Face Detection and Recognition Techniques through the Cloud Network: An Exploratory Study

Manjunath Reddy[1], Anusha Bodepudi[2], Mounika Mandapuram[3], Sai Srujan Gutlapalli[4]

[1]Customer Engineering Lead, Qualcomm, San Diego, CA, **USA**
[2]Staff Engineer, Intuit, Plano, TX, **USA**
[3]EKIN Solutions, 13800 Coppermine Rd, Herndon, VA 20171, **USA**
[4]Interior Architect, Slce Architects LLP, New York, **USA**

[*]Corresponding Contact:
Email: reddymanjushari@gmail.com

Manuscript Received: 14 Nov 2020 - Revised: 15 Dec 2020 - Accepted: 24 Dec 2020

ABSTRACT

Face recognition is one of the fundamental functions performed by biometrics, and it is becoming increasingly influential as new technologies like the internet and digital cameras require improved security critical features. Other applications also make use of face recognition. Face recognition software can work with static photos or visual sequences to accomplish tasks. In addition, it can handle either one of the following tasks: face identification (also known as face recognition) or face verification (also known as face authentication). People can quickly and reliably recognize known faces and identities, even when presented with challenging viewing conditions such as changing illuminations, occlusion, scale, or rotation. This ability is a hallmark of the human species. Motivated by its significance in human-to-human communication and leading to various applications, ranging from biometrics to human-computer interaction, the face recognition challenge is an essential issue in the field of computer vision as well as other related areas. Finally, this article provides a summary of the most recent and cutting-edge strategies that have been developed to deal with challenging tasks like the one being discussed.

Keywords: Face Detection, Face Recognition, Cloud Network, Cloud Computing, Facial Recognition Algorithms, Gesture Recognition

INTRODUCTION

The consensus among experts is that advancements in computer vision research will provide neuroscientists and psychologists with valuable insights into the functioning of the human brain and vice versa. This is the consensus among experts. Image analysis has a wide variety of practical applications, but one of the most important is face identification. Building an automated system that is on par with humans in terms of its ability to recognize faces is an arduous task (Buciu, 2008). Even though humans are incredibly adept at recognizing familiar faces, we could be more skilled in simultaneously dealing with many unfamiliar faces. Because of their lightning-fast processing power and nearly infinite memory, computers should be able to overcome human constraints.

The face identification process is challenging since the recognition ability drastically declines with illumination, position, scale, or occlusion changes. This makes face recognition a challenging task. The face detection technique involves localizing and separating the face region from the surrounding background (Mandapuram, 2017). This is another crucial stage in facial recognition, and it has received much attention in computer vision research. Earlier face identification methods, such as the Viola-Jones face detector, could recognize facial regions in real-time from input photos. As time passed, it became an area actively researched and an essential component of any visual face interpretation framework. In recent years, there has been a significant increase in research initiatives reported for robust face detection utilizing various methods.

The process of feature extraction is essential to the operation of any face recognition system. It considerably impacts the operating efficiency of the system as a whole. SIFT, SVM, STIP, and STISM are examples of the various feature extractor models developed. In the later parts of this paper, we explore not only these current feature extractors and descriptors but also a great many others. For example, the feature extraction process has been classified using various criteria, including global versus local feature extraction methods, hand-crafted versus learning-based methods, and 2D versus 3D feature extraction methods. A feature extractor or descriptor often outputs a vast feature space in response to a single image (Mandapuram, 2016). This process gets significantly more difficult when the goal is to detect a person from video streaming. After this, the considerable feature space is subjected to further processing in PCA, SVD, MDS, LDA, and LDR to pick the significant features and accomplish dimensionality reduction. This benefits the system's performance due to the decreased total cost and improved utilization of system time for recognizing purposes that it enables.

