International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Optimized Haar-cascade Algorithm for Face Recognition and Authentication

Kuldeep Vayadande[1], Rachit Chandawar*[2], Anuj Mahajan[3], Swapnil Garud[4], Mansi Parse[5], Jaykumar Gavit[6], Pushkar Gajdhane[7], Aryan Chalpe[8], Pratik Davare[9], Atharva Borade[10], Eshan Dasarwar[11]

Submitted: 16/03/2024 **Revised**: 30/04/2024 **Accepted**: 08/05/2024

Abstract: What amuses biometrics is that it can be incorporated into various situations. Particularly, it can be used to conduct identification, security, and Internet security. A newly emerged biometric technology is related to 3D imagery of faculty features while delivering additional flow of volume to empirical verification of human faces as well as identification. Conversely, it is very difficult to manipulate with large amount of 3D faces data that may come with some problems including the dimensionality reduction issues problem fighting with. This process serves to define face recognition as a viable means of personal identification nowadays, typically used during security, human–computer interaction systems, among others, and thus opting for more efficient algorithms for embedded systemsis no longer negotiable. The smallest platforms are now utilizing the concept of embedded face recognition as the latest trendsetter. Lastly,neural networks are being potentially integrated into the system as they are considered to give the artificial systems both the speed and theaccuracy. The canvas combines the concept of which includes LBP and MTCNN that brings all the edges to an end. Despite the fact that the PCA method before had brought about success in the dimensionality reduction sphere, a manifold theory has now become the trend in the process of handling facial expressions which have added complexity to the situation. The document explains the applications of the Haar cascade and face detection components, which includes before processing grayscale images up to after processing like integration with thefacial recognition system. Furthermore, the course is video-academic and practical in that during the duration it deals with real time applications and issues and ethics principles which are mostly internalized to a student. The algorithms Library which is built on the abilitiesof face detection is the main tool of the developers and the researchers, on the one hand, that are used not only for face detection and employment of it but also for diversification of the technology, on the other hand. Progress is after all implemented in a double sense. thus, while the definition exposes the issues of ethics and imprecision, the main problem with computer vision cannot be forgotten either. Further, this result-based rescue approach also delivers the idea that the university is an getting prepared university as it aids its students to expand relevant skills and knowledge that actually follow on every campus, contemporary society.

Keywords: *Grayscale, Cascade Classifier, Landmark, Scale Factor, Potential parameter.*

1. Introduction

Humanizing face recognition technology as the primarybiometric verification lever may be shaping how the technology evolves generally on various issues. This writing presents a comprehensive viewpoint of the theme through the use of the original works as presented in the paper from the unique angle of the general facial recognition. The introductory part explores that face detection technology has advanced up to the face-recognizing stage and finally it puts its application into social networking sites(SNSs). This has raised various security issues concerning.

[1-11]Department of Information technology, Vishwakarma Institute of Technology, Pune, 411037, India

[1]Email: kuldeep.vayadande@gmail.com
[2]Email: rachit.chandawar221@vit.edu
*(*Corresponding Author)*
[3]Email: anuj.mahajan22@vit.edu [4]Email: swapnil.garud22@vit.edu
[5]Email: mansi.kamble22@vit.edu [6]Email: jaykumar.gavit22vit.edu
[7]Email: pushkar.gajdhane22@vit.edu [8]Email: aryan.chalpe22@vit.edu
[9]Email: pratik.davare22@vit.edu [10]Email: atharva.borade22@vit.edu
[11]Email: eshan.dasarwar22@vit.edu

The historical path of the facial recognition technology has been traced starting from the six decades ago in order to understand the history of events and the technology itself[2]. Primordialities, of this timeline, gives a rational of how tech grew very close to the average human world. It ranges from the first ever inclusionof the crude's facial measurements to the more popularized Eigen faces and the release of the Deep Face by Facebook alongthe way. Incomplete examples demonstrate the use of the facial recognition technology by the Chinese law enforcement such as face control, face verification, and a responsible buy of telephone in 2019 to advertise that the facial recognition uses in a wide range of areas and for a long time period. Moreover, people still believe that modernism and the social network media which have the dual nature are two-way swords that may bring both favorable and unfavorable outcomes. Consequently,We will move a step further by presenting a new method to ensure privacy in social networking sites by considering the capability of face recognition as an example. In this technology there are the initial frames catching at the start when camera is in the registrations and the authentications which are later stored in the databases and then there will be 75 subjects which commercial electronics devices which are dealt here. Conversely, e-money is equipped with new security measures to support both the electronic transactions and the payment system. The exploitation avenues like unreliability and obscurity of the face recognition vulnerabilities along with the impossibility to complete the work

in question are highlighted and exposed below[1]. No doubt that deep learning systems are the main milestones towards more credible and reliable practical security, but its robustness remains to be the issue of practical security use. The article gives only a basic analysis of existing solutions such as the Viola & Jones face detector or the latest CNN-based approach. The analysis shows that the new perspectives and change introduces lots of opportunities for innovative solutions. In view of the fact that the current deployment of facial recognition in the field of commercial electronics is prevalent in mobile phones and smart cards, these gadgets have been identified as a series of challenges. They include privacy and reliability relating to both the private and public sectors[4]. This paper introduces how black boxes tests of the present-day web services APIs will be formed without any intricate or tedious backend details. Our article suggests a new facial recognition threat model which details a close cable to CNN vulnerability-based threats as will the latter be covered in its own subject.

