IJIRCCE

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

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 11, Issue 2, February 2023

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.165

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 11, Issue 2, February 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1102004 |

Implementation of DND CyberScam's using OpenCV &Django

Yeswanth Reddy Chilakala, Bhavani Sankar. A.B, Chandra Sekhar Reddy. K,

Prof. Bhagyesha Pandhi

Department of Computer Science, Parul University, India

Department of Computer Science, Parul University, India

Department of Computer Science, Parul University, India

Asst. Professor, Department of Computer Science and Engineering, Parul University, India

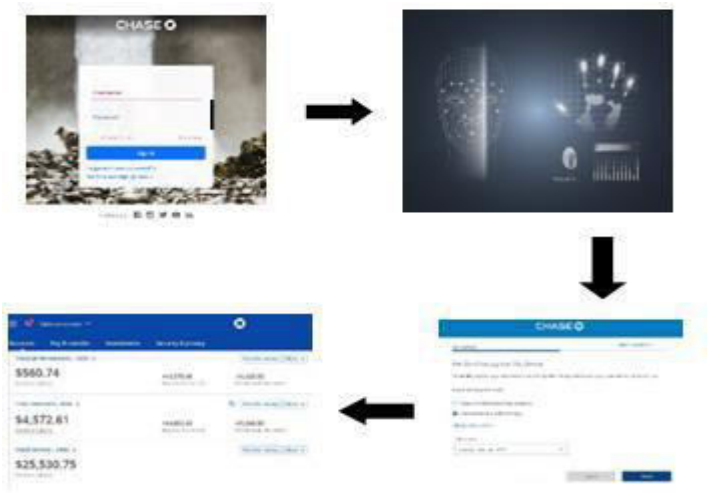
ABSTRACT: -We have brought up this project because of the current situation all people are not aware of banking scams, and it is difficult to identify the links for bank logins for that we have one solution which is adding facial prints to bank pages. So, it solves the raised problems in the banking system during the pandemic situation of covid -19 and for that face, recognition is a powerful tool for a biometric system that takes data from both images and videos.

The additional security of bank credit data. Our subject is to create additional security for a bank's credit report. So, hackers can get any email or phone number. We link biometric and face prints to the bank check page.

KEYWORDS: OpenCV, Django, DeepID... etc.

I.INTRODUCTION

Currently, when you log into online banking, you are asked for OTP from your phone number or email address, So, hackerscan get any OTP from your email or number or via OTP bots. Our main theme is to create additional security for banking credentials and prevent users from identity theft. So instead of asking for OTP, it will ask for face prints to recognize the person and prevent cyber attackers.Unlike other identification solutions such as passwords, email verification, selfies or photos, or fingerprint recognition, biometric facial recognition uses unique mathematics that makes this system one of the most secure and effective. Use target and dynamic patterns. There are many benefits that facial recognition can bring to society. From preventing crime and increasing security to reducing unnecessary contact and work. In some cases, it can even support medical efforts.



| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 11, Issue 2, February 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1102004 |

II. OPENCV(COMPUTERVISION)

OpenCV isa Python open-sourcelibrary used for computer vision in areas such as artificial intelligence, machine learning, and facial recognition. OpenCV stands for Computer Vision and is defined as a research field. It helps computers understand the content of digital images such as photos and videos. Objects, text descriptions, and his three- dimensional model, etc. Extract descriptions from possible images.

Object Classification –When classifying objects, we train the model on a dataset of specific objects and the model classifies the new objects as belonging to one or more of your training categories.

Object Identification –Our model will identify a specific instance of an object in the object identification phase.

Fig.1: Identification Method in OpenCV

The pixel values are used to convert the image to numbers. A pixel is the smallest unit of a digital image or graphic that canbe displayed and represented on a digital display device. In the image above, the grayscale image pixel value is shown as a single number representing the intensity ofblackat that location.

DJANGO

Django is a high-end Python web framework that enables the rapid development of secure and maintainable websites. Built by experienced developers, Django handles most of your web development, so you can focus on building your app instead of starting over.

