IJIRCCE

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

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 11, Issue 5, May 2023

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 5, May 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1105075 |

Securing Confidential Data using Effigy Face Detection and Conceal

I S.Deepakchandhiran[1], S.Karthick[2] , M.Krishnaraj [3], A.Sendhooren[4]

U.G Students, Department of Computer Science and Engineering, Trichy Engineering College, Konalai, Trichy, Tamilnadu, India[1,2,3]

Assistant Professor, Department of Computer Science and Engineering, Trichy Engineering College, Konalai, Trichy, Tamilnadu, India[4]

ABSTRACT: Face detection is a technique that identifies or locates human faces in digital images. A typical example of face detection occurs when we take photographs through our smartphones, and it instantly detects faces in the picture. Face detection is different from Face recognition. Face detection detects merely the presence of faces in an image while facial recognition involves identifying whose face it is. Often the problem of face recognition is confused with the problem of face detection is to decide if the "face" is someone known, or unknown, using for this purpose a database of faces in order to validate this input face. Face detection is a computer vision technology that helps to locate/visualize human faces in digital images. Effigy Conceal is the process of hiding information which can be text, image or video inside a cover image. The secret information is hidden in a way that it not visible to the human eyes. Deep learning technology, which has emerged as a powerful tool in various applications including Effigy Conceal, has received increased attention recently. The main goal of this paper is to explore and discuss various deep learning methods available in image Conceal field. Deep learning techniques used for Effigy Conceal can be broadly divided into three categories - traditional methods, Convolutional Neural Network-based and General Adversarial Network-based methods.

KEYWORDS: Python, OpenCV, Deep Learning, Face detection, Effigy Conceal etc…

I. INTRODUCTION

Face Detection is a computer vision technique in which a computer program can detect the presence of human faces and also find their location in an image or a video stream. Isn't it mind-boggling how the mobile camera automatically detects your face every time you try to take a selfie? You must've also noted that it captures other people's faces in the frame. Well, all this wouldn't have been possible without Face Detection algorithms. Every year, Facial Detection algorithms are evolving faster and becoming more robust. Architecture of ISGAN Steganography is a process of hiding secret data within an image **.** In this technique the image that is used to hide the data is called the cover and the image containing the embedded hidden message is called the conceal image.

1.1 Motivation

An automatic face analysis system is proposed which uses face recognition and facial physiognomy. It first detects human's face, extracts its features, and classifies the shape of facial features. It will analyze the person's facial physiognomy and then automatically make an avatar drawing using the facial features. Face recognition technology is a biometric technology, which is based on the identification of facial features of a person. People collect the face images, and the recognition equipment automatically processes the images. The paper introduces the related researches of face recognition from different perspectives.

1.2 Problem Statement

Face recognition has many challenges due to illumination variations, large dimensionality, uncontrolled environments, pose variations and ag- ing. In the recent years, Face recognition get remarkable improvement and accuracy to overcome these challenges, but illumination change is still challenging. Effigy conceal using to hide the data from image and to download. That image can encryption and decryption to securely transger the data.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 5, May 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1105075 |

II. LITERATURE SURVEY

a. OpenCV: OpenCV is a powerful open-source computer vision library that can be used to detect faces in images and videos. It provides a pre-trained Cascade Classifier for face detection, which can be used out-of-the-box.
b. Dlib: Dlib is a machine learning library that can be used for face detection, among other tasks. It provides a pre-trained shape predictor for face detection, which can be used to detect faces in images and videos.
c. Face_recognition: face_recognition is a python library that provides an easyto-use interface for face detection and Recognition. Modern facial recognition created with deep learning is used in the library by dlib.
d.MTCNN: Multi-task Cascaded Convolutional Networks (MTCNN) is a popular face detection algorithm that can be used to detect faces in images and videos.
e. TensorFlow: TensorFlow is a popular machine learning framework that can be used to build custom face detection models. It gives users access to a potent API for developing and implementing system mastery models.