After we have extracted the primary features from the incoming face image, we will iteratively match those characteristics with an existing feature database to achieve the goal we have set for ourselves. The identity is gleaned from the database, which is basically what the system does (Daugman, 1997). A wide variety of well-known classification approaches, including SVM, RBFNN, NC-K-mean, PNI, and CNN, are utilized for feature matching. One of the primary difficulties that must be overcome in research is the performance evaluation task for a face recognition system. In order to ease the development of newly proposed algorithms, a significant number of face recognition benchmarks have been produced and are now available to the public.

HOW DOES FACIAL RECOGNITION WORK?

The process of using an individual's face to identify or verify that person's identification is referred to as facial recognition, and it is a form of biometric technology. These kinds of systems use biometrics to examine a person's face, either through a photograph, video, or real-time livestream, and then compare that face to a database of previously trained photographs (Ruparelia, 2016). When a face is compared against a particular database of faces, biometrics are recorded, mapped, and processed to establish the identification of the face in question. It is possible for the incoming image of the face to be collected in either two dimensions or three dimensions. The specifications of the camera device and the facial recognition system determine this.

The faces are examined based on the geometry of their facial features, which may include, but is not limited to, the following:

- The width of the space between the eyes and the distance between them
- The bridge of the nose and its shape
- The contour of the chin, ears, and lips

The most sophisticated facial recognition algorithms can identify faces from various perspectives and numerous faces concurrently inside a single photograph, video, or live stream. This kind of facial recognition attribute determination can be utilized to discover the ages, genders, and moods of the individuals depicted in a photograph and match their faces to those in a database.

There are primarily three stages (Figure 1) involved in facial recognition. 1. Face detection 2. The process of extracting features 3. Face recognition.

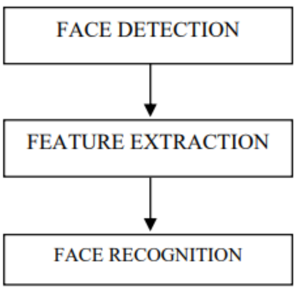

Figure 1: Comprehensive Look at Face Detection and Recognition

Facial Recognition and Cloud Computing

Cloud computing is a model that enables ubiquitous, convenient, and on-demand network access to a shared pool of configurable computing resources (such as networks, servers, storage, applications, and services). These resources can be rapidly provisioned and released with minimal management effort or interaction from service providers. Cloud computing is a model. Cloud computing is a model. It possesses five highly desirable qualities: on-demand self-service, extensive network access, resource pooling, and rapid elasticity. The facial recognition engine used in a facial recognition system implemented using cloud infrastructure is located in the cloud rather than in the local processing unit utilized in the conventional facial recognition technique. It is good knowledge that artificial intelligence and machine learning are the fundamental technologies behind facial recognition. A predetermined algorithm is used, which consists of identifying patterns from large amounts of previously collected data until the algorithm can provide prenatal (Sin Yee et al., 2020). In machine learning, a convolutional neural network, sometimes known as a CNN, is a category of deep artificial neural networks that have been effectively utilized to interpret visual data. One of its uses is the recognition of people's faces. For example, a facial recognition system that is hosted in the cloud has recently appeared as a means of expanding the capabilities of this technology.

A more seamless system can be accomplished by moving the facial recognition engine and the facial recognition database onto the cloud (Thodupunori & Gutlapalli, 2018). This concept is utilized by some different commercial programs in order to perform security checks. For example, the user takes a picture of their query face, which is then sent to a server in the cloud to authenticate it against the gallery faces stored in the facial recognition database hosted in the cloud.

