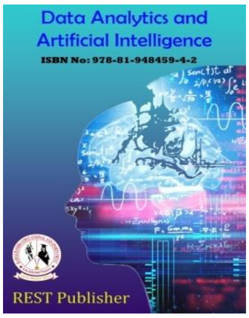
Data Analytics and Artificial Intelligence

Vol: 3(1), 2023

REST Publisher; ISBN: 978-81-948459-4-2

Website: http://restpublisher.com/book-series/daai/

DOI: https://doi.org/10.46632/daai/3/1/21



Local Binary Pattern Histogram Based Web Facial Authentication System

Nitish Kumar M, Yuvaraj R, Devakumar V, *Lavanya R

Veltech high-tech Dr.Rangarajan Dr, Sakunthala Engineering College, Chennai, Tamil Nadu, India.

*Corresponding Author Email: lavanya.r@velhightech.com

Abstract: *The objective of the project is to Detect and Recognize Human Facial Features via a Camera. The basic concept of this project is:- To convert the input image to HSV format to extract the binary image and additionally remove the noise from binary image using morphological operations and finally then contours are used to segment out the region of interest and further the region is analyzed to get the final result. While biometric data is generally considered one of the most reliable authentication methods, it also carries significant risk. That's because if someone's credit card details are hacked, that person has the option to freeze their credit and take steps to change the personal information that was breached. What do you do if you lose your digital 'face'? Around the world, biometric information is being captured, stored, and analyzed in increasing quantities, often by organizations and governments, with a mixed record on cybersecurity. A question increasingly being asked is, how safe is the infrastructure that holds and processes all this data? As facial recognition software is still in its relative infancy, the laws governing this area are evolving (and sometimes non-existent).*

Keywords: *HSV Format, Binary Image, Contour, Morphological operation, Cyber security Biometric data,*

1. INTRODUCTION

Facial recognition is a way of identifying or confirming an individual's identity using their face. Facial recognition systems can be used to identify people in photos, videos, or in real-time. Facial recognition is a category of biometric security. Other forms of biometric software include voice recognition, fingerprint recognition, and eye retina or iris recognition. The technology is mostly used for security and law enforcement, though there is increasing interest in other areas of use. The use of facial recognition technology has increased dramatically in the last few years with new products and applications being conceived and released every day. Once science fiction, this exciting and strong area of growth is quickly becoming a real-world reality. The COVID-19 pandemic has also accelerated the need for many industries to embrace the opportunities presented by facial recognition technology. Contactless experiences will become the norm as a way for businesses to offer customers and staff a safer experience when interacting with their business. From boarding a plane to buying a burger, we can expect facial recognition to become more integrated in our day to day lives. Of course, many of us are already used to daily interactions using facial recognition. Many of today's smart phones come equipped with facial recognition technology to unlock them seamlessly and without the need for contact. At NEC, we've been leading the field in facial recognition technology since the late 1980s and have contributed to its many advancements throughout the years. A lot has changed in that time, so we thought we'd list the 5 most common uses of facial recognition to demonstrate just how widespread and vital this form of technology has become.