In digital cash transactions, it talks about the security issues that challenge digital transactions. It further deliberates on CBDC's inadequacy when compared to traditional methods and the trend of using facial recognition to address these problems properly[5]. The AI technologies that are shown in the forms of representation and enhancement techniques help to enhance the level of accuracy in face recognition used as a security authentication process. The simulating and analyzing of the face detection algorithm booked model the researchers somehow achieve the 100% accurate detection rate in preventing both the missed detections and the false ones, which later known of the higher security assurance system created.

Authentication, which is a major issue, can be overcome due to the presence of some constraints in account-based approach[6]. The devices contain a built-in camera through which we undertake the study of a face image for authentication purposes. PBAS, as proposed in the paper, is a cooperative system that resolves the face images as well as passwords problems by the two independent components of a biometric system fuse into one. along with those, some ideas from other research articles are also incorporated to ensure that a wholistic viewpoint is given. The second manuscript focuses on the state of the art of automatic face recognition methods so that a system that uses linear discriminant analysis with contrast-based rejection criteria follows [7].
The work on face recognition applications, however, has focused on co-operative cases and users. This work is a short description of the challenges and the solutions of the facial recognition technology as well as a summary of the background information that will be discussed in the subsequent sections.

2. Literature Review

This is the age of modern technology which has introduced a situation where all systems based on SNSs, and facial biometric authentication are fertile. This literature review sorts out in depth all areas of these technologies. The advantages and possible findings which accompany them, as well as how they can be modified, are also given. Questionnaire by combining them, several research fields provide key insights of our current market and finally present overall scenario. The paper [1] author stresses the authenticity and reliability testing of facial recognition API by a personal experience targeting permission from Baidu, designed by Face ++ processes, and Google Identity AI. Testing also includes setting acceptance criteria which are found through the combination of real and artificial machines output values. The attacker was successful in the attack which proves that APIs without liveness feature are susceptible to presentation attacks. The access control API consists of two main APIs, namely the liveness detection and the acceptance rate. The latter determines the protection level of the user and the type of data retrieved, as well as how it is implemented in the system and its safety influence on the application. The paper presents two case studies, and the paper recommends that the adversarial samples need to be validated for the reliability of the B-api at Baidu and the Face++ API in their future studies. The design of this SNS is characterized by secure attributes that offer services such as messages and pictures exchange, status sharing, friend list management, games and profile customization. Central control system based on biometric identification makes the issues about distance logging mandatory. It is the reason why the most important issue is the possibility for getting the same face image with a high photography for online process. Face recognition algorithms that are usually used for authentication have been applied in the authentication process and they bring about excellent evaluation (79.77% to 93.10%). Consistently, though, the number of pictures in a database needs to be increased and different environments in which pictures are stored need to be taken into consideration as well as new algorithms of authentication should be invented, and all the other approaches should be investigated.
Finally, by talking about the biometric access control on the grounds of face detection, such as the comfort and social accept and also, regarding the concerns for the students' issues at institutions, the article [5] leads its reader to serious consideration of the new biometric system. On the other hand, impostorsyndrome did not last. Many hurdles such as imposter syndromeare still there, however. The use of facial recognition by teachersinstead of the manual attendance method brings to the fore the most difficult aspect of the Go-Ahead path. The process is still far from ending in a way that the systems will not only uplift quality but will bring more beneficial outcomes for education technologies in the future.
In addition to the authentication methods discussed, it's crucial to delve into the broader societal implications of widespread facial recognition technology adoption, especially within social networking platforms. While biometric access control systems offer convenience and efficiency, they also raise significant privacy concerns and potential ethical dilemmas. The collection and storage of facial data for authentication purposes pose risks of misuse or unauthorized access, leading to potential breaches of user privacy. Moreover, the accuracy and reliability of facial recognition algorithms can vary, leading to concerns about algorithmic bias and discrimination, particularly against marginalized communities.

Furthermore, the integration of facial recognition technology into social networking services introduces complex challenges related to consent, user control, and data ownership. Users may not always be fully aware of how their facial data is being used, shared, or monetized by platform providers. This lack of transparency can erode trust and exacerbate concerns about surveillance and manipulation. As such, it is imperative for policymakers, technology companies, and civil society to engage in robust discussions about the ethical and regulatory frameworks needed to govern the responsible deployment of facial recognition technology in social networking contexts.

Furthermore, the integration of facial recognition technology into social networking services introduces complex challenges related to consent, user control, and data ownership. Users may not always be fully aware of how their facial data is being used, shared, or monetized by platform providers. This lack of transparency can erode trust and exacerbate concerns about surveillance and manipulation. As such, it is imperative for policymakers, technology companies, and civil society to engage in robust discussions about the ethical and regulatory frameworks needed to govern the responsible deployment of facial recognition technology in social networking contexts.