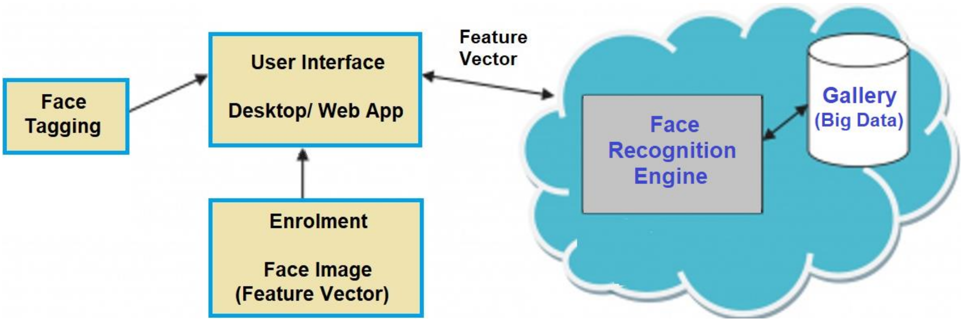

Figure 2: Faces stored in the facial recognition database hosted in the cloud

Cloud-based facial recognition systems offer a variety of advantages resulting from their intrinsic qualities. They offer an advantage in that the processing happens in real-time. Customers can quickly acquire and access the services they desire through on-demand self-service. In addition, cloud computing allows the system to become widely accessible because cloud services can quickly and reliably integrate with other applications. In addition, cloud services enable a high degree of scalability, making it more likely that the system will be able to accommodate many users.

The user interface, often called the user application, is how new users are registered (Sinha et al., 2017). The user interface carries out the process of Face Tagging by communicating with the cloud-based web API (application programming interface), which houses the facial recognition engine and a database of faces. The cloud-based API is then responsible for running the encoded face image through the facial recognition engine after receiving it from the user interface, which is responsible for adding new faces and enrolling them (Mandapuram & Hosen, 2018). The facial recognition engine implements a facial recognition algorithm that has been pre-defined. After receiving the query face from the user interface, the facial recognition engine will compare it to a collection of photos. Following the identification of a conclusive match, the inquiry face will be labeled as belonging to a specific person or not belonging to anyone. After then, the outcome will be communicated to the user via the interface.

Find and analyze faces within a file using Cloud Storage.

Conduct facial recognition analysis on a file that is saved in the cloud. Face Detection is finding several faces inside an image and the essential facial characteristics connected with each face, such as how the person feels or wears a hat.

Code sample

Before attempting to use this sample, we need to follow the setup instructions in the Vision quick start utilizing client libraries (https://cloud.google.com/vision/docs/detect-labels-image-client-libraries). Next, we must configure Application Default Credentials before you can authenticate to Vision.

```
//detect faces get faces from the Vision API for an image at the given file path.
func detectFacesURI(w io.Writer, file string) error {
	ctx := context.Background()

	client, err := vision.NewImageAnnotatorClient(ctx)
	if err != nil {
		return err
	}

	image := vision.NewImageFromURI(file)
	annotations, err := client.DetectFaces(ctx, image, nil, 10)
	if err != nil {
		return err
	}
	if len(annotations) == 0 {
		fmt.Fprintln(w, "No faces found.")
	} else {
		fmt.Fprintln(w, "Faces:")
		for i, annotation := range annotations {
			fmt.Fprintln(w, "  Face", i)
			fmt.Fprintln(w, "    Anger:", annotation.AngerLikelihood)
			fmt.Fprintln(w, "    Joy:", annotation.JoyLikelihood)
			fmt.Fprintln(w, "    Surprise:", annotation.SurpriseLikelihood)
		}
	}
	return nil
}
```

How Facial Recognition Algorithms Work

The process begins with face detection. In most cases, the algorithms will iterate through several boxes while searching for faces with a particular dimension. Within those boxes, the system looks for facial landmarks and then assigns a score to them. This score provides confidence in whether the image contains a face (Mandapuram et al., 2018). The technology will develop a template after determining that the object in question is a face. This template will typically be based on parameters such as the distance between the eyes, the area just below the nose and above the lip, and the distance from ear to ear. The newly developed mathematical representation is compared to previously recognized faces. As can be seen in Figure 3, the process of recognizing an individual by their face is iterative.