2. LITERATURE SURVEY

Facial Action Recognition for Facial Expression Analysis From Static Face Images—Automatic recognition of facial gestures (i.e., facial muscle activity) is rapidly becoming an area of intense interest in the research field of machine vision. In this paper, we present an automated system that we developed to recognize facial gestures in static, frontal- and/or profile-view color face images. A multidetector approach to facial feature localization is utilized to spatially sample the profile contour and the contours of the facial components such as the eyes and the mouth. From the extracted contours of the facial features, we extract ten profile-contour fiducial points and 19 fiducial points of the contours of the facial components. Based on these, 32 individual facial muscle actions (AUs) occurring alone or in combination are recognized using rule-based reasoning. With each scored AU, the utilized algorithm associates a factor denoting the certainty with which the pertinent AU has been scored. A recognition rate of 86% is achieved. [2]Simultaneous Facial Feature Tracking and Facial Expression Recognition —The tracking and recognition of facial activities from images or videos have attracted great attention in computer vision field. Facial activities are characterized by three levels. First, in the bottom level, facial feature points around each facial component, i.e., eyebrow, mouth, etc., capture the detailed face shape information. Second, in the middle level, facial action units, defined in the facial action coding system, represent the contraction of a specific set of facial muscles, i.e., lid lightener, eyebrow raiser, etc. Finally, in the top level, six prototypical facial expressions represent the global facial muscle movement and are commonly used to describe the human emotion states. In contrast to the mainstream approaches, which usually only focus on one or two levels of facial activities, and track (or recognize) them separately, this paper introduces a unified probabilistic framework based on the dynamic Bayesian network to simultaneously and coherently represent the facial evolvement in different levels, their interactions and their observations. Advanced machine learning methods are introduced to learn the model based on both training data and subjective prior knowledge. Given the model and the measurements of facial motions, all three levels of facial activities are simultaneously recognized through a probabilistic inference. Extensive experiments are performed to illustrate the feasibility and effectiveness of the proposed model on all three level facial activities [3] Facial Expression Recognition with Convolutional Neural Network— Emotions are a powerful tool in communication and one way that humans show their emotions is through their facial expressions. One of the challenging and powerful tasks in social communications is facial expression recognition, as in non-verbal communication, facial expressions are key. In the field of Artificial Intelligence, Facial Expression Recognition (FER) is an active research area, with several recent studies using Convolutional Neural Networks (CNNs). In this paper, we demonstrate the classification of FER based on static images, using CNNs, without requiring any pre-processing or feature extraction tasks. The paper also illustrates techniques to improve future accuracy in this area by using preprocessing, which includes face detection and illumination correction. Feature extraction is used to extract the most prominent parts of the face, including the jaw, mouth, eyes, nose, and eyebrows. Furthermore, we also discuss the literature review and present our CNN architecture, and the challenges of using max-pooling and dropout, which eventually aided in better performance. We obtained a test accuracy of 61.7% on FER2013 in a seven-classes classification task compared to 75.2% in state-of-the-art classification. Facial expressions are essential to human social communication, as this communication is both verbal and non-verbal.

3. TECHNOLOGY USED

The various use of facial recognition is given below: -

3.1 Unlocking Phones: Various phones, including the most recent iPhones, use face recognition to unlock the device. The technology offers a powerful way to protect personal data and ensures that sensitive data remains inaccessible if the phone is stolen. Apple claims that the chance of a random face unlocking your phone is about one in 1 million.

3.2 Law Enforcement: Facial recognition is regularly being used by law enforcement. According to this NBC report, the technology is increasing amongst law enforcement agencies within the US, and the same is true in other countries. Police collects mugshots from arrestees and compare them against local, state, and federal face recognition databases. Once an arrestee’s photo has been taken, their picture will be added to databases to be scanned whenever police carry out another criminal search. Also, mobile face recognition allows officers to use smartphones, tablets, or other portable devices to take a photo of a driver or a pedestrian in the field and immediately compare that photo against to one or more face recognition databases to attempt an identification.

3.2 Airports and Border Control: Facial recognition has become a familiar sight at many airports around the world. Increasing numbers of travellers hold biometric passports, which allow them to skip the ordinarily long lines and instead walk through an automated ePassport control to reach the gate faster. Facial recognition not only reduces waiting times but also allows airports to improve security. The US Department of Homeland Security predicts that facial recognition will be used on 97% of travellers by 2023. As well as at airports and border crossings, the technology is used to enhance security at large-scale events such as the Olympics.

3.3 Finding Missing Persons:Facial recognition can be used to find missing persons and victims of human trafficking. Suppose missing individuals are added to a database. In that case, law enforcement can be alerted as soon as they are recognized by face recognition — whether it is in an airport, retail store, or other public space.