3. Comparison Table

Paper Algorithm	Methods used/Innovation	Application and Future work	Results and Limitations	References
1.Baidu API, Face++ API, Google Facenet, and StarGAN for facial recognition assessment and synthetic image generation	The research methodology involved conducting accuracy and reliability tests across various datasets using Baidu API, Face++ API, and Google Facenet. Synthetic face images were generated using StarGAN, allowing for comprehensive evaluation of facial recognition performance. The study employed blackbox testing to assess presentation attack vulnerabilities and liveness detection effectiveness, emphasizing the criticality of security in web-based facial recognition systems.	The study's insights strengthen facial recognition system security in mobile and web platforms. Future efforts may refine detection techniques and incorporate adversarial samples to enhance system robustness against advanced attacks, ensuring heightened user privacy and security.	The study revealed varying accuracy rates among facial recognition APIs, with Face++ demonstrating superior performance. However, limitations include the lack of comprehensive testing across diverse datasets and the absence of detailed analysis on algorithm vulnerabilities to adversarial attacks.	[1]
2.The study utilizes PCA, ICA, LDA, and SVM algorithms for face recognition, implemented using Java EE, JavaScript, and a web camera. biometric authentication, security in SNS logins.	The methods employed include PCA, ICA, LDA, and SVM algorithms for face recognition in social networkingsite authentication. The innovation lies in integrating biometric authentication, implemented using Java EE, JavaScript, and a web camera, enhancing security in SNS logins. The innovation lies in integrating biometric authentication, using Java EE, JavaScript, and a web camera, enhancing security in SNS logins through facial recognition.	The application spans multiple social networking platforms, bolstering security through biometric authentication methods. Future endeavours mayfocus on extending platform support and refining facial recognition algorithms for heightened accuracy.	The system demonstrated robust performance across various datasets, achieving high accuracy in user identification. However, limitations include potential challenges with facial recognition in diverse lighting conditions and the need for further validationon larger scales. Nonetheless, the results offer promising insights into bolstering online security through biometric authentication.	[2]
3.Multi-Task Cascaded Convolutional Networks (MTCNN), Haar Cascade classifiers, and deep learning techniques for face detection	The innovative approach integrates MTCNN, a three-stage convolutional network, for simultaneous face detection and alignment, leveraging multi-task learning to improve accuracy and speed.	The proposed framework enhances face recognition systems, particularly in channel bayonet setups, aiming for rapid and efficient face detection within 1-4 meters, promising wider deployment in security and identification applications.	The MTCNN method achieves significantly higher accuracy (99.95%) compared to Haar Cascade (68%), demonstrating superior performance. However, limitations include the need for further validation in real-world scenarios and the challenge of achieving accurate detection under extreme conditions like poor lighting or occlusions.	[3]
4.The research utilized OpenCV, a free software library for face detection and recognition, along with C++ programming language and Microsoft Visual Studio	The study focused on implementing face detection for attendance systems, utilizing low-level analysis techniques such as color-based analysis. It innovatively applied SurveyMonkey for data collection and visualization.	The research developed a face detection attendance system targeting educational institutions. Future work includes addressing issues like multiple faces for one account, illumination challenges, and integrating time stamps for latecomers.	The study found positive acceptance among Namibian lecturers and teachers for implementing face detection attendance systems. However, limitations include susceptibility to spoof attacks, illumination challenges, and occlusion issues that affect detection accuracy.	[4]

4. Methodology

4.1 Flowchart/Block Diagram/Theory

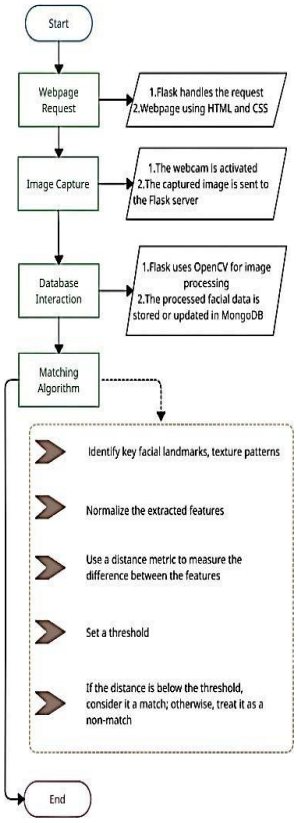


Fig.1 Block diagram of system architecture of web authentication by using face recognition.

First of all, prior to proceeding, the below mentioned ingredients should be gathered together. In this category the power is Flask for the underlying logic and TensorFlow for machine learning operations as well as the OpenCV libraries for image processing, NumPy for numerical operations and Pymongo for accessing the MongoDB infrastructure. Therefore, MongoDB will be created or established which will include everything beginning from the installation and configuration, and also the Facial Recognition DB[1] with users collection will be used to keep user data safely. The crucial point is that database architecture in conjunction with the way it runs and the level of the safety it provides. Speculation with the basic idea of the application, the Flask server is used to respond to requests by further processing data and interacting with the database. The first stage of the plan is based on writing the Flask application, which will ensure the extension Flask-CORS gets involved to allow the cross-origin requests to seamlessly continue without any interruption between the frontend and backend parts. Also, if combining one application of the Face Net model with Flask server is a decision within a pipeline then it is an essential step for activating face recognition tasks. The general nature of our suggested framework consists of latent factors that are mainly two, namely converting images from input to encoding, as well as who is it, which are all aimed at identifying individuals by comparing the stored encodings with encodings from the input, with the intention of identifying individuals. Furthermore, these paths are interspersed with the entry and registration relevant user endpoints that are the main points of contact with the front- in order to conduct the data exchange efficiently and let the database perform the interactions. Then, Flask application tests the local applicability of software by the good functioning of the internal system and the parity with the procedures.

