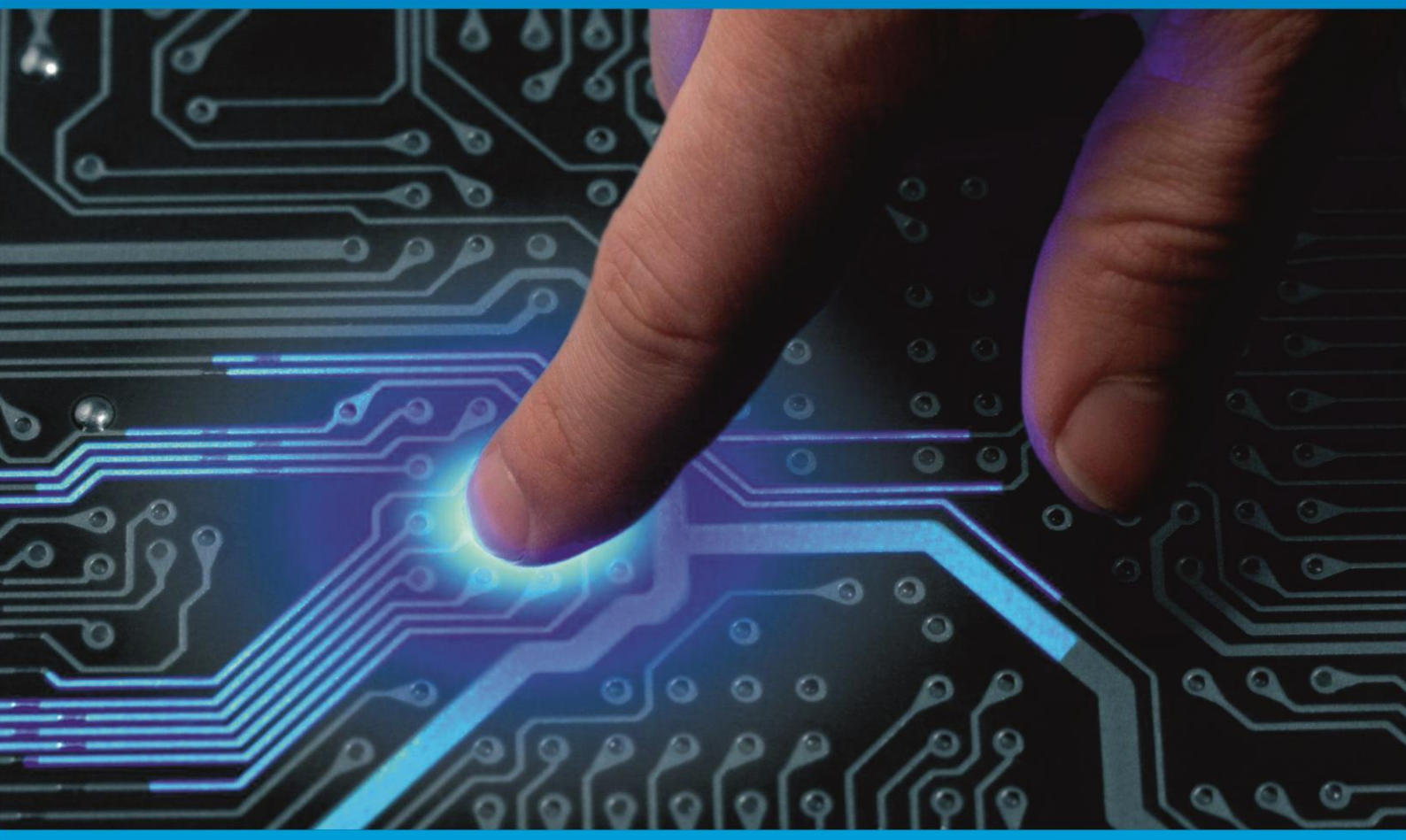
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 5, May 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.488

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905219 |

Implementation of Secure Bio-metric Authentication with Facial Recognition

Awari Abhijit, Andhale Ambadas, Khemnar Rutuja, Gosavi Archana, Chavan Mayuri, Prof. S. A. Thanekar