III. EXISTING SYSTEM

Face detection uses machine learning (ML) and artificial neural network (ANN) technology, and plays an important role in face tracking, face analysis and facial recognition. In face analysis, face detection uses facial expressions to identify which parts of an image or video should be focused on to determine age, gender and emotions. In a facial recognition system, face detection data is required to generate a faceprint and match it with other stored faceprints. Face detection applications use AI algorithms, ML, statistical analysis and image processing to find human faces within larger images and distinguish them from nonface objects such as landscapes, buildings and other human body parts. Before face detection begins, the analyzed media is preprocessed to improve its quality and remove images that might interfere with detection. Least significant bit (LSB) is the simplest form of steganography. LSB is based on inserting data in the least significant bit of pixels, which lead to a slight change on the cover image that is not noticeable to human eye. Since this method can be easily cracked, it is more vulnerable to attacks.

3.1 Disadvantage

- Face detection improves surveillance efforts and helps track down criminals and terrorists. Personal security is enhanced when users use their faces in place of passwords, because there's nothing for hackers to steal or change.
- The disadvantage of Conceal is that it can be generally used to secretly send messages without the case of the transmission being found. By using encryption, it can recognize the sender and the receiver.
- The primary advantage of using Conceal to hide data over encryption is that it helps obscure the fact that there is sensitive data hidden in the file or other content carrying the hidden text.
- Conceal is a method that makes it easy to conceal a message within another to keep it secret. The result is that the hidden message remains hidden. A conceal approach can benefit images, videos, and audio files.

IV. PROPOSED SYSTEM

To increase the security and the size of stored data, a new adaptive lsb technique is used. Instead of storing the data in every least significant bit of the pixels, this technique tries to use more than one bit in a pixel in such a way that this change will not affect the visual appearance of the host image. It uses the side information of neighboring pixels to estimate the number of bit which can be carried in the pixels of the host-image to hide the secret data. A Steganography System consists of two functions: embedding and extraction. The objective of the proposed work is to design robust algorithms which generate stego media, can carry large amount (capacity) of secret data without reducing imperceptibility. The steganographic algorithm uses one public key and one private key to generate a binary sequence of pseudorandom numbers that indicate where the elements of the binary sequence of a secret message will be inserted. The insertion takes eventually place at the first seven AC coefficients in the transformed DCT domain.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 5, May 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1105075 |

4.1 Advantage

- These proposals focus on areas, or regions, in a photo that are similar to other areas, such as the pixelated region of an eye. If this region of the eye matches up with other regions of the eye, then the R-CNN knows it has found a match. Face detection is the process of identifying or verifying the identity of a person using their face.
- It captures, analyzes, and compares patterns based on the person's facial details. The face detection process is an essential step in detecting and locating human faces in images and videos.
- The benefit of using CNNs is their ability to develop an internal representation of a two- dimensional image.
- This allows the model to learn position and scale of faces in an image.
- After train the CNN it can able to recognize face in an image One can effectively use Convolutional Neural Network for Image data.
- A Steganography System consists of two functions: embedding and extraction. The objective of the proposed work is to design robust algorithms which generate stego media, can carry large amount (capacity) of secret data without reducing imperceptibility.
- The steganographic algorithm uses one public key and one private key to generate a binary sequence of pseudorandom numbers that indicate where the elements of the binary sequence of a secret message will be inserted.