3.4 Reducing Retail Crime: Facial recognition is used to identify when known shoplifters, organized retail criminals, or people with a history of fraud enter stores. Photographs of individuals can be matched against large databases of criminals so that loss prevention and retail security professionals can be notified when shoppers who potentially represent a threat enter the store.

3.5 Improving Retail Experiences: The technology offers the potential to improve retail experiences for customers. For example, kiosks in stores could recognize customers, make product suggestions based on their purchase history, and point them in the right direction. “Face pay” technology could allow shoppers to skip long checkout lines with slower payment methods.

3.6 Banking: Biometric online banking is another benefit of face recognition. Instead of using one-time passwords, customers can authorize transactions by looking at their smartphone or computer. With facial recognition, there are no passwords for 11 hackers to compromise. If hackers steal your photo database, 'liveless' detection – a technique used to determine whether the source of a biometric sample is a live human being or a fake representation – should (in theory) prevent them from using it for impersonation purposes. Face recognition could make debit cards and signatures a thing of the past.

4. ARCHITECTURE DIAGRAM

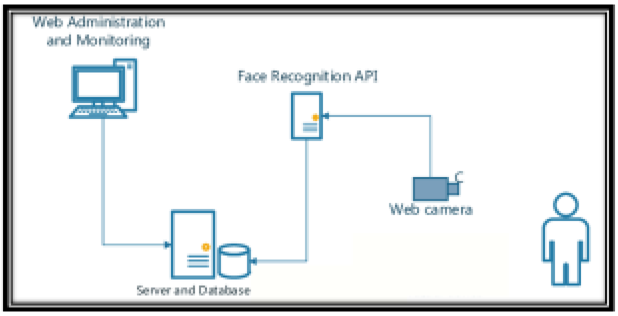


FIGURE1.A Architecture diagram

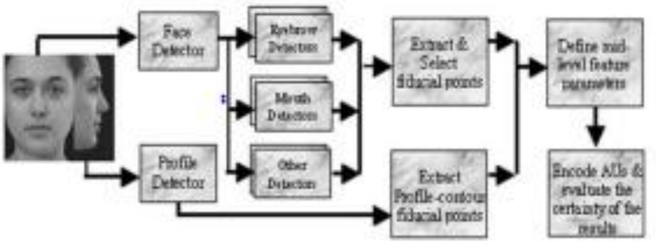

Face Detector
Eyebrow Detection
Mouth Detection
Other Detection
Profile Detector
Extract & Select fiducial points
Extract Profile-contour fiducial points
Define mid-level feature parameters
Encode AUs & evaluate the certainty of the results

FIGURE 2.B Project Flowchart

5. WORKING

Many people are familiar with face recognition technology through the FaceID used to unlock iPhones (however, this is only one application of face recognition). Typically, facial recognition does not rely on a massive database of photos to determine an individual’s identity — it simply identifies and recognizes one person as the sole owner of the device, while limiting access to others. Beyond unlocking phones, facial recognition works by matching the faces of people walking past special cameras, to images of people on a watch list. The watch lists can contain pictures of anyone, including people who are not suspected of any wrongdoing, and the images can come from anywhere — even from our social media accounts. Facial technology systems can vary, but in general, they tend to operate as follows:

Step 1: Face detection The camera detects and locates the image of a face, either alone or in a crowd. The image may show the person looking straight ahead or in profile.

Step 2: Face analysis Next, an image of the face is captured and analyzed. Most facial recognition technology relies on 2D rather than 3D images because it can more conveniently match a 2D image with public photos or those in a database. The software reads the geometry of your face. Key factors include the distance between your eyes, 22 the depth of your eye sockets, the distance from forehead to chin, the shape of your cheekbones, and the contour of the lips, ears, and chin. The aim is to identify the facial landmarks that are key to distinguishing your face.

Step 3: Converting the image to data The face capture process transforms analog information (a face) into a set of digital information (data) based on the person's facial features. Your face's analysis is essentially turned into a mathematical formula. The numerical code is called a faceprint. In the same way that thumbprints are unique, each person has their own faceprint.