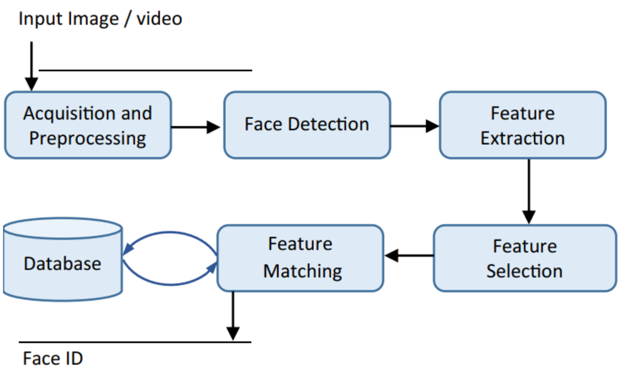

Figure 3: An iterative approach can be thought of as an overview of facial identification recognition

A score on a logarithmic scale is determined by the similarity in ratios between distances on various points of the face, often centered on anchors such as the nose, the eyes, the ears, and the lips (Gutlapalli, 2017b). The number of close matches can range from three to five, whereas the number of definitive nonmatches can be less than one. It is possible to earn a score of 40 or higher using the same image for both the probe and the target.

Cloud Network for 3D Face Recognition

Face recognition, a viable biometric technology for identification and verification, has traditionally been a research hotspot. Security, surveillance, and finance use it. 2D face recognition first uses artificial feature extractors. EigenFace, FisherFace, and LPB Face are successful classics. Deep learning In recent years, deepLFW and CASIA-WebFace training data have improved 2D face recognition. In recent years approaches have done well on this vast data.

End-to-end networks, which directly input raw data and output recognition results, are a famous network architecture. End-to-end networks automatically extract features while learning without a feature extractor. Most 2D face recognition algorithms are end-to-end networks, such as FaceNet, SphereFace, and ArcFace, with LFW dataset accuracy ratings of 99.63%, 99.76%, and 99.83%. After these successes, many academics hope to use end-to-end deep learning networks for 3D face recognition.

2D face recognition has good dataset accuracy but several practical issues. Different positions and lighting change 2D face photos. More crucially, 2D face recognition is vulnerable to image forgery. 3D facial recognition may solve these issues. The 3D model shows the face's anatomical structure rather than its texture or color, boosting facial recognition. It resists posture and illumination changes. According to, many 3D face recognition methods exist. Like 2D face recognition, deep learning-based 3D face recognition replaces artificially constructed feature extractors. Most deep learning algorithms project 3D input into 2D depth or range images, then use 2D networks for recognition.

These approaches are not end-to-end since 3D data is projected into 2D images using artificially created extractors. This approach can capture prominent facial traits but does not fu utilize 3D data. However, training data determines how well deep learning performs. Many articles train the network with more data. These approaches compare recognition rates on the same dataset but utilize different training sets, making the comparison unfair. The state-of-the-art method proposed uses six datasets, 22K scans, and ten times more accurate data for training than testing. In large-scale practical applications, the training set is frequently smaller than the test set. Hence identification rates may be much lower than expected (Bodepudi et al., 2019). These findings show that training an end-to-end 3D face recognition network with minimal data is still an issue.

End-to-end networks are widely utilized in 3D object classification and segmentation, segmentation, and. Charles et al. suggested an end-to-end network PointNet handles point clouds directly, and PointNet++ builds on PointNet. PointCNN, KPConv, DGCNN, and DPAM are end-to-end 3D object categorization and segmentation networks. 3D object categorization and segmentation are breakthroughs for these end-to-end 3D networks. Not built for faces, these networks perform poorly on 3D better cognition. Many academics wonder if these end-to-end 3D networks can improve 3D face recognition with superficial modifications. Progress has been made, but not enough.

FACE RECOGNITION APPLICATIONS

Leading technological businesses are harvesting face recognition systems in the digital age (Gutlapalli, 2017a). These organizations compete to produce the most incredible performance due to future commercial uses and growing market trends. IBM, Google, Microsoft, and Apple also compete in face recognition technologies. Patents for "face recognition" and "face identification" have increased dramatically in the past two decades. Companies are patenting face recognition frameworks. WIPO and USPTO figures show the same trend. Google has filed several face recognition patents since its successes in August 2017 and January 2018. These tendencies will help Google recognize faces from personal conversations, social networks, collaboration apps, blogs, and more.