4.1.1 Architecture

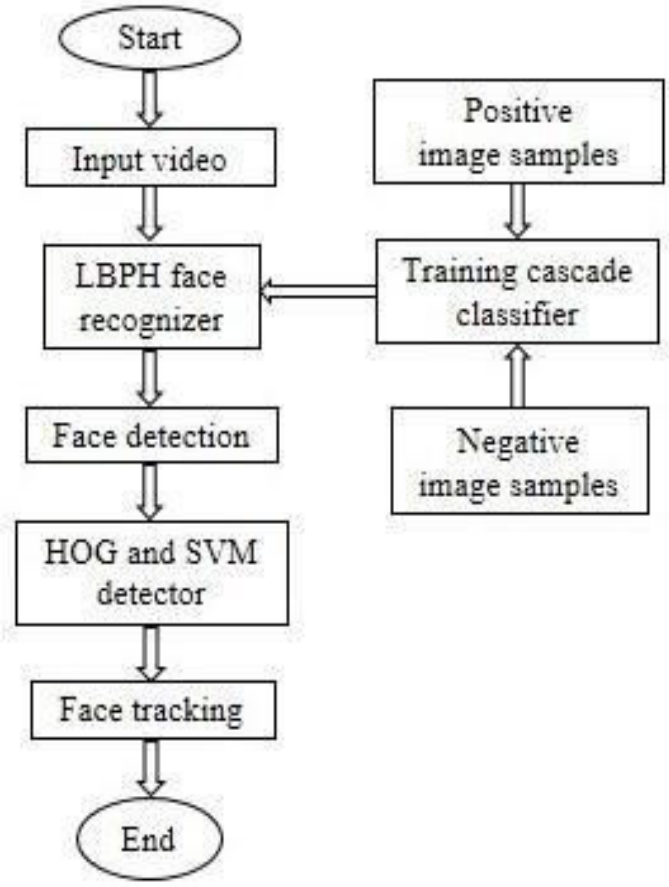

Figure: Architecture of the Project

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 5, May 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1105075 |

V. METHODOLOGIES

- OpenCV
- dlib
- Face_recognition

OpenCV is an image and video processing library and is used for image and video analysis, like facial detection, license plate reading, photo editing, advanced robotic vision, optical character recognition, and a whole lot more. The dlib library, maintained by Davis King, contains our implementation of "deep metric learning" which is used to construct our face embeddings used for the actual recognition process.

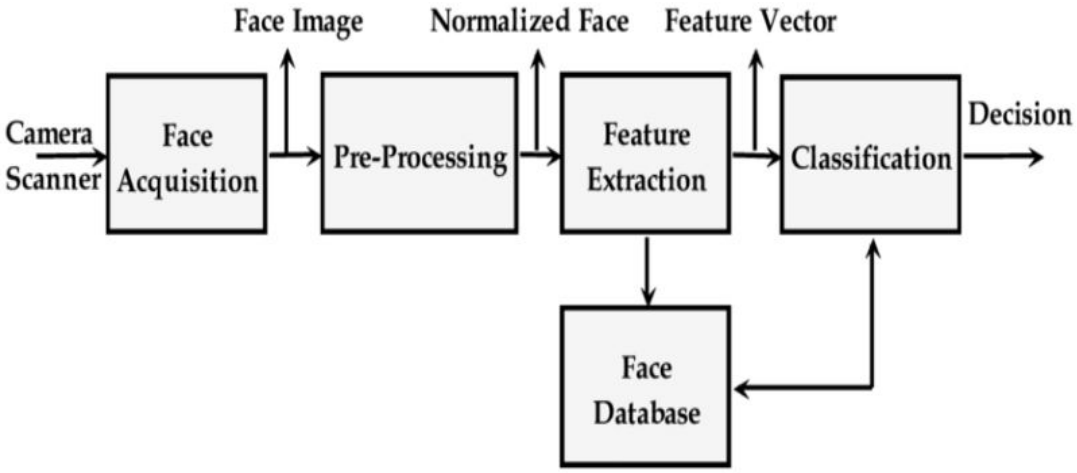

Figure: Implementation of the Project

The face_recognition library, created by Adam Geitgey, wraps around dlib's facial recognition functionality, and this library is super easy to work with and we will be using this in our code. Remember to install dlib library first before you install face_recognition. the science of communicating in a hidden manner. SSIS conceals a message of substantial length within digital imagery while maintaining the original image size and dynamic range.

The hidden message can be recovered using the appropriate keys without any knowledge of the original image. he most commonly method used for steganography technique is a Least Significant Bit (LSB) algorithm. LSB algorithm performs the embedding operation of message along with the image file where each pixel has a size of 3 bytes.

Digital Watermarking –
Digital watermarking is the procedure of embedding data into a digital signal in a way that is complex to delete.

Visible Watermarking − In this visible watermarking, the information is visible in the picture or video.

VI. TEST PLAN

Searches for the control's image on the screen pixel-by-pixel. For desktop and web applications, it will search for the image on the PC desktop, and for mobile application, it will search for the image on the screen of the connected mobile device. If the image is found, gets its coordinates. Simulates a needed user actions at the image's coordinates.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 5, May 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1105075 |

6.1 Analyze the System

In face analysis, face detection uses facial expressions to identify which parts of an image or video should be focused on to determine age, gender and emotions. In a facial recognition system, face detection data is required to generate a faceprint and match it with other stored faceprints.