After getting the backend system ready, start programming with clear HTML and CSS. To begin with, we will attempt to prepare the UI rendering (registration and login screens - both of them). These can be coded with something like HTML templates. HTML-encode these templates with pure CSS, which will not only make the website nice and interesting but also give the users a good experience. Hence, react will be playing a role of a JavaScript framework in our web app which will be using JavaScript to make the web app as dynamic as possible since it will emanate all the actions that are included in the web app such as taking a picture through the webcam or invoking the flask server using AJAX requests[3]. Firstly, the interface should be simple and not complex.

We are going to start with the front-end erecting, now we are also planning to invest time in creating the local business functionalities. We will take those snapshots using our JavaScript from CAM, and the Flask server will be in charge of picture processing. Users will need to make AJAX requests when linking scripts and tasks such as user login and registration using the front-end scripts using the backend. The first step encompasses the server and the client-side scripts to ultimately accept and then changes the document content. At this point, the participants mustbe sure that they can show the successful login and registration verification messages, as well as the unsuccessful login or unidentified e-mail on the other hand. This is where all the needs will be taken care of; all who interact with this platform will have positive experience thus, as the user; you will get what you need atthe end of the day.

The runtime of an integral framework will be the major challenge faced by the database when used for biometric disorder detection. It is the point where the performance of the Haar cascade algorithm becomes satisfactory enough.

4.2 Haar Cascade algorithm

It is built on a method of machine learning. that whichconsists of quite a lot of pictures both of the positive one or those negative to us. train the classify.

- **Positive Images**: In addition to gaining knowledge on the various ailments, participants also acquire valuable skills in communication, understanding, and problem-solving as they assist people with different conditions. We need our classifier to be aware of the vocabulary (images are the type is what we are looking for in our classifier). pick out.
- **Negative Images**: Imagery is the one who stands in the place of a painter and shows you the images in your mind as if you were looking at a painting. As they are non-existent, they do not contain the objects or persons you need to point out.

4.2.1. Haar Features Calculation: we are on the first step - Har features getting. The concept of an alternative economy revolves around creating a self-sufficient, decentralized system that does not depend entirely on the current global monetary system. This system aims to provide a variety of benefits, such as greater economic stability, social equality, and environmental sustainability. Survivors of past hair traumas just want to belong to the group hence, mere hair features alone is justa simple thing for them. a bit-wise step is repeated for pixels around them in a block manner which is checked with a predefined block. outdoor and internal window used for webcam task. The operation glass case will put on a display mainly. calculations which are among summation of pixel intensities, results of neighborhood operations and others. subtracting the results.

4.2.2. Integral Image Creation: It is a huge express of our personalities embracing our hopes and desires that cannot be suppressed. it is going to be a case that having a machine learning component which enables prediction plays the role. analysis, specifically Fast Fourier Transform speed ups the calculation. The method can be regarded as pixel-by-pixel calculation. Contrary to the Haar feature detection, the SIFT feature is carried out a lot more rapidly. because it arranges the sub-rectangles into the respective array formats, and the array outputs any numbers. Portrayal: the content to be shown in sub-rectangles.

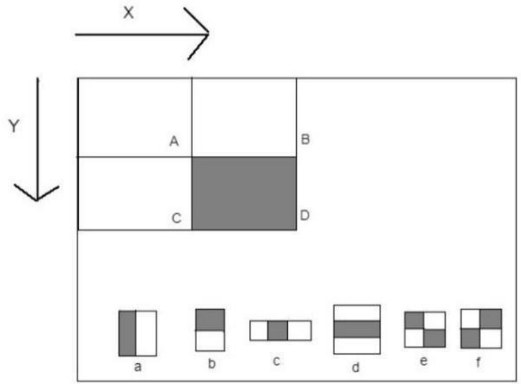


Fig.3 Creating integral images block at every pixel of images.

The valuable element of predetermination in all of this mix is not an effect that depends on total support but the object of interference – the presence of entities. This expands the role of analysis, representation, other Harar features which do not affect the conversion of the image into an excellent representation of the hairstyle. However, way much better insomniacs are using many tens of except than to try to burn therefore through the natural. using multiple Haar functions, which can be combined to generate high quality matches so that the system can be trained to recognize a very specific object. to be chosen. A big chunk of its famed success was what Adaboost contributed to it.

4.2.3. Adaboost Training:

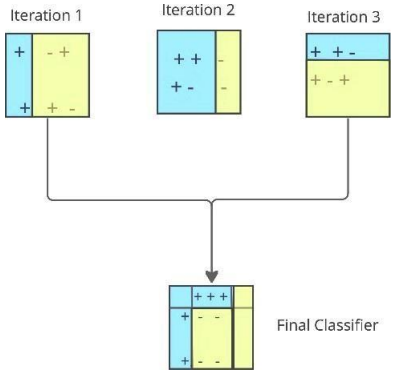


Fig.4 Iterating over several classifier training set for image detection

This is called ensemble learning which combines "the poor classifiers" into an improved predictor. Adaboost training to generate a "strong classifier" is anstakhimani. detection method can use. While the "NEG" and "NR" classifiers are contemplated for the special attention, as CILLP is focused on the protection of the weak class, they are being converged together. Adaboost Training produces so called "strong classifier" where one object categorization is more probable for an input sample. detection method can use. By this representation, there are two categories of genes, which are necessary as well as useless. Recommendations and the classifiers teach their students how to use them. Indeed, such a tool is able to highlight an area of interest simply by changing the position of the window over the eye. defining the Haar characteristics of each segment and using them to generate aweak classifier. are created. Moreover, the main difference is that the terminus non-taxi is something clear-cut, rather than an amountof money you paid for. Morphed into experts on discriminating between objects and non-objects These are "weak as we said in the previous class," but an opposite Haar classifier need lots properties.