Department of Computer Engineering, Amrutvahini College of Engineering, Sangamner, Ahmednagar, Maharashtra

ABSTRACT: It has been shown that face images can be reconstructed from their representations (templates). We propose a randomized CNN to generate protected face biometric templates given the input face image and a user-specific key. The use of user-specific keys introduces randomness to the secure template and hence strengthens the template security. To further enhance the security of the templates, instead of storing the key, we store a secure sketch that can be decoded to generate the key with genuine queries submitted to the system. We have evaluated the proposed protected template generation method using three benchmarking datasets for the face (FRGC v2.0, CFP, and IJB-A). The experimental results justify that the protected template generated by the proposed method are non-invertible and cancellable, while preserving the verification performance.

KEYWORDS: Biometric, template security, deep templates, template protection, randomized CNN, protected templates.

I. INTRODUCTION

BIOMETRIC recognition systems are being widely deployed in security sensitive (e.g.,personal devices1 and border security2) and privacy aware applications (banking3 and patient ID4). It is critical to protecting the biometric data stored in the system because biometrics is unique and irrevocable once it is compromised. To ensure the security and privacy, biometric vendors generally store biometric templates, representations of raw biometric data (e.g., face images), instead of raw biometric data in the systems. However, recent studies show that, raw biometric data can be reconstructed from plaintext biometric templates and then used to access the target system and identify the target users . Thus, biometric templates stored in the systems have to be protected. One straightforward approach to protect biometric templates is to use standard ciphers such as SHA-3. However, due to the intra-subject variation in biometric templates and the avalanche effect of standard ciphers, biometric templates must be decrypted before comparison5 . This is different from traditional passwords that can be compared in their encrypted (hash) form. Another possible cipher for the protection of biometric templates is homomorphic encryption. Such encryption approaches compare templates in their encrypted form to give the encrypted results, which are then decrypted to yield the decision. However, homomorphic encryption is computationally expensive, especially for high-dimensional biometric templates. It also suffers from the same key management issue as most homomorphic encryption construction , in which the decryption key of the encrypted results can be used to decrypt the encrypted templates. An alternative approach is the use of biometric template protection schemes , which generates a pseudonymous identifier (PI)6 and auxiliary data (AD)7 from the plaintext enrolment template and store them in the systems. During authentication, the stored PI is compared directly with the PI* generated from the query template and the stored AD.

II. RELATED WORK

A. Multi-scale feature extraction for single face recognition

The Single sample face recognition has always been a hot but difficult issue in face recognition. By considering selecting robust features and generating virtual samples simultaneously, the paper proposes a multi-scale support vector transformation (MSSVT) based method to generate multi-scale virtual samples for single image recognition. The methods to solve problem are divided into two categories. One is to look for and select features that are robust to the number of samples, from the point of view of feature selection, such as PCA and 2DPCA. But when each person has only one face to be trained, the feature information extracted from the feature extraction algorithm will also be very limited, resulting in a bad recognition

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905219 |

performance. The other is to generate multiple virtual samples from the point of view of the extended sample, thus reducing the impact of the sample size.[3]

B. Face recognition method based on sparse representation and feature fusion

This The authors propose a multi-feature fusion face recognition method based on sparse representation. The core idea is to find the sparseness through training, and then use the sparse coefficient and training samples to represent the test samples, and then the optimal sparse solution is obtained by solving the l1-norm problem. The recognition results of feature fusion method are better than any single feature algorithm under the condition of non-occlusion or occlusion. When there are less than 10 pictures of each category of people in the training sample and the occlusion type is not controllable, our algorithm can still obtain a high recognition rate. [5]

C. Spatial pyramid pooling in deep convolutional networks for visual recognition

For Visual Recognition, Scales, Sizes and Aspect Ratio are considered as important factor. SPP (Spatial Pyramid Pooling) is a flexible solution for handling these factors. In context of deep networks, these factors have received less consideration ,thus the system is trained with deep layer networks considering SPP layer. SPP-net shows outstanding accuracy in classification/detection tasks and greatly accelerates DNN-based detection. Their studies also show that many time-proven techniques/insights in computer vision can still play important roles in deep-networks-based recognition.1]

