



(REVIEW ARTICLE)



Secured personal notes using face recognition-based decryption

Anshid K T * and R. Vadivel

Department of Information Technology, Bharathiar University, Coimbatore, Tamil Nadu, India- 641046

World Journal of Advanced Research and Reviews, 2023, 18(01), 668–672

Publication history: Received on 27 February 2023; revised on 09 April 2023; accepted on 11 April 2023

Article DOI: <https://doi.org/10.30574/wjarr.2023.18.1.0594>

Abstract

Data are kept in our local database and used by the Android Note program. The data for this project was stored in a cloud database, and anyone with the necessary login information can view the data from any device. The data is encrypted using a monoalphabetic substitution cipher encryption method, which is also used for decryption, to increase security. However, the decryption process adds an extra layer of security with the aid of a machine learning model. The program requests that the user's face be recognized in order to the data decrypted; otherwise, data cannot be decrypted. Cloud-based info will be encrypted and kept safe.

Keywords: Cloud Database; Decryption; Encryption; Firebase; Private Note.

1 Introduction

A real-time Android application for taking notes for personal use is used in this work, along with a cloud storage facility and an encryption algorithm for data security. Additionally, the MIT platform's Cloud DB for data storage and App Inventor to build an entire application are both used. Data encryption and decryption is performed using a monoalphabetic substitution cipher.

2 Literature Survey

Information security is enhanced using a variety of cipher techniques, including monoalphabetic and polyalphabetic cipher. By using cryptography, readable communications are rendered unreadable. Vigenere cipher is the most widely used cipher polyalphabetic methods. Although the Vigenere encryption has been around for a while, it has flaws. Because the encryption calculation only uses additive cipher, this algorithm is susceptible to attacks based on letter frequency analysis. The research's suggested approach entails combining the Vigenere encryption with a monoalphabetic cipher to increase its complexity [Kurniawan Muchamad(2019)]. A lot of introductory cryptology and computer security courses begin with or include a discussion of classical ciphers, which typically considers some cryptanalysis methods used to break them. An program called Ganza (picklock in Spanish) is made to help with the decryption of ciphertext generated by mono- or polyalphabetic ciphers. It can acquire the standard relative frequencies of many languages, use virtually any character set for the plain and cipher alphabets, and provide other useful information [Jose Galaviz (2006)].

The realm of facial recognition applications has been rapidly growing and evolving, with numerous algorithms being developed over time. However, in our research, we have employed a HOG face detector, unlike other machine learning algorithms like Haar Cascade, as it yields more accurate outcomes. We have implemented Contrast Limited Adaptive Histogram Equalization for preprocessing the data during the identification process, which helps in contrast enhancement and noise reduction. In addition, we have utilized HOG for feature extraction, which is a commonly used

* Corresponding author: Anshid K T

technique. We have extracted HOG features for both the training and test images. Our classification technique involves the use of SVM (Support_Vector_Machine) that is given the HOG features. The process approach used helps in improving illumination, contrast, and noise reduction. Finally, our research concludes by evaluating the pros and cons of improved face recognition performance. [Raktim Nath, Kaberi Kakoty, Dibya jyoti Bora, Udari Welipitiya(2021)].

Facial recognition technology has become increasingly prominent in the fields of defense and crime prevention. However, the development of mobile applications for on-site use has presented several challenges, including limited storage and processing capabilities, security and privacy concerns, and unstable network connections with limited bandwidth. To address these issues, a novel approach has been proposed that uses a compression method based on the discrete cosine transform (DCT) to create a compressed image database that can be stored easily on mobile devices. This compressed database allows face recognition algorithms to run directly on it, without the need for decompression [Mukherjee, Shibnath (2008)].

This study proposes an innovative and robust approach to facial recognition technology. The system uses a combination of skin color detection, light normalization, and normalized cross correlation techniques for face detection, while principal component analysis (PCA) is employed for face verification. To ensure user data confidentiality, the Advanced Encryption Standard (AES) is utilized for encryption. For every user, a unique encryption/decryption key is generated and not saved in the database but extracted by expanding the submitted user identification (ID). To enhance the security of the AES algorithm, the researchers employ a simulation using field programmable gate array (FPGA) and very high-speed integrated circuit hardware description language (VHDL). [Abdel-Ghaffar, Eman A(2008)]

3 Methodology

3.1 Machine Learning

Artificial intelligence (AI) refers to capability of machines or computer systems to perform tasks that require intelligent human behavior. These systems are designed to solve complex problems similar to how humans do. One of the examples of AI is machine learning, which is responsible for the creation of various applications such as predictive text, chatbots, and personalized social media feeds. Machine learning also powers equipment used to detect medical problems through photos and the development of autonomous vehicles.