This section summarizes rich facial recognition applications and commercial importance. IBM, Innovatrics, Advanced Biometrics, and IDEMIA offer easy, reliable, and versatile face recognition solutions with global installation. In addition, face recognition technologies are transforming automation in crucial applications. Below are many ways FR can be used for these two reasons.

- Verification, also known as one-to-one matching, is the process of determining whether or not a person is who they say they are when they are supplied with a face photograph of an unknown individual and their identification claim.
- Identification (one-to-many matching): Given an image of an unknown human, discovering that person's identification by comparing (potentially after encoding) that image with a database of (possibly encoded) photos of known individuals. This process is referred to as "one-to-many matching."
- Controlling access to buildings, airports/seaports, automated teller machines, and checkpoints at international borders; securing computers and networks; authenticating email on multimedia workstations; are all security aspects.
- Mugshot and booking systems, post-event analysis, and forensics are all part of the criminal justice system.
- Investigations using picture databases include searching for images of licensed drivers, benefit beneficiaries, missing children, immigrants, and anyone booked by the police.
- Applications of Smart Cards Instead of maintaining a database of facial images, the face print can be stored in a smart card, bar code, or magnetic stripe, and verification of the card are achieved by matching the live image to the template stored on the card.
- Face verification, which involves comparing a person's visage with that of a single enrolled exemplar, is well within the capability of today's personal computer hardware for access control. Unfortunately, the use of PC cameras for face-based PC logon has become viable in recent years because of the proliferation of PC cameras; nevertheless, the take-up of this feature is entirely restricted.
- Surveillance is the application domain with the most interest in face recognition. Video is the medium of choice for surveillance because of the wealth and variety of information it contains, and it stands to reason that face recognition is the most accurate biometric that can be applied to video data in the context of applications that require identification.

- Border Control: Using biometric technology allows for efficient identification procedures, making it an essential security solution for Border Control and Airports. Biometric technologies such as iris recognition, fingerprinting, vascular verification, and document verification are all currently in their early stages of development.

Gesture Recognition: Overview

Human-human gesture recognition is natural, while human-computer interaction relies on signals and actions that are not. Although keyboard and mouse are advantageous over tabular switches and punch cards, developing more natural and intuitive interfaces that do not require specialized training remains challenging. We would instead teach machines to recognize faces, gestures, and speech than teach humans to do so. Natural language interfaces with continuous speech processing, speaker-independent recognition, and natural-sounding speech synthesis will progress these goals best (Vinay et al., 2015). However, effective ways to understand and imitate non-verbal human expressiveness, like manual or facial gesticulation, will be crucial. Our faces automatically convey, react, probe, modulate, and add nuance to speech. In face-to-face discussions, we commonly communicate assent, dissent, uncertainty, irony, and other emotions using facial expressions and head movements.

The birth rate of identical twins, below one percent, sets an upper constraint for facial recognition. Genetically identical monozygotic twins show the extreme genetic penetrance of facial features. Aging is the critical phenotypic factor for facial appearance, reflecting development rather than DNA, although it cannot be utilized to separate identical twins. However, morphological distinctions allow humans to identify familiar identical twins. Computer vision algorithms may fail this test.

Dimensionality and variance of encoded degrees of freedom determine face (or other) recognition system performance. Their inter-class variation should be high, and their intra-class variance low, such that different faces generate face codes that are as distinct as possible and different photos of the same face generate remarkably similar codes. Recent studies have examined face coding scheme invariances under changes in illumination, perspective angle, position, and expression. Their findings suggest that a given face has more variability across these three sorts of alterations than across various faces when these three characteristics are constant. Several publications in this thematic part address this fundamental classical pattern recognition theory problem.