D. Face and Gender Recognition System Based on Convolutional Neural networks

The proposed Face and Gender Recognition System realizes the combination of image face recognition and gender recognition module, which enables not only face recognition but also gender recognition in complex background. Based on the ResNet50 neural networks, we use the global average pool (GAP) instead of the fully connected layer before final output, followed by the softmax layer, which reduced the size of the networks. By constructing such a simple structure, the accuracy of the system recognition has been improved.[6]

E. Dynamic Feature Matching on Partial Face Recognition

In The partial face recognition is having application in a broad spectrum of different fields. The different approaches used for the partial face recognition are the key point-based approach, region-based approach, and CNN-based approach. In key point-based, the popular method was MKD-SRC. In region-based partial face recognition approach, the prominent model is MR-CNN. In the midst of different approaches in partial face recognition, it is concluded that the CNN-based approaches are the comparatively best approach. The current novel approach proposed for partial face recognition. in CNN– based is called Dynamic Feature Matching (DFM). The dynamic feature dictionary correlating to the probe is achieved. DFM is able to yield the advantages of the properties of FCN and generate identifying features more precisely. DFM is having a promising application in various video recognition approaches in the future. [2]

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905219 |

III. PROPOSED METHODOLOGY

A. *System Design:*

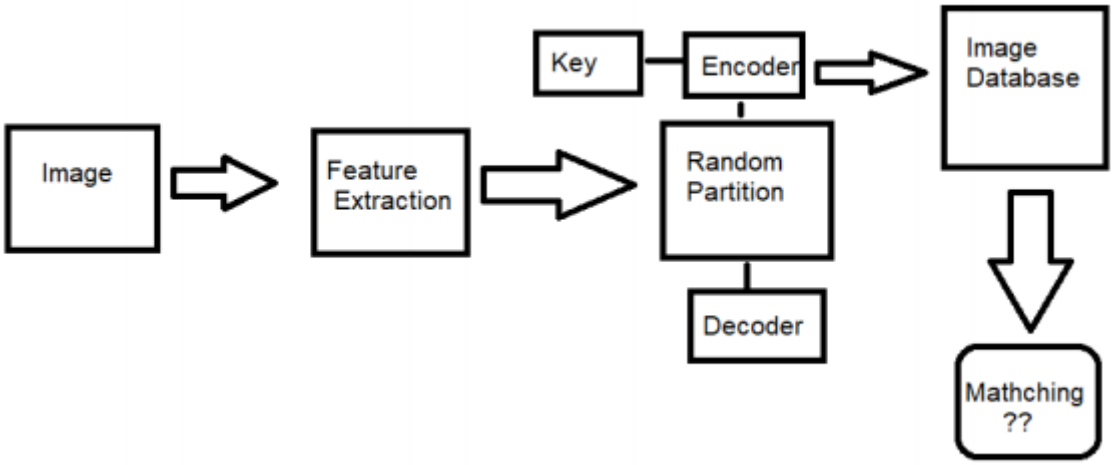


Fig.1. System Architecture

B. *Proposed Algorithm:*

Two Algorithms are used in system. One is used for Face recognition and the other for security.

1) CNN:

system has used feature extraction as a technique for facial recognition. In papers such as [3] and [5], multiple feature extraction is used with sparse representation. The papers [1] [6] make use of CNN as a latest framework for facial recognition. We put forth study CNN as a basic framework which will be used in proposed system.

The traditional neural network is not capable of dealing with images. Consider in case of the regular network, imagine each pixel is connected to one neuron and there will be thousands of neurons which will be computationally expensive. Convolutional Neural Network (CNN) handles images in different ways, but still, it follows the general concept of Neural Network. In constructing the CNN, it mainly consists of three parts – Convolution, Polling, Flattening. The fundamental purpose of convolution is to select characteristics from the input image. It conserves the spatial relationship between pixels by learning image characteristics using small squares of input data. The output obtained is a matrix known as the feature map. A further operation called ReLU is used after every convolution operation. The next step is of Pooling which is also known as sub-sampling or down-sampling. Pooling reduces the length of each feature map but maintains the most important information. In Max Pooling, it defines a spatial neighbourhood and takes the biggest element from the rectified feature map within that window. The other method is to take the average of all elements in that window. After pooling, next stage comes is flattening. In this step, the matrix is converted into a linear array so that to input it into the nodes of the neural network. The full connection is connecting a convolutional network to a neural network and then compiling network. The usage of CNN helps in minimizing the number of parameters needed for images. It also helps to do the parameter sharing as it can possess translation invariance.