Step 4: Finding a match Your faceprint is then compared against a database of other known faces. For example, the FBI has access to up to 650 million photos, drawn from various state databases.

6. RESULT

The program is able to detect and recognize Student facial features and display them. The model is quite certain, namely with 99.19% certainty that the image shows a "Human Face". As a human we can definitely say this is wrong. From this we learn that a probability below 100% always needs to be questioned - even if it is very close to 100%.

6.1 login page: The camera detects and locates the image of a face, either alone or in a crowd. The image may show the person looking straight ahead or in profile.

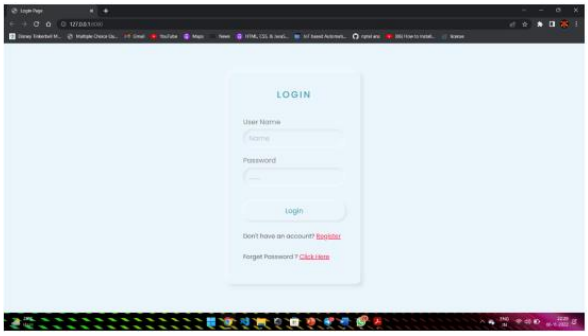


FIGURE 3. A Login Page

The login page requires the user to register and then login using the given id through which he has registered. The user data is stored in the local database and is again retrieved during the login time. The user does not need to register each time of login event. Acts as an outer security for data situated inside the program such that- each user gets allocated a separate database.

6.2 Image Training, Detection and Recognition Page

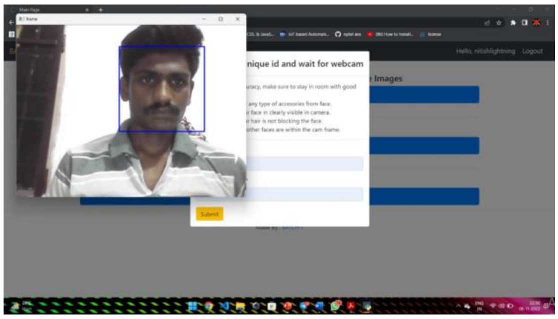
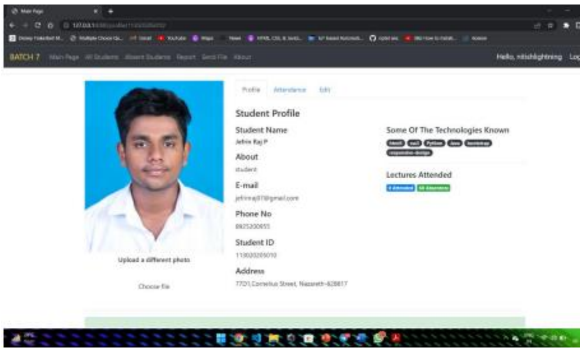

Main Page
frame
Hello, nitishfightning
Logout
nique id and wait for webcam
Images
uracy, make sure to stay in room with good
any type of accesories from face.
r face in clearly visible in camera.
r hair is not blocking the face.
other faces are within the cam frame.
Submit

FIGURE 4. B Main Page

An Interactive page to create datasets, train the model and recognize the face in front of the cam has been implemented here.

6.3 Attendance Page



Student Profile

Student Name
Jefrin Raj P

About
student

E-mail
jefrinraj07@gmail.com

Phone No
8825200655

Student ID
113020205010

Address
7701,Cornelius Street, Nazareth-628617

Some Of The Technologies Known

Lectures Attended

FIGURE 5.C Student Attendance page

The noted attendance of the respective student in front of the image is displayed in this section.