In the educational field, assisted instruction (AI) has been used for years to support the learning process with the aid of computer systems. However, with the advancement of AI technology, intelligent computer-aided instruction (ICAI) has replaced assisted instruction. ICAI uses AI techniques to develop automated teachers that can adjust the teaching methods to cater to each student's unique learning style. This study paper provides an in-depth analysis of machine learning and artificial intelligence through a comprehensive review of current literature. The goal is to equip information workers with the necessary knowledge to use AI technology effectively in their studies and teaching. [Ku. Chhaya A. Khanzode and Dr. Ravindra D. Sarode(2020)].

3.2 Personal Image classifier

Image classification is used in this project the task of categorizing and labeling groups of images or vectors within an image based on predetermined criteria can be accomplished through image classification. This involves the use of algorithms and techniques to assign predefined categories or labels to the images or vectors, based on certain characteristics or features identified within the data. One or more criteria may be used to give a label. Single-label image categorization is an option.

An improved multimodal personal identification method is suggested for improved mobile device security. The suggested method combines data from speech, teeth, and facial sources to enhance performance. We use a variety of fusion methods, including weighted-summation rule, K-NN, Fisher, and Gaussian classifiers, to combine three senses, and they assess the effectiveness of the suggested system's authentication. A collection of 1000 biometric characteristics that correlate to the visage, dentition, and vocal modalities of 50 people is used to assess the performance [D. -J. Kim, K. -W. Chung and K. -S. Hong (2010)].

3.3 Encryption and decryption

Encryption is a technique used to render a readable message unintelligible to unauthorized parties by converting it into an unreadable format. The procedure of converting an encrypted message is known as decryption. Fig. 1. Likewise emphasises methods for picture encryption, How to safeguard the privacy, integrity, and validity of pictures becomes more crucial as digital methods for transmitting and saving images are used more frequently. Various methods for

encrypting pictures are continuously being developed to increase their security [Pakshwar, Rinki, Vijay Kumar Trivedi, and Vineet Richhariya(2013)].

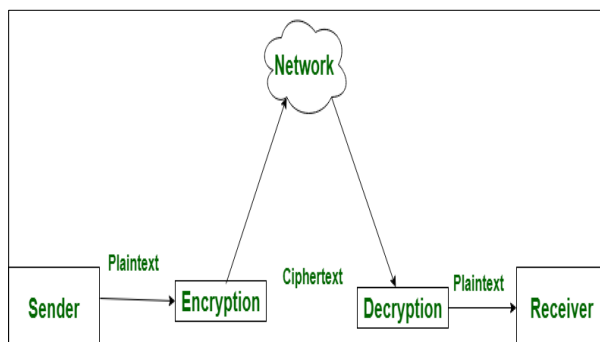


Figure 1 Encryption and decryption

3.3.1 Encryption

Encryption is a security technique that can be utilized to obfuscate data, ensuring that it can only be understood by authorized parties. In essence, encryption involves transforming human-readable plaintext into incomprehensible ciphertext, as shown in Fig.2.

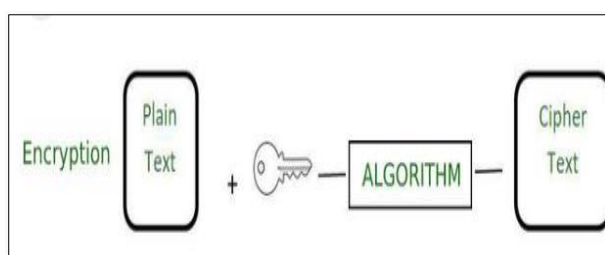


Figure 2 Encryption which information is transformed into a code to conceal its real meaning

3.3.2 Decryption

Decryption is a critical process that involves the conversion of encoded or encrypted data into readable and understandable text, either by a computer or a human. This term can refer to various methods, including direct decryption techniques or the use of appropriate keys or codes to decrypt the data. As depicted in Fig. 3, decryption plays a crucial role in ensuring the confidentiality and integrity of sensitive information.