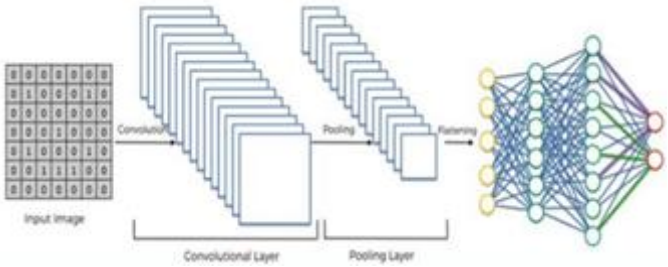


Fig.2. CNN (Source Meduim)

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905219 |

2) AES:

AES algorithm helps to encrypt the template. The algorithm uses 10 or 14rounds for encryption with given key depending on 128 bytes or 256bytes respectively . Each Round consist of 4 steps which includes SubByte where one each byte is substituted with another byte. The next is row shifting were whole row is shifted. next is mixcolumn where columns are mixed and the last one is adding round key. One round is shown in Fig

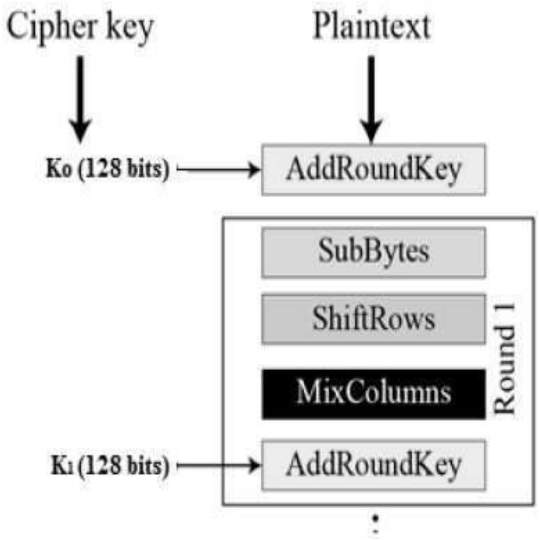


Fig.3. AES

IV. EXPERIMENTAL RESULTS

A) Registration to Database

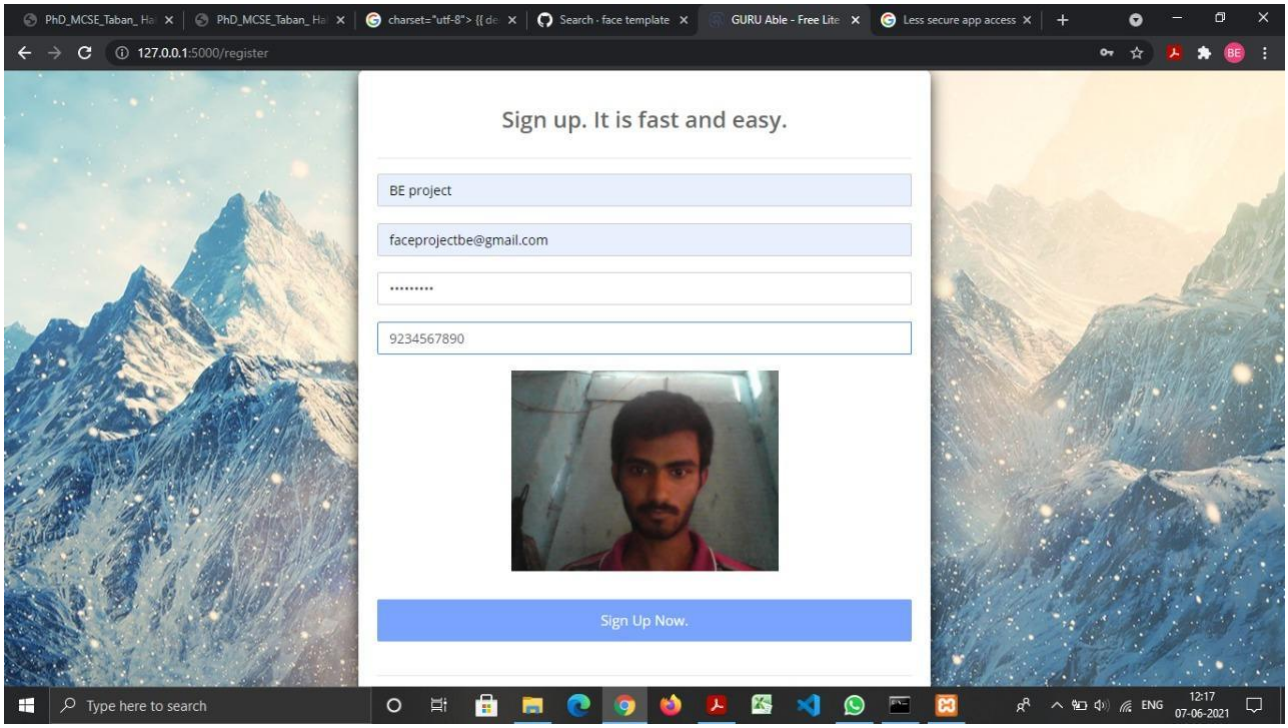


Fig.4. Registration with Face

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905219 |

B) Encrypted Database

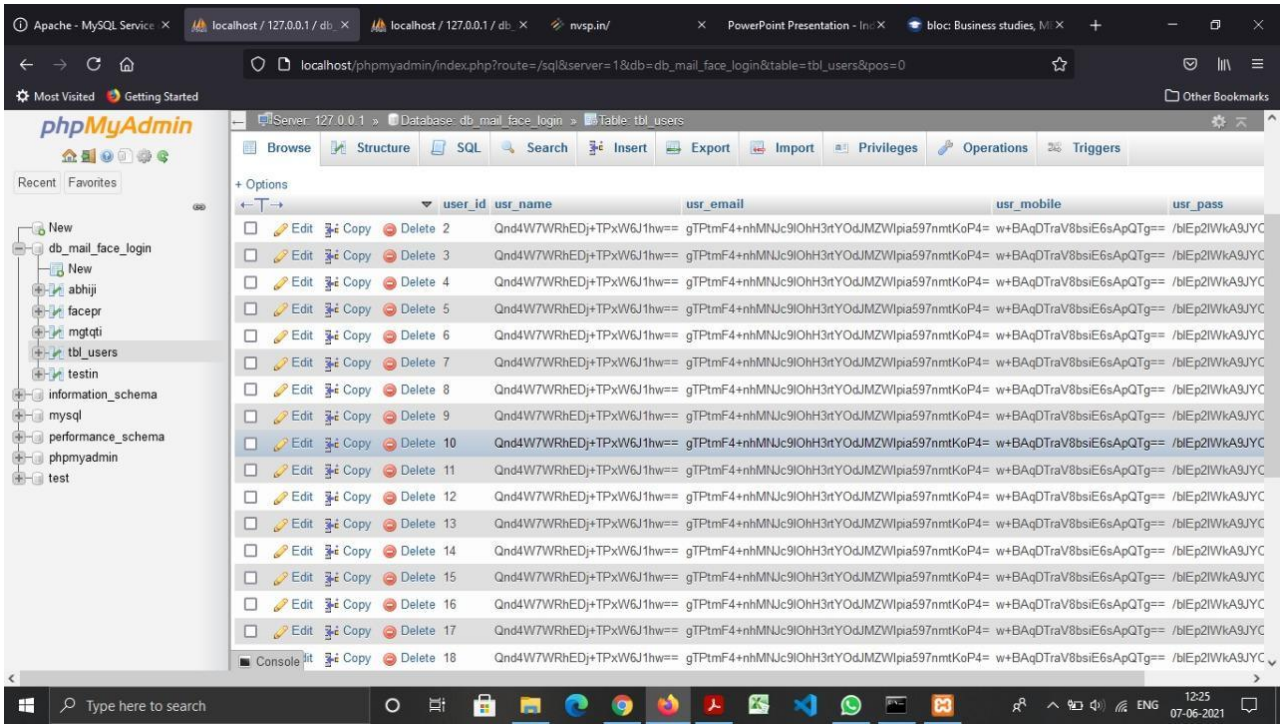


Fig.5. Encrypted Database

C) Login with Facial Features:

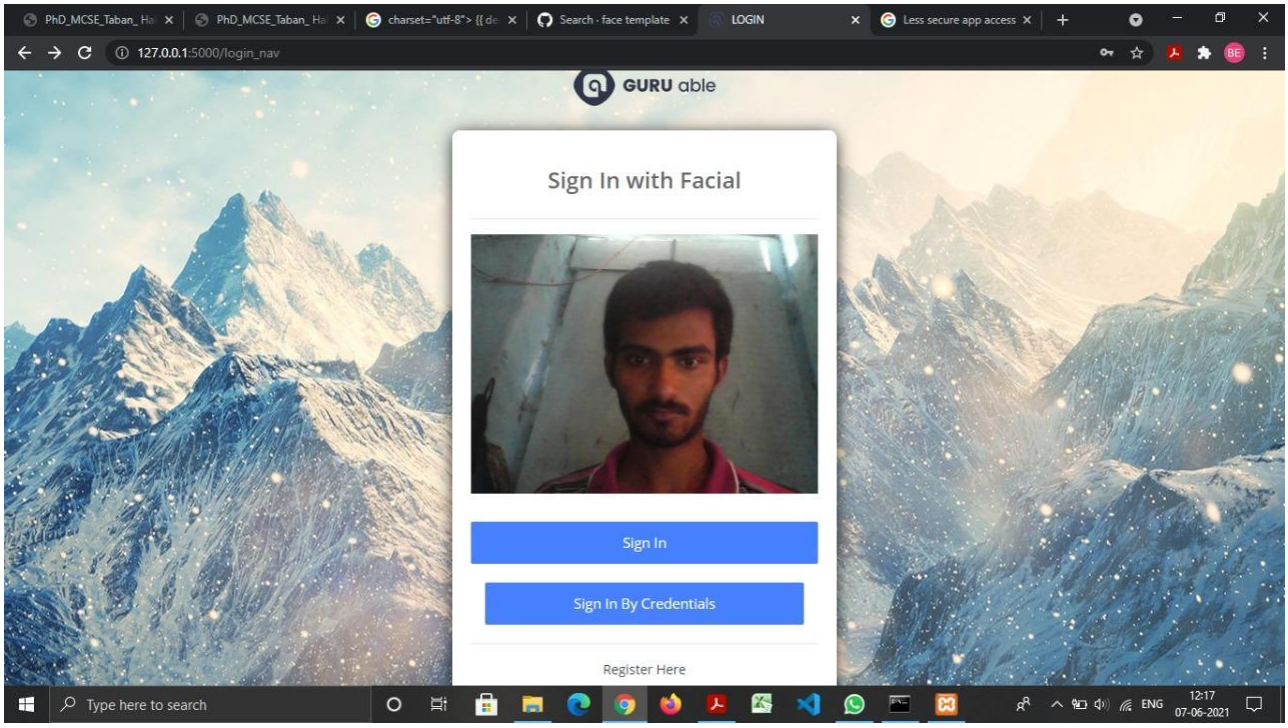


Fig.6. Login with Facial Features

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905219 |