Faces are partially deformable surfaces of three-dimensional solids. Pose, perspective angle, illumination, age, cosmetics or adornments, and expression determine its picture. 2D appearance-based vs. 3D model-based face representation is debated. Which degrees of freedom should be extracted? Which ones are generic for all faces (essential for face detection) and specific for one face (relevant for recognition)? How should evidence be integrated and uncertain decisions made? Face recognition is machine intelligence's "Holy Grail" and a classic pattern recognition challenge.

Factors Influence the Accuracy of Facial Recognition

The precision of these systems is a function of several different parameters being combined. The accuracy rate of the facial recognition system will be significantly impacted by the quality of the face images provided during both the dataset training stage and the live identification stage of the process. It is strongly advised that several photographs of the same person are included in the training dataset when training this type of system. These photographs should be taken from a variety of angles and under a variety of lighting conditions. This will allow for a higher grade of image recognition to be attained. The resulting prediction becomes increasingly precise when additional information is added to a dataset. Other characteristics that play a role in determination include face posture, facial expression, glasses, makeup, hair and facial hair, and hairstyle.

KEY CHALLENGES FOR FACE RECOGNITION

The processes of face detection and recognition are not without their difficulties, some of which are as follows:

Illumination Challenged: Although face recognition systems in indoor platforms have reached a certain level of performance, face recognition in outdoor platforms remains a challenging topic. Variation in illumination conditions, which causes dramatic changes in facial appearance, is one of the most challenging problems a practical face recognition system must solve.

Face pose: Surveillance cameras are usually situated out of reach. Mounting a high camera angle faces. City surveillance's simplest case. The next and most brutal instance is people organically passing past the camera view. They ignore the lens. Public behavior cannot be regulated. Such circumstances require proper recognition. Even cutting-edge facial recognition methods have a 10–15 degree angle constraint. Recognizing faces from multiple angles is challenging.

Face expression: Face expression is a less major issue when compared to the angle, yet it still impacts the face.

Results of recognition: Although a closed eye or smiling face does alter the recognition rate by one percent to ten percent, a face with a big laugh influences as much as thirty percent because a laughing face modifies the appearance of the face and distorts the correlation of the eyes, mouth, and nose.

Aging: Face recognition algorithms use geometrical, feature-based, or holistic methodologies. None fix aging. Most allow 20 years following training. Since faces change quickly, 1–15-year-olds cannot be recognized. Teens' faces stabilize. No algorithm recognizes faces of all ages.

Dynamic Background: When the background is static or solitary, it is much simpler to distinguish a person's face; nevertheless, difficulties arise when the background is changing or dynamic. Multiple-face recognition is far more complicated than single-face recognition, making it one of the most difficult challenges in this industry.

LIMITATIONS OF FACIAL RECOGNITION TECHNOLOGY

Despite the significant effort put into developing a reliable face recognition system, existing face recognition systems still need to improve. The technology behind face recognition has yet to be reliable, particularly in unrestricted contexts, and the recognition accuracy needs to be more satisfactory, particularly for large-scale applications (Rath & Rautaray, 2014). Alterations in the lighting, position changes, and time variances between the gallery image(s) and the probe image(s) all contribute to a performance decline. In

FRVT 2002, some of the best commercial systems were utilized to analyze these factors. This degree of precision is not appropriate for use in a security system at an airport because the number of passengers there is far higher than in an access control system with a remote database containing only a few hundred persons, which may or may not be adequate for use in such a system (Gutlapalli, 2016). The findings of the FRVT 2002 tests help explain why many systems deployed at airports and other public places have not gotten positive feedback due to the poor performance of such systems. One illustration of this is how the crowd monitoring system evaluated by the police in Tampa, Florida, identified 14 instances of a probable criminal match over four days. However, all of them turned out to be false alarms. It appears that the Tampa Police Department has given up on the system.