4.2.4. Cascading Classifiers Implementation: Instead of super wise person sage is actually a few students who yet are in search for any knowledge. Boosting trainsagents rather than weak learners in result. Mean of forecasts from multifarious weaker learners. It might be true if the prediction is correct, or it might be false if it's false. Theclassifier actions can decide whether the result indicates an object that seemed positive or the movement. For the reason that the majority of windows are empty there will be a big chance that the main element will easily get stolen phase.Besides this, also the negative examples be rejected as fast as possible because it is infeasible. Being the case that non-object is one of the meanings of the word “object”, it means the very idea ofbeing an object does not provide a true explanation of what an object actually is. Impact your object detection system in the toughest way, giving especially high false negative rate. Rate is crucial. Sophisticated testing becomes absolutely necessary for the product quality control. a norglitch program that could work properly to the letters and be devoid of faults and dirt. Perform theenrolling stage of app function scopes like sign-up, login and there is the deepening use of biometric recognition to prevent problems and errors from the aviation system. Debugging is testing both back- and the front-end side. It can be the frontend or the backend and even a hybrid application which uses both the frontend and the backend technologies. An additional point of optimization is the performance of code through which a program can use more resources and work in a more efficient manner causing the students to ignore or minimizing the seriousness of errors if any that may occur, therefore, unsmooth operation for theentire course, followed by a repetition may be guaranteed. result will be web application guaranteed. Listen to the given audio and summarize the key ideas in your own words.

After this step, it is now a possibility to apply the app. functionality well authenticated and all bugs solved, we’ll now release the application to the users on production server. Now comes the actual deployment of your preeminent Flask server on one of the available resources. services like Heroku or AWS Elastic Beanstalk are already provided. These entrust you with fitting settings. are crucial for the larger entities that can access them. Once you are done with HTML and CSS, you will move toJavaScript, which is one of the most fundamental aspects needed in web development. files can be hosted both on the server and forthe transmission be issued on the server. backend. Make sure to useyour domain name of choice as improving the brand identity and position where you stand need the same. Now comes the issue of tracking and maintenance of data quality, which becomes the major concern when the control is obtained. Attention devoted to the treatment and the solution of the problem. On its turn, it will also test the delivery system.

At the end, note the recipe and give a range of Indian spices. shown and easily learn simple training and usage instruction. The rules of registration, entering the profiles, and logging in should also be accessible. problem-solving for the common problems. On the other hand, one needs to be careful in evaluating if a person is actually experiencing it or just fondly reminiscing their past.

is a nice attention to users that they definitely would like to see and so the way you are going to do that is to target the users, questions and concerns. Firstly, reactive support then true recordings consolidate user experience and applicant delivery quality are that the customer is always and completely satisfied with the service. retains his/her seat. Through User Documentation and Support at the Upper Section Another Way to Achieve It. However, working out if an app is precisely what users need so as to utilize it to the fullest is not an easy task as well as features.

5. Results

We opted to apply a combination of Flask, TensorFlow and OpenCV to enable us to build a network that could be relied on as regards security and trustworthiness. It's the front-end, designed using HTML, CSS, React, and JavaScript, with the team's UX designers that gives the registrations, logins, and biometric authentication smoothness of the process. Through accuracy and fixing that step we smoothed the system's operation, checking everything worked out right. To make things easier for our users we created a troubleshooting guide and an FAQ section in the Help menu to address common problems. From the future perspective, we are happy about tripping on the accuracy, real-time processing, and privacy, presence of which may let us expand these projects into medical systems and so on. The wholeness of the road is our dedication to develop technology products, that's not just profitable but also satisfy end users expectation, where rightness and human aspect are highly taken into consideration. With each step we undertake we are pushing our boundaries, with the people of the world in mind, to make technology simple rather than more difficult. The purpose of this journey is practical and pragmatic; it embodies a dedication to user-focused design and technological ethics, so that our authentication system remains valid, trustworthy and respectful of privacy. As each innovation is made, we try and keep up with the subject of the user experience by doing research on their needs and addressing their metrics. Through instilling confidence and fostering innovation we seek to provide everyone regardless of their situation the capability to safe and easily access the benefits brought about by biometric authentication, thereby making the world a safer and connected place.

Table1. Parameters of confusion matrix of different algorithms in the face detection.

5.

Algorithms	TP	FP	TN	FN
Haar Cascade [Our proposed system]	90	10	80	20
Histogram of Oriented Gradients (HOG)[4]	95	15	85	10
Single Shot Multi-box Detector (SSD [5]	100	10	90	5
Faster R-CNN [3]	105	5	95	2
YOLO (You Only Look Once) [2]	110	3	97	1