D) Login with Credentials

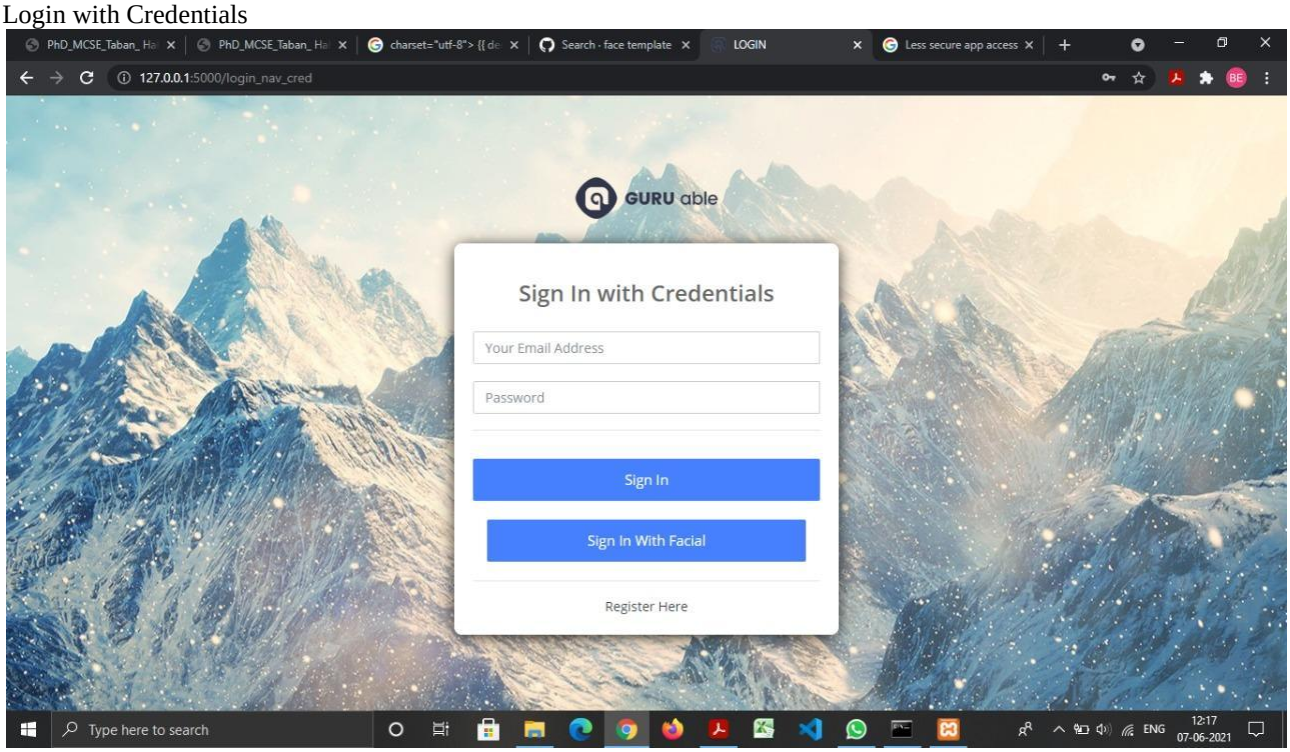


Fig.7. Login with Credentials

E) Successful Login :