6.2 Design the Test Strategy

Designing a test strategy for all different types of functioning, hardware by determining the efforts and costs incurred to achieve the objectives of the system. For any project, the test strategy can be prepared by

1. Define the project scope.
2. Agree on a project methodology.
3. Formulate a development approach.
4. Estimate and plan the project.

6.3 Define the Test Objectives

The objective of face recognition is, from the incoming image, to find a series of data of the same face in a set of training images in a database. The great difficulty is ensuring that this process is carried out in real-time, something that is not available to all biometric face recognition software providers Face Detection is the first and essential step for face recognition, and it is used to detect faces in the images. It is a part of object detection and can use in many areas such as security, bio-metrics, law enforcement, entertainment, personal safety, etc.

Face recognition and Face detection using the OpenCV. The face recognition is a technique to identify or verify the face from the digital images or video frame. A human can quickly identify the faces without much effort. It is an effortless task for us, but it is a difficult task for a computer.

6.4 Define Test Criteria

Two integral images used for computing the mean and variance in EEC. Also in our experiments the values for variances and ◌ כ has been set with 64 and 0.9, respectively. These values determined by a thresholding process. By using these values, 3 faces have been lost in the CMU-MIT dataset. Also, RM and ADT criteria 0 0.2 0.4 0.6 0.8 1 0 5 10 15 20 25 30 35 Detection rate # false positives (1.0e6) Cascade ADT Reg min LIT EEC Hossein ZiaeiNafchi and SeyedMortezaAyatollahi / Procedia Computer Science 13 (2012) 162 – 170 169 lose one face, while LIT criterion lost another face. Totally, proposed criteria failed to detect two faces in CMUMIT dataset.

The proposed preprocessing criteria show significant advantage against EEC in terms of detection rate, rejection rate and speed. The first part of EEC is fast enough but the second part is not. Therefore, still variance classifier part of EEC can be a proper preprocessing step. Table 1 provides the performance of the proposed criteria and EEC.

6.5 Resource Planning

In order to create this system first we will have to make the datasets. When the image quality becomes favourable different procedures will take place in the face recognition system the tasks are performed using the python queries “python encode_faces.py”. The input will be taken from the dataset which will be received in the “encodings.py”. There will be precision formatting in the system wherein face embedding for each face will occur. Secondly a file “recognize_faces_images.py” will contain all the required methods and the techniques for the process of identification of the face of the person from the given image of the dataset. The given file will be executed by the python command “python recognize_faces_image.py-encodings”.

We can resize or turn the image for approximity with the goal for getting the desired output. The present classifier along with OpenCV libraries will enhance the outcome or results in the face recognition system.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 5, May 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1105075 |

6.6 Plan Test Environment

It works by identifying and measuring facial features in an image. Facial recognition can identify human faces in images or videos, determine if the face in two images belongs to the same person, or search for a face among a large collection of existing images.

6.7 Schedule & Estimation

AI photo recognition and video recognition technologies are useful for identifying people, patterns, logos, objects, places, colors, and shapes. The customizability of image recognition allows it to be used in conjunction with multiple software programs. For example, after an image recognition program is specialized to detect people in a video frame, it can be used for people counting, a popular computer vision application in retail stores.

Depth Estimation is the task of measuring the distance of each pixel relative to the camera. Depth is extracted from either monocular (single) or stereo (multiple views of a scene) images. Traditional methods use multi-view geometry to find the relationship between the images.

Depth estimation is a computer vision task designed to estimate depth from a 2D image. The task requires an input RGB image and outputs a depth image. The depth image includes information about the distance of the objects in the image from the viewpoint, which is usually the camera taking the image Pose Estimation. **Keypoint Detection** involves simultaneously detecting people and localizing their keypoints. Keypoints are the same thing as interest points. They are spatial locations, or points in the image that define what is interesting or what stand out in the image.

1) The concept of depth estimation refers to the process of preserving 3D information of the scene using 2D information captured by cameras. Monocular solutions tend to achieve this goal using only one image. These methods aim to estimate distances between scene objects and the camera from one viewpoint.