7. CONCLUSION

As the technology is booming with emerging trends therefore The Web Facial Login System which can possibly contribute to public welfare. The model is trained on an authentic dataset. We used OpenCV, Numpy and imutils to detect the shown Faces ad Recognize them. The models were tested with images and real-time video. The accuracy of the model is achieved and, the optimization of the model is a continuous process and we are building an accurate solution by tuning the hyper parameters. This specific model could be used as a use case for edge analytics. By the developing this system, we can recognise the given Face and would be of great help to the society.

REFERENCES

[1].S. P. Mohanty, U. Choppali, and E. Kougianos, ‘‘Everything you wanted to know about smart cities: The Internet of Things is the backbone,’’ IEEE Consum. Electron. Mag., vol. 5, no. 3, pp. 60–70, Jul. 2016, doi: 10.1109/MCE.2016.2556879.

[2].(Nov. 21, 2014). Report: Cisco and IBM Leaders in the Smart Cities Technology Market. Accessed: Feb. 24, 2022. [Online]. Available: https://www.smartcitiescouncil.com/article/report-cisco-and-ibm-leaderssmart-cities-technology-market

[3].A. Mitra, S. P. Mohanty, P. Corcoran, and E. Kougianos, ‘‘iFace: A deepfake resilient digital identification framework for smart cities,’’ in Proc. IEEE Int. Symp. Smart Electron. Syst. (iSES), Dec. 2021, pp. 361–366, doi: 10.1109/iSES52644.2021.00090.

[4].N. K. Ratha, J. H. Connell, and R. M. Bolle, ‘‘Enhancing security and privacy in biometrics-based authentication systems,’’ IBM Syst. J., vol. 40, no. 3, pp. 614–634, Apr. 2001, doi: 10.1147/sj.403.0614.

[5]. J. Hernandez-Ortega, J. Fierrez, A. Morales, and J. Galbally, ‘‘Introduction to presentation attack detection in face biometrics and recent advances,’’ 2021, arXiv:2111.11794.

[6].P. Korshunov and S. Marcel, ‘‘DeepFakes: A new threat to face recognition? Assessment and detection,’’ 2018, arXiv:1812.08685.

[7].Y. Nirkin, Y. Keller, and T. Hassner, ‘‘FSGAN: Subject agnostic face swapping and reenactment,’’ 2019, arXiv:1908.05932.

[8]. S. P. Mohanty, ‘‘Security and privacy by design is key in the internet of everything (IoE) era,’’ IEEE Consum. Electron. Mag., vol. 9, no. 2, pp. 4–5, Mar. 2020, doi: 10.1109/MCE.2019.2954959.

[9].M. Wang and W. Deng, ‘‘Deep face recognition: A survey,’’ Neurocomputing, vol. 429, pp. 215–244, Mar. 2021, doi: 10.1016/j.neucom. 2020.10.081.

[10]. P. N. Belhumeur, J. P. Hespanha, and D. Kriegman, ‘‘Eigenfaces vs. fisherfaces: Recognition using class specific linear projection,’’ IEEE Trans. Pattern Anal. Mach. Intell., vol. 19, no. 7, pp. 711–720, Jul. 1997, doi: 10.1109/34.598228.

[11]. X. He, S. Yan, Y. Hu, P. Niyogi, and H.-J. Zhang, ‘‘Face recognition using Laplacianfaces,’’ IEEE Trans. Pattern Anal. Mach. Intell., vol. 27, no. 3, pp. 328–340, Mar. 2005, doi: 10.1109/TPAMI.2005.55.

[12]. J. Wright, A. Y. Yang, A. Ganesh, S. S. Sastry, and Y. Ma, ‘‘Robust face recognition via sparse representation,’’ IEEE Trans. Pattern Anal. Mach. Intell., vol. 31, no. 2, pp. 210–227, Feb. 2009, doi: 10.1109/TPAMI.2008.79.

[13]. C. Liu and H. Wechsler, ‘‘Gabor feature based classification using the enhanced Fisher linear discriminant model for face recognition,’’ IEEE Trans. Image Process., vol. 11, no. 4, pp. 467–476, Apr. 2002, doi: 10.1109/TIP.2002.999679.