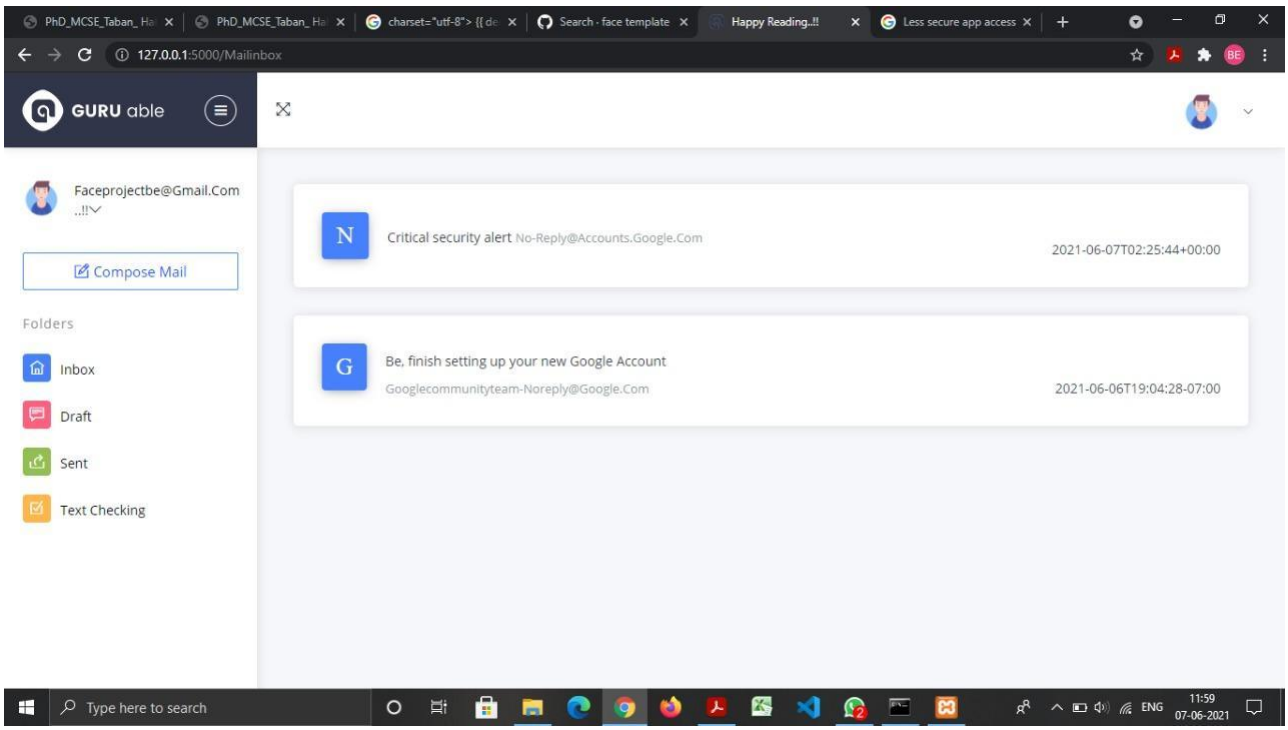


Fig 8. Login Sucessful

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905219 |

V. CONCLUSION AND FUTURE WORK

The system is used which to construct protected biometric systems whose stored deep templates are non-invertible, cancellable and dis-criminative. A randomized CNN is proposed to generates secure deep biometric templates based on the input face image . In construction, no user-specific key is stored in the system, where a secure sketch generated from both a user-specific key and an intermediate feature which is stored in the enrollment stage. In the query stage, the user-specific key can be decoded from a stored secure sketch if the query image is sufficiently close to the corresponding enrollment image.

REFERENCES

[1] Kaiming He, Xiangyu Zhang, Shaoqing Ren, and Jian Sun. Spatial pyramid pooling in deep convolutional networks for visual recognition. In European Conference on Computer Vision, pages 346–361. Springer,2014

[2] Wei Bu, Jiangjian Xiao, Chuanhong Zhou, Minmin Yang, Chengbin Peng A Cascade Framework for Masked Face Detection, IEEE 8th International Conference on CIS & RAM, Ningbo, China, 2017.

[3] X. Xu, L. Zhang and F. Li, "MSSVT: Multi-scale feature extraction for single face recognition," 2018 24th International Conference on Pattern Recognition (ICPR), Beijing, 2018, pp. 1996-2001, doi: 10.1109/ICPR.2018.8545343.

[4] Lun Zhang, Rufeng Chu, Shiming Xiang, Shengcai Liao, and Stan Z Li. Face detection based on multi-block lbp representation. In International Conference on Biometrics, pages 11–18. Springer, 2007.NaliniPriya G, Priyadarshani P, RajaRajeshwari K, IEEE 6thInternational Conference on smart structures and systems ICSSS 2019.

[5] C. Jiang, M. Wang, X. Tang and R. Mao, "Face recognition method based on sparse representation and feature fusion," 2019 Chinese Automation Congress (CAC), Hangzhou, China, 2019, pp. 396-400, doi: 10.1109/CAC48633.2019.8997456.

[6] Y. Zhou, H. Ni, F. Ren and X. Kang, "Face and Gender Recognition System Based on Convolutional Neural networks," 2019 IEEE International Conference on Mechatronics and Automation (ICMA), Tianjin, China, 2019, pp. 1091-1095, doi: 10.1109/ICMA.2019.8816192.

[7] M. R. Reshma and B. Kannan, "Approaches on Partial Face Recognition: A Literature Review," 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, India, 2019, pp. 538-544, doi: 10.1109/ICOEI.2019.8862783.

[8] W. Stallings, Cryptography and network security: principles and practice. Pearson, 2016, vol. 7

INNO SPACE

SJIF Scientific Journal Impact Factor

Impact Factor:
7.488

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details