2) This requires the method to perform depth estimation on low-cost embedded systems. There are a variety of devices commercially available to provide depth information, however, their processing power, computational time, range limitation and cost make them impractical for consumer devices. Sensors such as Kinect are commonly used in consumer devices .

3) These types of sensor are categorized as Time-of-Flight (ToF) where the depth information is acquired by calculating the time required for a ray of light to travel from a light source to an object and back to the sensor .ToF sensors are more suitable for the indoor environment and short range.

4) The key advantages of LiDAR sensors are high resolution, accuracy, performance in low light and speed. However, LiDARs are expensive devices and they require extensive power resources which make them unsuitable for consumer products.

5) It has been shown in the state-of-the-art that monocular depth estimation methods could be a potential solution to address many of these challenges. These methods perform with a relatively small number of operations and in less computation.

6) They do not require alignment and calibration which is important for multicamera, or multi-sensor depth measurement systems. Accurate monocular depth estimation methods can play an important role in understanding 3D scene geometry and 3D reconstruction, particularly in cost-sensitive applications and use cases.

VII. SYSTEM STUDY

Take the facial recognition transfer as an example, we will test the connectivity, message format, invalid parameter verification, and return code, etc. Besides, facial recognition uses biometric technology and artificial intelligence algorithms and models. The transfer speed and result will be affected by the light, the background, the hairstyle, glasses, and other decorations. Although the model is built and trained perfectly, 100% accuracy is currently not guaranteed. Therefore, the standard divers in different sectors, the face recognition accuracy rate and pass criteria are determined by each domain. The general face recognition accuracy rate of the industry is greater than or equal to 99%.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 5, May 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1105075 |

When the interface of the face recognition model can be successfully invoked, and the accuracy rate of recognition meets the standard requirements, it is deemed to have passed the test.

Figure : Testing Diagram of the Project

7.1 Unit Testing

The following figure shows the main test process of a facial recognition model. Firstly, we need to prepare a certain amount of test data of two parts: one is a set of test materials, such as a pair of face photos, the other one is to tag label for the materials according to the model to be tested, that is, the matchup of face photos. After the data preparation is done, we can start testing.

A message requesting the service of the model is constructed for each test material and sent to the "face recognition service", and compares the returned result with the label. After all the test data are been tested, calculate the accuracy rate, recall rate, misrecognition rate, and other indicators based on the result set to evaluate the tested model.

7.2 Integration Testing

The method was proposed to improve the efficiency of finding the lost person in Al Nabvi mosque, Madinah. This will facilitate the department of lost and found to automate the current manual work. The method integrates the reporting and finding of lost persons in a single framework, where a complainant registers the missing report through a mobile app and provides the basic profile info of the lost person; then, the system fetches the face images of that person from the central database and extracts the learning features, which are necessary to train the face-recognition algorithms.

The proposed method examines the video streams at the frame's level and employs the Viola–Jones algorithm for real-time face detection, which first extracts the feature images into a large sample set and then uses the cascading AdaBoost algorithm as the face detector. The algorithm not only locates the human faces but also applies a bounding box around the human face to localize the entire face region.

7.3 Functional Testing

The system must have an unbiased 'with_mask' dataset.The dataset must have over 1500+ images in both 'with_mask' and 'without_mask' classes. The dataset must not re-use the same images in training and testing phases. The system must be correctly able to load the face mask classifier model. The system must be able to detect faces in images or video stream. The system must be able to extract each face's Region of Interest (ROI).

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 5, May 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1105075 |

There must not be any object between the system and the face of the user for a successful facedetection and hence the face mask detection. The end position of the face must be fit inside the webcam frame and must be closer to thecamera.Correctly able to detect masks in 'png', 'jpg', 'jpeg', and 'gif' format images.The system must be able to detect face masks on human faces on every frame in a live video.The results must be viewed by showing the probability along with the output of 'Mask' or 'NoMask'. The test data is very important because, on the one hand, the number of data will influence the result. Too little data is prone to contingency.