Facial recognition technology is hindered in its efficiency by the following four factors:

1. The effectiveness of facial recognition is hindered when images are of poor quality

The accuracy of facial recognition algorithms is significantly impacted by image quality. Compared to the image quality of a digital camera, the quality of an image obtained through scanning video is relatively poor. Even high-definition video only comes at a maximum resolution of 1080p (progressive scan), while the standard resolution is 720p. These figures are equivalent to 2 megapixels and 0.9 megapixels, respectively. However, an affordable digital camera can get 15 megapixels. The difference is easily recognizable.

2. The use of images with a low resolution makes it more difficult to recognize faces.

When a face-detection algorithm discovers a face in a picture or a still from a video capture, the relative size of that face compared to the size of the whole image will determine how accurately the face will be identified. Due to the small size of the image and the fact that the target is some distance away from the camera, the size of the recognized face is only between 100 and 200 pixels on each side. In addition, the action of scanning an image for different face sizes requires a significant amount of processing power. The vast majority of algorithms enable the definition of a face-size range, which helps reduce the number of false positives during detection and speeds up the processing of images.

3. A variety of face angles can negatively impact the accuracy of facial recognition.

Significant weight is given to the relative angle of the target's face in determining the recognition score. When a face is enrolled in the identification software, numerous angles of the face are typically employed (the profile, frontal, and 45-degree views are the most popular). The ability of the algorithm to produce a template for the face is hindered when it is given a view of the face that is not frontal. The score of any ensuing matches is given based on how direct the picture is (both the image that was enrolled and the image that was probed) and how high its resolution is.

4. Capabilities of facial recognition technology may be constrained by data processing and storage

Even while high-definition video has a relatively modest resolution compared to the photographs produced by digital cameras, it nevertheless uses up a considerable amount of storage space on a disk. Because the processing of each video frame is such a monumental task, a recognition system is typically only applied to a small percentage of the frames (10–25 percent) that are captured. Agencies have the option of utilizing computer clusters in order to cut down on the total amount of time required for processing. Adding more computers, however, requires significant data transport via a network. This data transfer may be constrained by input-output limits, which further slows down the processing speed.

When identifying people based on their faces, surprisingly, humans are far more adept than technology. However, when watching a source video, humans can only focus on a few individuals at a time. For example, a computer can compare many persons to a database containing thousands of entries.

CONCLUSION

Research in the field of biometrics frequently focuses on various aspects of face recognition from images. Surveillance cameras are often installed in various open areas for video collection, and these cameras have their own vital value for maintaining safety. Since it does not require the aid of the object, facial recognition has been given much credit for playing an essential part in the surveillance framework. This fact is widely acknowledged. The main advantages of using a person's face as a form of identification over other biometrics are its uniqueness and widespread acceptability. At the outset, we provide a fundamental introduction to face identification and review the various elements influencing face shape, structure, and texture. For the purpose of calculating age, the user's age tasks are combined with the aging process. After that, the user will utilize the judge age function, typically a vector-generating function or a feature vector of the actual image, to generate and include feature vectors at the destination age. Finally, the user can display an image of the user's face by anticipating it in the Eigenspace of structure using structure and texture vectors. In this article, the author primarily focused on the field of face recognition. Finally, they present an overview of the existing research launched in this area.

Additionally, we analyze the benefits and limitations of research coined in the literature. Face recognition is the primary subject of this essay. In recent years, researchers in the fields of biometrics, pattern recognition, and computer vision have paid a significant amount of attention to face recognition. There are a significant number of applications in the commercial, security, and forensic sectors that call for the utilization of facial recognition technologies. As can be seen, a facial recognition system plays a significant role in our day-to-day activities. It has a very significant benefit that must be noticed. The facial recognition system is the most reliable and accurate of all the different kinds of biometrics. In this study, a classification of face detection approaches has been done, and several face recognition algorithms and techniques have been reviewed, along with a tabular representation of each method's advantages and disadvantages.