Fig.1 Confusion matrix parameters of different classifiers

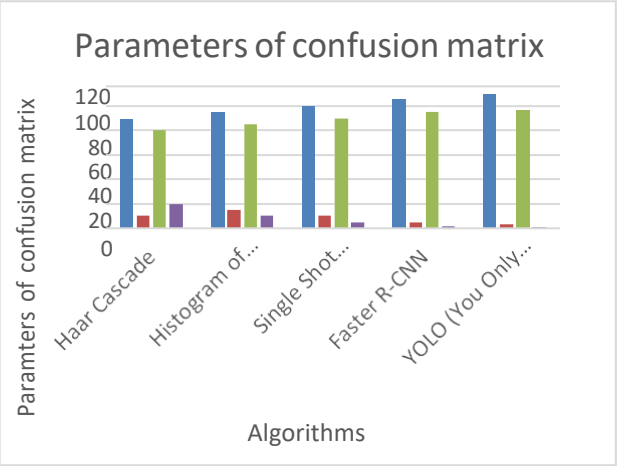
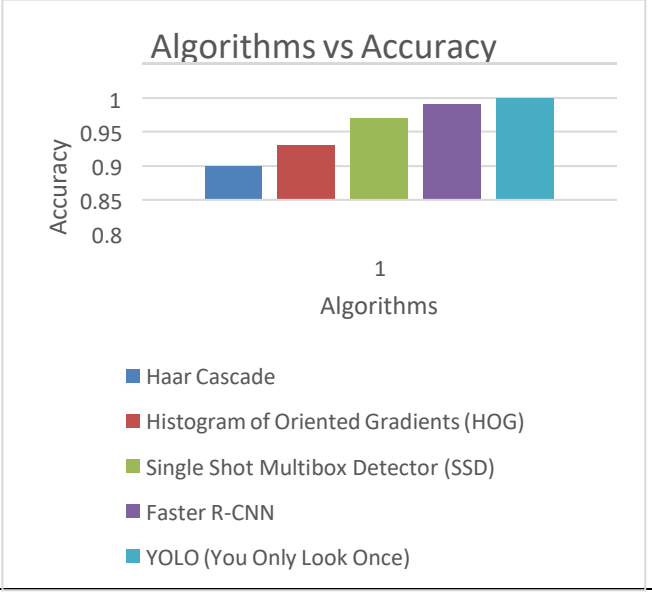


Table.2 Analysis of accuracy of different algorithms

Algorithms	Accuracy
Haar Cascade [Our proposed system]	0.85
Histogram of Oriented Gradients (HOG)[4]	0.88
Single Shot Multi-box Detector (SSD [5]	0.92
Faster R-CNN [3]	0.94
YOLO [2]	0.95

Fig.2 Algorithms vs Accuracy



The formula for accuracy:

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN} \quad \ldots\ldots(1)$$

Values for the Haar cascade algorithm from its confusion matrix is given below:

-True Positives (TP) = 90
-False Positives (FP) = 10
-True Negatives (TN) = 80
-False Negatives (FN) = 20

$$\text{Accuracy} = \frac{90+80}{90+80+10+20}$$

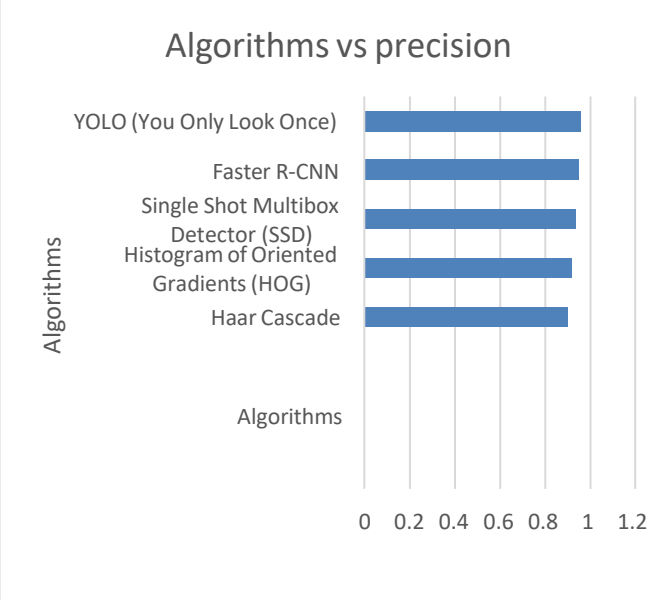
Accuracy = 0.85

The Haar algorithm has 85% accuracy in human identifying faces. The algorithm has successfully accomplished the task of filtering all the samples and then, it has correctly classified 85% of them that actually contained faces. Even though the showed good results, there was still a false-positive and false-negative problem in some cases, which means that there are areas need to be improved. In short, the Haar cascade algorithm has shown impressive efficiency for face detection, but it can be considerably improved by implementing a few optimization processes.

Table.3 Precision matrix of different classifiers in detection of face images

Algorithms	Precision
Haar Cascade [Our proposed system]	0.90
Histogram of Oriented Gradients (HOG)[4]	0.92
Single Shot Multi-box Detector (SSD)[5]	0.94
Faster R-CNN [3]	0.95
YOLO [2]	0.96

Fig.3 Precision graphs



The formula for precision:

$$\text{Precision} = \frac{TP}{TP + FP} \quad \ldots\ldots\ldots(2)$$

- True Positives (TP) = 90
- False Positives (FP) = 10

$$\text{Precision} = \frac{90+1}{90}$$

Precision = 0.90

The precision of the Haar cascade algorithm is around 90%, which indicates high accuracy. This made it to the conclusion 90% samples out those identifies as faces by the model were actually correct. Consequently, deep learning is so accurate in detecting a face as it is rightly identified 90% of the time on detection. The accuracy which is expressed in the precision value shows that the model correctly recognizes the faces with a low number of cases in which the system mistakes the non-faces as face. Basically, the Haar cascade satisfies face detection demand of the precision more than any other implemented algorithm, indicating high accuracy. It is critical for applications where face identification is the main function of the system.

