Web-Based Facial Recognition System

Gande Sai Teja, Mohammed Adnan, Gilla Samanth, Motupally Chaithanya

Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Hyderabad-500075, Telangana, India.

Abstract

A web-based facial recognition system is a software application that uses facial recognition technology to identify individuals from their facial features. This system is accessible through a web browser and can be used for various purposes, such as security, identification, and authentication. The system works by capturing an image of a person's face using a camera or uploading a preexisting image. The system then analyzes the facial features, such as the distance between the eyes, the shape of the nose, and the contours of the face, to create a unique biometric template. Web-based facial recognition systems have a wide range of applications, including security, border control, access control, and customer service.

Introduction

Face recognition is a popular and important technology integrated in many applications such as payment, door unlock, video monitoring systems, etc. A face recognition system is a technology that can identify and verify people from digital images and footage. The state-of-the-art face recognition approaches for web authentication include luxury and simplified from electronic Sid. These are both provided as commercial products. To recognize faces (human faces), Images are taken using a digital camera. the first step is to perform face detection, this is performed as a preprocessing step to locate the face in an image. Web-based facial recognition system is a software application that uses advanced biometric technology to identify individuals through their facial features. It is a rapidly growing field with applications in various sectors such as security, identification, and authentication. With the increase in demand for quick and accurate identification methods, web-based facial recognition systems have become a popular solution for many businesses and organizations. The system works by analyzing the unique features of an individual's face, such as the distance between the eyes, the shape of the nose, and the contours of the face, to create a biometric template that can be used for identification purposes.

Methods and Materials

The process begins by capturing an image of a person's face using a camera or uploading a pre-existing image. The system then uses algorithms to analyze the facial features and create a biometric template that is unique to that individual. The biometric template includes information such as the distance between the eyes, the shape of the nose, and the contours of the face. This template is then compared to a database of stored templates to identify the individual. If there is a match, the individual is identified and authenticated..

Figure 1.

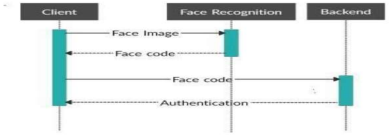
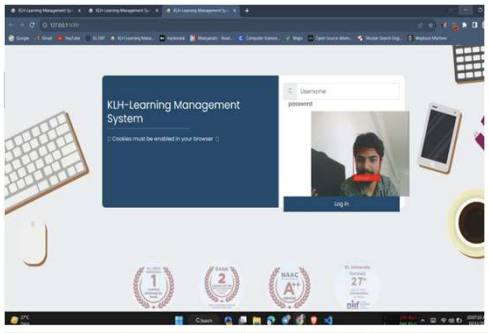
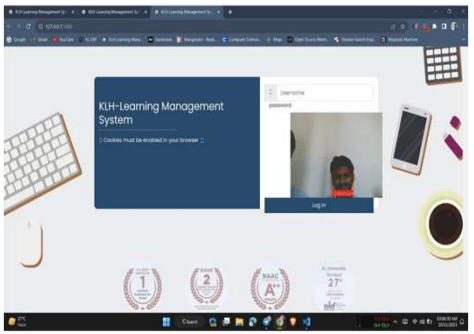


Figure 2.

Results

A web-based facial encryption system using AES and CNN typically involves several components, including a web interface, image capture, facial detection, facial recognition, AES encryption, and database storage. The system allows users to capture and encrypt facial data and later decrypt it based on their authentication. Expected Results: Facial Detection: The CNN-based facial detection model should accurately locate and identify faces within the captured images. The expected result is bounding boxes or regions around detected faces. Facial Recognition: The CNN-based facial recognition model should be able to recognize individuals' faces and authenticate users. The expected result is a match or a confidence score indicating the likelihood of a match. Protection against password list and phishing., Password theft is not possible with facial authentication, It protects against brute force attacks, It enhances your cyber security posture, User no need to remember any passwords.





Discussion

As this technology continues to advance, it is important for businesses, organizations, and policymakers to keep up with the latest developments and ensure that facial recognition technology is used in a way that is transparent, fair, and respectful of individuals' privacy and rights. By doing so, we can continue to benefit from the convenience and security provided by this technology while avoiding its potential pitfalls. The responsible development and use of this technology can help to enhance security and convenience, but it must be done in a way that does not violate individual rights and freedom.

Conclusions

In conclusion, web-based facial recognition systems are a rapidly growing technology that offers many benefits for various sectors, including security, identification, and authentication. These systems use advanced biometric algorithms to analyze unique facial features and create a biometric template that can be used for identification purposes. However, the use of facial recognition technology also raises concerns around privacy and surveillance. Therefore, it is essential to carefully consider ethical and legal issues when developing and deploying web-based facial recognition systems. The implementation of appropriate safeguards is crucial to protect the privacy and rights of individuals. The responsible development and use of this technology can help to enhance security and convenience, but it must be done in a way that does not violate individual rights and freedoms.

Future Directions

Therefore, it is essential to carefully consider ethical and legal issues when developing and deploying web-based facial recognition systems. The implementation of appropriate safeguards is crucial to protect the privacy and rights of individuals. The responsible development and use of this technology can help to enhance security and convenience, but it must be done in a way that does not violate individual rights and freedoms.

Contact Information

G.Saiteja (2010030055)
Md.Adnan (2010030236)
G.Samanth(2010030272)
M.Chaithanya (2010030366)

References

1. Abbadi, I.M., Alawneh, M., 2012. A framework for establishing trust in the Cloud. Comput. Electr. Eng. 38 (5), 1073–1087.
2. Abbadi, I.M., Martin, A., 2011. Trust in the Cloud. Inf. Secur. Techn. Rep. 16, 108–114.
3. Adjei, J.K., Blackman, C., Blackman, C., 2015. Explaining the role of trust in cloud computing services. Info 17.

Acknowledgements

We would like to thank the following people for their support and guidance without whom the completion of this project in fruition would not be possible. Dr.P Sree Lakshmi, our project guide, for helping us and guiding us in the course of this project . Dr.Arpita Gupta, the Head of the Department, Department of Computer Scinece And Engineering. Our internal reviewers, Dr.P Sree Lakshmi , Dr.Sumit Hazra , Dr.SR Muguntan for their insight and advice provided during the review sessions.