REFERENCES

Bodepudi, A., Reddy, M., Gutlapalli, S. S., & Mandapuram, M. (2019). Voice Recognition Systems in the Cloud Networks: Has It Reached Its Full Potential? *Asian Journal of Applied Science and Engineering*, *8*(1), 51–60. https://doi.org/10.18034/ajase.v8i1.12

Buciu, I. (2008), OVERVIEW OF FACE RECOGNITION TECHNIQUES, *Journal of Electrical and Electronics Engineering,* (1), p. 173.

Daugman, J. (1997). Face and gesture recognition: overview. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, *19*(7), 675–676. https://doi.org/10.1109/34.598225

Gutlapalli, S. S. (2016). An Examination of Nanotechnology's Role as an Integral Part of Electronics. *ABC Research Alert*, *4*(3), 21–27. https://doi.org/10.18034/ra.v4i3.651

Gutlapalli, S. S. (2017a). Analysis of Multimodal Data Using Deep Learning and Machine Learning. *Asian Journal of Humanity, Art and Literature*, *4*(2), 171–176. https://doi.org/10.18034/ajhal.v4i2.658

Gutlapalli, S. S. (2017b). The Role of Deep Learning in the Fourth Industrial Revolution: A Digital Transformation Approach. *Asian Accounting and Auditing Advancement*, *8*(1), 52–56. Retrieved from https://4ajournal.com/article/view/77

Mandapuram, M. (2016). Applications of Blockchain and Distributed Ledger Technology (DLT) in Commercial Settings. *Asian Accounting and Auditing Advancement*, *7*(1), 50–57. Retrieved from https://4ajournal.com/article/view/76

Mandapuram, M. (2017). Application of Artificial Intelligence in Contemporary Business: An Analysis for Content Management System Optimization. *Asian Business Review*, *7*(3), 117–122. https://doi.org/10.18034/abr.v7i3.650

Mandapuram, M., & Hosen, M. F. (2018). The Object-Oriented Database Management System versus the Relational Database Management System: A Comparison. *Global Disclosure of Economics and Business*, *7*(2), 89–96. https://doi.org/10.18034/gdeb.v7i2.657

Mandapuram, M., Gutlapalli, S. S., Bodepudi, A., & Reddy, M. (2018). Investigating the Prospects of Generative Artificial Intelligence. *Asian Journal of Humanity, Art and Literature*, *5*(2), 167–174. https://doi.org/10.18034/ajhal.v5i2.659

Rath, S. K., & Rautaray, S. S. (2014). A Survey on Face Detection and Recognition Techniques in Different Application Domains. *International Journal of Modern Education and Computer Science, 6*(8), 34-44. https://doi.org/10.5815/ijmecs.2014.08.05

Ruparelia, N. B. (2016). *Cloud Computing* (Cambridge, MA: MIT Press). Selections. Read chapter, Readoduction, 1-3.

Sin Yee, J. L., Sheikh, U. U., Musa, M. M., & Syed, A. R. (2020). Face Recognition and Machine Learning at the Edge. *IOP Conference Series. Materials Science and Engineering*, *884*(1). https://doi.org/10.1088/1757-899X/884/1/012084

Sinha, D., Pandey, J. P., & Chauhan, B. (2017). Face Recognition Age Invariant: A Closer Look. *International, Internationalmputer Science, and Information Security*, *15*(2), 477.

Thodupunori, S. R., & Gutlapalli, S. S. (2018). Overview of LeOra Software: A Statistical Tool for Decision Makers. *技术与管理回顾*, *1*(1), 7–11. http://技术与管理回顾.移动/index.php/tmr/article/view/4

Vinay, A., Shekhar, V. S., Rituparna, J., Aggrawal, T., Murthy, K. N. B., & Natarajan, S. (2015). Cloud-based big data analytics framework for face recognition in social networks using machine learning. *Procedia Computer Science, 50*, 623-630. https://doi.org/10.1016/j.procs.2015.04.095

--0--