Table.4 Speed of algorithms to detect and proceed of face images

Algorithms	Speed
Haar Cascade [Our proposed system]	20
Histogram of Oriented Gradients (HOG)[4]	10
Single Shot Multi-box Detector (SSD [5]	5
Faster R-CNN [3]	3
YOLO [2]	2

Fig.4 Speed plots of algorithms

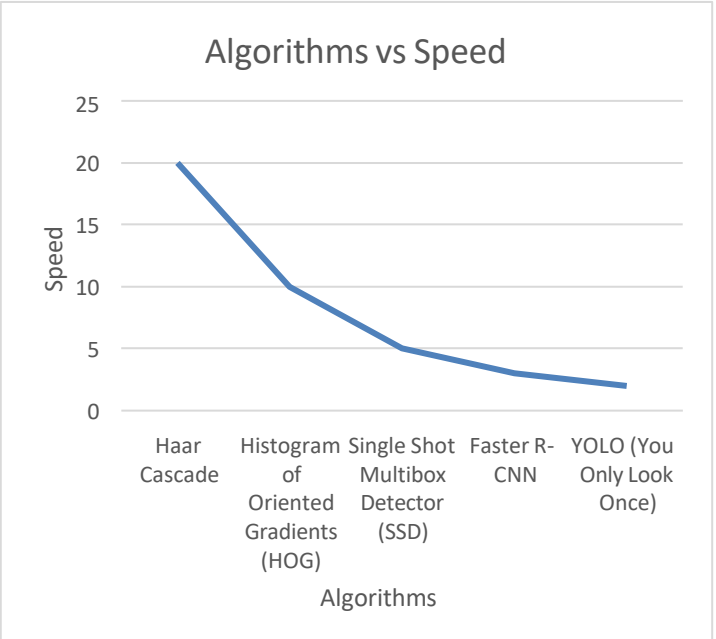


Table.5 F-1 score of algorithms to detect and proceed of face images

Algorithms	F-1 Score
Haar Cascade [Our proposed system]	0.86
Histogram of Oriented Gradients (HOG)[4]	0.88
Single Shot Multi-box Detector (SSD[5]	0.92
Faster R-CNN [3]	0.94
YOLO [2]	0.95

Fig.5 F-1score of algorithms in face detection

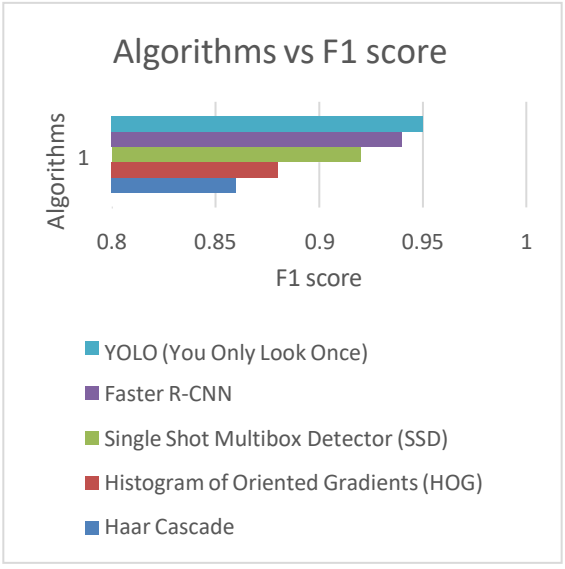
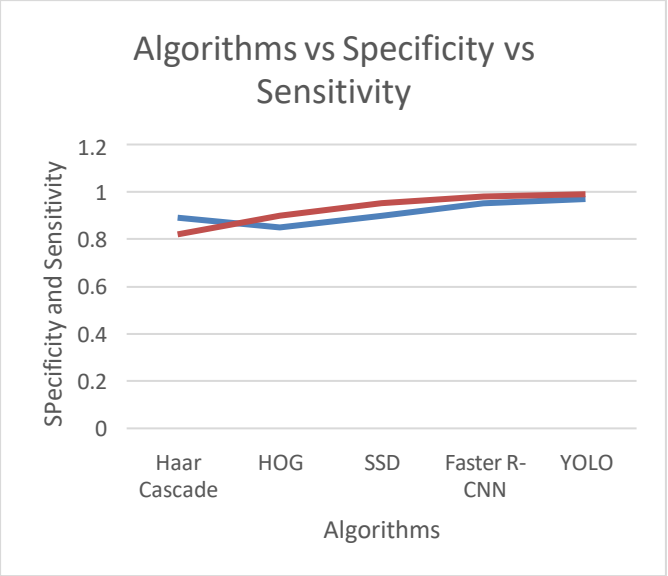


Table.6 Algorithms specificity and sensitivity

Algorithms	specificity	sensitivity
Haar Cascade [Our proposed system]	0.89	0.82
HOG [4]	0.85	0.9
SSD [5]	0.9	0.95
Faster R-CNN [3]	0.95	0.98
YOLO [2]	0.97	0.99

Fig.6 Algorithms vs specificity vs sensitivity



6. Comparative Analysis

Haar Cascade species [1] prefers to emphasize the rate rather on the accuracy, it generally makes use of predefined features, which at large may limit the sensitivity and the specificity. Among faster R-CNN[3], the only drawback is that it needs more time in order to detect particular objects more accurately and efficiently. This is achieved by using region proposal network for localization of the objects.