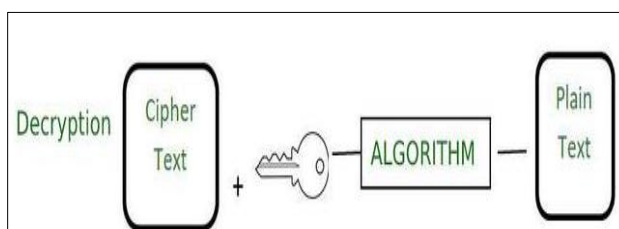


Figure 3 Decryption which is the process of decrypting data and returning it to its initial shape.

3.4 Face recognition model score based on decryption

The user can decrypt the message which is stored in the database but he has to undergo a machine learning test which takes the user's face as input and predicts the model score. The model score should be high as 0.9 or above to pass the test to start the decryption. The model score usually will be around 0.8 to 0.99 for a good image and approximately 0.5 to 0.7 for average images. But we need to ensure the user's identity is highly matched. So we are taking 0.9 as the base model score to pass the test to decrypt the data. Modern educational institutions are increasingly concerned with ensuring that their students achieve consistent success. One of the factors that can contribute to a decline in pupil achievement is insufficient attendance. Traditional methods of attendance monitoring, such as signing attendance

sheets or contacting individual students, were time-consuming and often inaccurate. There is a growing need for computer-based attendance monitoring systems that can efficiently and accurately record attendance. In this study, we propose an intelligent attendance system based on facial recognition technology. We recommend implementing a "Smart Attendance System for Face Recognition" that can offer multiple benefits to educational institutions. By utilizing facial recognition technology, the present application includes a system of face authentication that can significantly reduce the time required for attendance monitoring and effectively eliminate the possibility of proxy attendance. [Raj, A. Arjun, et al (2020)]

4 Workflow

First here create a new user secured by firebase and let login when authentication is successful. After the authentication, it enters a new page where can enter notes. These entered notes will store in the cloud by encrypted. The encrypted notes will decrypt using a personal image classifier. In face recognition, If the model score is greater than 0.9, it will decrypt otherwise it displays that the user is not found or try again later. Fig. 4.

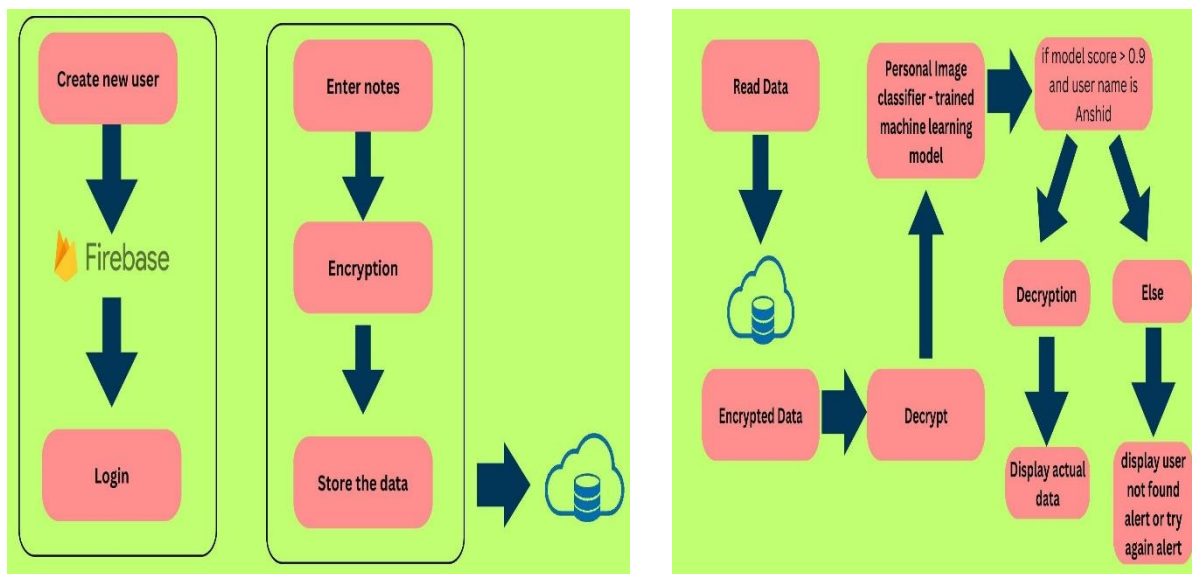


Figure 4 Work flow of the entire project.