[14]. T. Ahonen, A. Hadid, and M. Pietikäinen, ‘‘Face description with local binary patterns: Application to face recognition,’’ IEEE Trans. Pattern Anal. Mach. Intell., vol. 28, no. 12, pp. 2037–2041, Dec. 2006, doi: 10.1109/TPAMI.2006.244.

[15]. Y. Taigman, M. Yang, M. Ranzato, and L. Wolf, ‘‘DeepFace: Closing the gap to human-level performance in face verification,’’ in Proc. IEEE Conf. Comput. Vis. Pattern Recognit., Jun. 2014, pp. 1701–1708, doi: 10.1109/CVPR.2014.220.

[16]. G. B. Huang, M. Ramesh, T. Berg, and E. Learned-Miller, ‘‘Labeled faces in the wild: A database for studying face recognition in unconstrained environments,’’ Univ. Massachusetts, Amherst, MA, USA, Tech. Rep. 07-49, Oct. 2007.

[17]. Y. Sun, X. Wang, and X. Tang, ‘‘Deep learning face representation from predicting 10,000 classes,’’ in Proc. IEEE Conf. Comput. Vis. Pattern Recognit., Jun. 2014, pp. 1891–1898, doi: 10.1109/CVPR. 2014.244.

[18]. Y. Sun, X. Wang, and X. Tang, ‘‘Deep learning face representation by joint identification-verification,’’ 2014, arXiv:1406.4773.

[19]. Y. Sun, X. Wang, and X. Tang, ‘‘Deeply learned face representations are sparse, selective, and robust,’’ 2014, arXiv:1412.1265.

[20]. F. Schroff, D. Kalenichenko, and J. Philbin, ‘‘FaceNet: A unified embedding for face recognition and clustering,’’ in Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR), Jun. 2015, pp. 815–823, doi: 10.1109/CVPR.2015.7298682.

[21]. J. Deng, Y. Zhou, and S. Zafeiriou, ‘‘Marginal loss for deep face recognition,’’ in Proc. IEEE Conf. Comput. Vis. Pattern Recognit. Workshops (CVPRW), Jul. 2017, pp. 60–68, doi: 10.1109/CVPRW. 2017.251.

[22]. L. Tran, X. Yin, and X. Liu, ‘‘Disentangled representation learning GAN for pose-invariant face recognition,’’ in Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR), Jul. 2017, pp. 1415–1424, doi: 10.1109/CVPR.2017.141.

[23]. H. Wang, Y. Wang, Z. Zhou, X. Ji, D. Gong, J. Zhou, Z. Li, and W. Liu, ‘‘CosFace: Large margin cosine loss for deep face recognition,’’ in Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit., Jun. 2018, pp. 5265–5274, doi: 10.1109/CVPR.2018.00552.

[24]. J. Deng, J. Guo, N. Xue, and S. Zafeiriou, ‘‘ArcFace: Additive angular margin loss for deep face recognition,’’ in Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. (CVPR), Jun. 2019, pp. 4690–4699, doi: 10.1109/CVPR.2019.00482.

[25]. M. A. Ferrag, L. Maglaras, and A. Derhab, ‘‘Authentication and authorization for mobile IoT devices using biofeatures: Recent advances and future trends,’’ Secur. Commun. Netw., vol. 2019, p. 20, May 2019, doi: 10.1155/2019/5452870.

[26]. Q. Tao and R. Veldhuis, ‘‘Biometric authentication system on mobile personal devices,’’ IEEE Trans. Instrum. Meas., vol. 59, no. 4, pp. 763–773, Apr. 2010, doi: 10.1109/TIM.2009.2037873.

[27]. M. S. Hossain, G. Muhammad, S. M. M. Rahman, W. Abdul, A. Alelaiwi, and A. Alamri, ‘‘Toward end-to-end biomet rics-based security for IoT infrastructure,’’ IEEE Wireless Commun., vol. 23, no. 5, pp. 44–51, Oct. 2016, doi: 10.1109/MWC.2016.7721741.