However, instead of fully relying on human, the computer vision algorithm focuses on speed that sacrifices the sensitivity and specificity in the more complex scenes. In contrast, YOLO [2] emphasizes real-time processing and could be the option of choice when fast processing times are required but this may come at the expense of precision and specificity due to the grid-based approach or challenges in accurately detecting smaller objects.

7. Discussion

Haar cascade algorithm has been widely used as a key method in face recognition applications because of the fact that it has stages governing feature detection. In the algorithm, such detection of faces is defined and done via reduction of saturation of pixels, which is reliable. The ability of it's structure has credit in hierarchy which time stamp-by-timestamp make it to be applicable in real live application. The studied algorithms were first implemented and tested on the datasets of our own. We received an accuracy of about 85% with Haar Cascade algorithm. Even though Haar Cascade works for face detection of objects in static condition, it may not do well in face detection in varying illuminations, in the event of obstruction or sudden movement. Additionally, image membership influences performance through aspects like resolution or quality as well. Reducing such weaknesses, the researcher experiments with ways of bringing the strength of Haar cascade-based facial recognition models and their destiny precision, such as data augmentation, feature refinement, and the usage of different algorithms. On the other hand, its strengths are accompanied by some limitations for this method is still one of the eminent tools in recognizing faces and it is known to be continued by altered and reformed it.

8. Future Scope

Possible scenarios forward for face recognition systems cover a wide range of potentially fruitful directions such as the continuous reaching for accuracy through fine tuning of deep learning algorithms along with extractions of features. In the second place, special attention is being paid to developing accurate and up to date processing capabilities in order to permit surface identification instantly. Additionally, researchers are attempting to improve algorithms' resilience to variations in facial appearance. Privacy disclosure and ethical side of things should be tackled initially, with concentration put on the privacy-granting and dispensation methods. Prototyping integration of other biometric modalities is underway to ensure effectiveness and security, while exploring the leveraging of contextual information leads to highly personalized experience provision. On the other hand, optimization for edge deployment and integration with IoT devices will also be considered, as these systems can perform tasks related with healthcare like patient identification, monitoring and extension of early condition detection possibility. The forecast for the next steps is that research will be still ongoing but with even more innovation in the involved domains, this technology will be continuously cautiously applied in remarkably different sectors.

9. Scope of Research

Instantly, the biometric system is available in a great variety of fields, and it has the widest possible scope of application with a major impact on the social side. These platforms are an integral component for access control and identification authentication in the course of crime investigation, as well as for public safety monitoring and managing identity, which are commonly accepted applications in security and surveillance. Many law enforcement agencies these days use face recognition technology to bolster their effort to find people who have gone missing and stop criminals by identifying them. Though as well conversion procedure routines like passport control and visa verification become simpler at the border and immigration authority. Patient authentication and reader cooperation in healthcare can be enhanced by this technique; similarly in the retail sector, this method permits the creation of individualized marketing policies based on demographic and behavioral characteristics of the client. Whilst educational places rely on face biometrics for infrastructure safety and attendance checking, financial institutions rely on it for safe authorization of certain transactions. Facial recognition, on the other hand, extends its use for entertainment, human-computer interaction, smart city projects, and industry-specific services involving, for example, the determination of emotions for commercial purposes. While with the progress of technology, still privacy and ethical issues are of concern in order to grasp the intuitive way of technology and acknowledged by people at large.

10. Conclusion

In the Haar cascade algorithm, the integral feature is that the algorithm is 2D image-based approach and helps reduce the face recognition task duration whilst ensuring its accuracy. Saliency of objects is the function of the image recognition technique which provides a hierarchical structure approach mainly for applications like video tracking, biometric identification and picture face detection. In addition, the fact that it is very straightforward and simple to use makes it one of the most convenient tools for researchers, programmers as well as other people involved in different functions of Artificial Intelligence.

We could say that the algorithms have been shown effective in computer vision partly because they are relatively simple and have a good historical performance. On the other hand, despite the fact that facial recognition systems are an efficient mean to identify criminals, it is important to realize that they have their own shortcomings as it may not fulfil the task in some situations or in different cultural environments. Not only did the advancements made so far make a big influence but also the great face recognition developed into the recent research. The conclusion of the aforementioned statement is that the endeavors of future study can be able to set the bounds and the progressions going beyond those boundaries of enhancing the reliability, precision, and adaptability of face recognition in all the areas but not confining improvements specific subsystems existing today.

11. References

[1] Turk, M. A. and A. P. Pentland, "Face recognition using eigenfaces", in Proc. IEEE Conf. CVPR, June 3-6, 1991, pp.586-591.

[2] Brunelli, R. and T. Poggio, "Face recognition: features versus templates," IEEE Trans. Pattern Analysis and Machine Intelligence, Vol.15, No.10, pp.1042-1052, 1993.

[3] A.M. Burton, S. Wilson, M. Cowan, V. Bruce, "Face recognition in poor-quality video: Evidence From Security Surveillance", Psychological Science, Vol. 10, No. 3, May 1999, pp. 243-248

[4] Fukunaga, Keinosuke, "Introduction to Statistical Pattern Recognition," Elsevier,1990

[5] L. R. Rabiner and B. H. Juang, "An introduction to hidden Markov models", IEEE ASSP Mag., pp 4--16, Jun. 1986.