5 Conclusion

There is also a security layer for decryption incorporated in this suggested system. We have employed the Monoalphabetic Substitution Cipher encryption method for cryptography. The decoding process is also the same, but the system decrypts the data using a machine learning algorithm that has already been taught. Since we are in the age of AI and ML, we can also apply its features to better improve the security of current systems. It can be used for a variety of real-time apps.

Compliance with ethical standards

Disclosure of conflict of interest



No conflict of interest.

References

- [1] Kurniawan Muchamad, Modified Vegenerer Cipher to Enhance Data Security Using Monoalphabetic Cipher at 2019 International Journal of Artificial Intelligence & Robotics (IJAIR).
- [2] Jose Galaviz, A Cryptanalysis Tool for Monoalphabetic and Polyalphabetic Ciphers at 2006 Journal on Educational Resources in Computing

- [3] Raktim Nath, Kaberi Kakoty, Dibya jyoti Bora, Udari Welipitiya, Face Detection and Recognition Using Machine Learning at 2021 UGC Care Journal. Bharat, K.; Broder, A. (1998): A technique for measuring the relative size and overlap of public Web search engines. *Computer Networks*, **30**(1–7), pp. 107–117.
- [4] Sudha Sharma, Mayank Bhatt, Pratyush Sharma Face Recognition System Using Machine Learning Algorithm at 2020 5th International Conference on Communication and Electronics Systems (ICCES)
- [5] Mukherjee, Shibnath, et al. "A secure face recognition system for mobile-devices without the need of decryption." *Workshop on secure knowledge management*. 2008.
- [6] Abdel-Ghaffar, Eman A., et al. "A secure face recognition system." 2008 International Conference on Computer Engineering & Systems. IEEE, 2008.
- [7] Ku. Chhaya A. Khanzode and Dr. Ravindra D. Sarode, Advantages and Disadvantages of Artificial Intelligence and Machine Learning: A Literature Review, *International Journal of Library & Information Science*, 9(1), 2020, pp. 30-36.
- [8] D. -J. Kim, K. -W. Chung and K. -S. Hong, "Person authentication using face, teeth and voice modalities for mobile device security," in *IEEE Transactions on Consumer Electronics*, vol. 56, no. 4, pp. 2678-2685, November 2010, doi: 10.1109/TCE.2010.5681156.
- [9] Pakshwar, Rinki, Vijay Kumar Trivedi, and Vineet Richhariya. "A survey on different image encryption and decryption techniques." *International journal of computer science and information technologies* 4.1 (2013): 113-116.
- [10] Raj, A. Arjun, et al. "Face recognition based smart attendance system." 2020 International Conference on Intelligent Engineering and Management (ICIEM). IEEE, 2020.

Author's short biography

	<p>Anshid K T received Bachelors Degree in Computer Science in the year 2018 to 2021 from MES Kalladi College mannarkkad, Palakkad, Kerala, Afailiated to Calicut University. He is currently pursuing a Masters Degree in Information Technology from 2021 to 2023, at Bharathiar University, Coimbatore, Tamil Nadu. His area of interest is Python in Machine Learning</p>
	<p>Dr.R.Vadivel is an Associate Professor, in the Department of Information Technology, Bharathiar University, Tamil Nadu, India. He received his Ph.D degree in Computer Science from Manonmaniam Sundaranar University in the year 2013. He obtained his Diploma in Electronics and Communication Engineering from State Board of Technical Education in the year 1999, B.E., Degree in Computer Science and Engineering from Periyar University in the year 2002, M.E., degree in Computer Science and Engineering from Annamalai University in the year 2007. He had published over 96 journals papers and over 40 conferences papers both at National and International level. His areas of interest include Information Security, Data mining, Digital Signal Processing</p>