[28]. Q. Tao and R. N. J. Veldhuis, ‘‘Biometric authentication for a mobile personal device,’’ in Proc. 3rd Annu. Int. Conf. Mobile Ubiquitous Syst. Workshops, Jul. 2006, pp. 1–3, doi: 10.1109/MOBIQW.2006.361741.

[29]. M. E. Fathy, V. M. Patel, and R. Chellappa, ‘‘Face-based active authentication on mobile devices,’’ in Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP), Apr. 2015, pp. 1687–1691, doi: 10.1109/ICASSP.2015.7178258.

[30]. A. Hadid, J. Y. Heikkila, O. Silven, and M. Pietikainen, ‘‘Face and eye detection for person authentication in mobile phones,’’ in Proc. 1st ACM/IEEE Int. Conf. Distrib. Smart Cameras, Sep. 2007, pp. 101–108, doi: 10.1109/ICDSC.2007.4357512.

[31]. S. Sarkar, V. M. Patel, and R. Chellappa, ‘‘Deep feature-based face detection on mobile devices,’’ in Proc. IEEE Int. Conf. Identity, Secur. Behav. Anal. (ISBA), Feb. 2016, pp. 1–8, doi: 10.1109/ISBA.2016.7477230.

[32]. Y. Sutcu, Q. Li, and N. Memon, ''Secure biometric templates from fingerprint-face features,'' in Proc. IEEE Conf. Comput. Vis. Pattern Recognit., Jun. 2007, pp. 1–6, doi: 10.1109/CVPR.2007.383385.

[33]. T. Phillips, X. Zou, F. Li, and N. Li, ''Enhancing Biometric-Capsule-based authentication and facial recognition via deep learning,'' in Proc. 24th ACM Symp. Access Control Models Technol. (SACMAT). New York, NY, USA: Association for Computing Machinery, May 2019, pp. 141–146, doi: 10.1145/3322431.3325417.

[34]. K. Zhang, Z. Zhang, Z. Li, and Y. Qiao, ''Joint face detection and alignment using multitask cascaded convolutional networks,'' IEEE Signal Process. Lett., vol. 23, no. 10, pp. 1499–1503, 2016.

[35]. M. Masud, G. Muhammad, H. Alhumyani, S. S. Alshamrani, O. Cheikhrouhou, S. Ibrahim, and M. S. Hossain, ''Deep learning-based intelligent face recognition in IoT-cloud environment,'' Comput. Commun., vol. 152, pp. 215–222, Feb. 2020, doi: 10.1016/j.comcom.2020.01.050.

[36]. H. Chen, W. Wang, J. Zhang, and Q. Zhang, ''EchoFace: Acoustic sensor-based media attack detection for face authentication,'' IEEE Internet Things J., vol. 7, no. 3, pp. 2152–2159, Mar. 2020, doi: 10.1109/JIOT.2019.2959203.

[37]. Y. Chen, J. Sun, X. Jin, T. Li, R. Zhang, and Y. Zhang, ''Your face your heart: Secure mobile face authentication with photoplethysmograms,'' in Proc. IEEE Conf. Comput. Commun. (IEEE INFOCOM), May 2017, pp. 1–9, doi: 10.1109/INFOCOM.2017.8057220.

[38]. A. Mitra, S. P. Mohanty, P. Corcoran, and E. Kougianos, ''A novel machine learning based method for deepfake video detection in social media,'' in Proc. IEEE Int. Symp. Smart Electron. Syst. (iSES), Dec. 2020, pp. 91–96, doi: 10.1109/iSES50453.2020.00031.

[39]. A. Mitra, S. P. Mohanty, P. Corcoran, and E. Kougianos, ''A machine learning based approach for deepfake detection in social media through key video frame extraction,'' Social Netw. Comput. Sci., vol. 2, no. 2, p. 98, Apr. 2021, doi: 10.1007/s42979-021-00495-x.