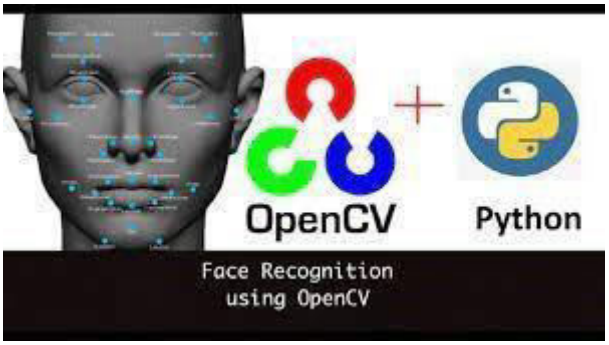


Fig.2: Face Recognition using OpenCV in Django

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 11, Issue 2, February 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1102004 |

III. ARTIFICIAL INTELLIGENCE

Facial Recognition is a category of biometric software that maps the facial features of people and stores the data as facial prints. The software uses deep learning algorithms to compare live images taken with stored facial prints to confirm identity. Image processing and machine learning are the backbones of this technology. Facial recognition has received considerable attention from researchers because of its human activity in various security applications such as airports, crime detection, face tracking, and forensics. Face biometrics may not stand out compared to other biometrics such as palm print, iris, and fingerprint. These can also be used without the user's knowledge and can also be used for security- based applications such as crime detection, face tracking, airport security, and forensic surveillance systems. Face Recognition The captures facial images from video or surveillance cameras. They are compared with a stored database. Face recognition involves training known images, classification using known classes, and saving to a database. When a test image is given to the system, it is classified and compared to a stored database.

Fig.3: HAAR Cascade classifier Algorithm

Impact of online frauds on people: -

Last year, identity fraud cost Americans a total of about $56 billion and killed about 9 million consumers. According to Javelin Strategy and Research's 2021 Identity Fraud Study, this is. About $13 billion in losses came from what Javelin calls "traditional identity fraud," in which cybercriminals steal personal information. and use it for their purposes, such as through data breaches.

But most of last year's $3 billion losses were due to identity theft fraud. In this scam, criminals interact directly with consumers to steal information through methods such as automated phone calls and phishing emails. Victims of these scams lost an average of $1,100, according to Javelin. John Buzzard, Senior Fraud and Security Analyst at Javelin Strategy and Research said: As the Covid-19 pandemic has changed the way people shop and send money, many criminals are targeting digital wallets and peer-to-peer payment methods such as Apple Pay and mobile phones. Javelin found that about 18 million victims fell victim to his scam using these digital payment methods last year.

IV. METHODOLOGY

As you know, Python is a general-purpose programming language with endless advantages and easy-to-use syntax code. You can also write your homework in various exercise books and file it as resource work. Our project, which is based on image processing for banking systems, is largely integrated with open computer vision, giving this concept a lot of power.

When a person approaches the webcam, it captures the person's face and says on the open resume that it is a human face. Next, we recognize faces through AI, and we know that people wearing masks or not wearing masks recognize faces by calculating the length and structure of a person's face. Calculates the length of the person's face when wearing the data after checking where the detected face matches the databasein the system based on the facial

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 11, Issue 2, February 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1102004 |

structure and eye length Ifthe person's presence is marked as present.

Here some of the python packages/modules used in the project are: -

1. NumPy–Scientific computing, the path of a multidimensional array object, linear algebra, and Fourier transformare all included in this library.
2. Tkinter–pythons'built-in library for creating interactive simple GUI programs, text, editors, games, and otherthings.
3. OpenCV–High-level understanding, task automation, and recognition are all included in this library.
4. PIL –Image manipulation and python reflection codes are handled by this package.

In our project, weuse OpenCV which is a high level of understanding of task automation and situation recognition that are used to write other types of programs that use tools like a flask.

