W. (2005). *Overview of the Face Recognition Grand Challenge **.

Szakál, A., IEEE Hungary Section, IEEE Systems, M., & Institute of Electrical and Electronics Engineers. (n.d.). *SISY 2017 : IEEE 15th International Symposium on Intelligent Systems and Informatics : proceedings : September 14-16, 2017, Subotica, Serbia*.

Yang, H., & Han, X. (2020a). Face recognition attendance system based on real-time video processing. *IEEE Access*, *8*, 159143–159150. https://doi.org/10.1109/ACCESS.2020.3007205

Yang, H., & Han, X. (2020b). Face recognition attendance system based on real-time video processing. *IEEE Access*, *8*, 159143–159150. https://doi.org/10.1109/ACCESS.2020.3007205

Zhang, T., & Institute of Electrical and Electronics Engineers. (n.d.). *2011 3rd International Conference on Computer Research and Development : ICCRD 2011 : March 11-15, 2011, Shanghai, China*.