V. CONCLUSION

To identify and recognize human faces via computer vision technology, this paper examines the algorithm and draws the following conclusions. The introduction of previous experiments and her analysis of skin color features allow better elimination of non-facial complex backgrounds. AdaBoost detection performs times better than using grayscale images directly, reducing the chance of false positives.

Also, a new sparsity feature is used to replace the hair feature in the traditional AdaBoost algorithm, making the system more consistent with the previous AdaBoost algorithm. A face with multiple poses such as B. The distraction slope effectively reduces face detection and improves recognition rate, while the skin color feature and sparse feature simultaneously improve system performance. The self-made face training sample has a higher recognition rate in the test because it added faces collected by the lab itself. The experiment compares the experimental results of the Ad boost method, the flesh tone method, and the flesh tone Ad boost method. The detection and false positive rates are superior to the AdaBoost method.

At the same time, we also found that the addition of the skin-tone feature allows the faces detected by AdaBoost to be filtered out by lighting, etc., and the AdaBoost method uses the new sparse features for recognition. More gesture mode faces. Complex backgrounds are more likely to be false positives, but because we are using skin color features, these false positives are limited to skin color background regions (such as hands). All operations in the KPCA and KFDA algorithms are performed by the inner product kernel function defined in the original space and do not involve any specific nonlinear mapping function. This is the Core Competency in Nuclear Learning Methods. His null-space-based KFDA overcomes lighting effects and is robust to facial expressions and attitudes changes. Null space methods can overcome the small sample problem in discriminant analysis by finding the best discriminant information that exists in the null space of the between-class variance matrix. Combining the null space method with the kernel discriminant analysis method not only improves the ability of discriminant analysis to extract nonlinear features but also overcomes the small sample problem in discriminant analysis. Secondary extraction of PCA features provides better recognition results than the PCA method. These two classical algorithms can be written in the same framework. That is, the corresponding linear feature space is first constructed, then the image is projected into the linear space, and the resulting projection coefficients are used as the identified feature vector. The only difference between the two methods is the different choice of feature space. Following the small sampling problem of two linear subspace methods, PCA and LDA, this paper also proposes a null-space-based Fisher discriminant analysis method. The experiment shows that the null space-based method makes the best use of the null space of the within-class covariance matrix. Useful identifying information improves the accuracy rate of face recognition to some extent.

REFERENCES

1. David Ellis (GCIH, QSA, PFI, CISSP) is VP of Forensic Investigations at Security Metrics with over 25 years.
2. SCADA Environment from Research gate: Authors (Vivek Kumar Singh from National RenewableEnergy Laboratory, Haytham Ebrahem from Iowa State University)
3. Trust in Cyberspace: Authors Present & Discuss Study's Findings - Public Notice, Aug 1, 2010 – event.
4. A Cybersecurity Agenda for the 45th President. (2017, January 5). Retrieved

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 11, Issue 2, February 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1102004 |

from https://www.csis.org/news/cybersecurity-agenda-45th-president.

5. AUSTRALIA'S CYBER SECURITY STRATEGY Enabling innovation, growth & prosperity [PDF]. (n.d.).
6. Retrieved from https://cybersecuritystrategy.pmc.gov.au/assets/img/PMC-Cyber-Strategy.pdf"LBPH-Based Enhanced Real-Time Face Recognition," International Journal of Advanced Computer Science and Applications, Vol. 10, No. 5, 2019.
7. Y. Zhang and J. L. Chen," Wide-area SCADA system with a distributed security framework," in Journal ofCommunications and Networks, vol.14, no. 6, pp. 597-605, Dec. 2012.
8. NERC Critical Infrastructure Protection Committee (CIPC) Cyber At-tack Task Force (CATF) Update,North American Electric Reliability Corporation (NERC), Dec. 2011
9. B. Miller and D. Rowe, A survey of SCADA and critical infrastructure incidents, Proceedings of the FirstAnnual Conference on Research in Information Technology, pp. 51–56, 2012.

INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 8.165

doi cross ref

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