The result of the test sample has a greater impact on the model evaluation index. On the other hand, the test data should be "real", fitting the real situation including the positive and negative examples. In order to be close to the use cases, you can prepare a photo collection(A) of daily life and a photo collection(B) of identification photos. When choosing the daily life photo, the ages, hats wearing, glasses-wearing, etc should be considered.

7.4 System Test

You should read about True positive and True negative, false positve and negatives. With this formula of your accuracy=(TP+TN)/(Total). face recognition accuracy cab be measured according to the percentage of the recognized faces per the total number of tested faces of the same person. 20 Thankfully, the OpenCV package comes with pre-trained models for face detection, which means that we don't have to train an algorithm from scratch. More specifically, the library employs a machine learning approach called Haar cascade to identify objects in visual data.

7.5 White Box Testing

A few of the other names given to white box testing are open box testing, transparent box testing, glass testing, and code-based testing. With the help of white box testing the tester can find whether or not there are any security loopholes, if the codes are perfectly structured, the input flow in the code, checking conditional loops and testing every element individually.

The testing on the features and components is repeatedly done to ensure that they work in the way they are expected. Small components are taken and tested and when the goal is achieved the next component is taken. It is also important that the testings are energy efficient, that is there is a balance between the amount of energy put to the amount of output obtained.

7.2.6. Black Box Testing

Black box testing can check additional aspects of the software, beyond features and functionality. A non-functional test does not check "if" the software can perform a specific action but "how" it performs that action. Black box tests can uncover if software is: Usable and easy to understand for its users.

Black-box testing, also called functional testing, relies on the input/output behavior of the system. In particular, the system is subjected to external inputs, so that the corresponding outputs are used to verify the conformance of the system to the specified behavior, with no assumptions of what happens in between.

VIII. IMPLEMENTATION

- Tkinter module – Tkinter is the standard interface in python for creating a GUI that is Graphical User Interface.
- tkinter import * – import everything from the module.
- tkinter.filedialog – This module is used to work with files.
- from tkinter import messagebox – Import message box separately for showing messages on the screen.
- PIL module – This is the images module from the pillow. The PIL module helps to open, manipulate and save many different forms of images.
- Import ImageTk – ImageTk module used to create and modify Tkinterphotoimage from PIL images.
- io import Bytesio – Bytes data in the memory.
- Import os – This module is used for creating and removing any directory.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 5, May 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1105075 |

IX. CONCLUSION

This paper proposes a novel system architecture of face detection, which is in possession of modular characteristic. What's more, the first module based on FPGA can be seen as a USB device with the characteristic, plug and play, making it possible to assist the target systems with USB interface, in implementing real-time face detection, especially the target systems with limited performance of processor and hardware resource.

Testing results show that for the input image with the resolution 640××480, real-time face detection can be implemented, and detection accuracy is 89 %. Face detection is a computer technology being used in a variety of applications that identifies human faces in digital images. Face detection also refers to the psychological process by which humans locate and attend to faces in a visual scene.

X. FUTURE SCOPE

The objective of face recognition is, from the incoming image, to find a series of data of the same face in a set of training images in a database. The great difficulty is ensuring that this process is carried out in real-time, something that is not available to all biometric face recognition software providers.

A face recognition system is a computer application for automatically identifying or verifying a person from a digital image or a video frame from a video source. One of the ways to do this is by comparing selected facial features from the image and a facial database.

Facial recognition solutions are expected to be present in 1.3 billion devices by 2024. Powered by AI, facial recognition software in mobile phones is already being used by companies like iProov and Mastercard to authenticate payments and other high-end authentication tasks.

Digital effigy conceal and its derivatives are growing in use and application. In areas where cryptography and strong encryption are being outlawed, citizens are looking at conceal to circumvent such policies and pass messages covertly.

The Future of conceal is an article that describes new and innovative technological methods used to hide information. The following is an excerpt of the article: Our ability to discover hidden information during our investigations is vital, especially as new and innovative methods continue to evolve.

REFERENCES

[1]Henniger O., Fu B., and Chen C.. 2020. On the assessment of face image quality based on handcrafted features. In Proceedings of the International Conference of the Biometrics Special Interest Group (BIOSIG). Gesellschaft für Informatike.V., 273–280.
[2]Rose J. and Bourlai T.. 2020. On designing a forensic toolkit for rapid detection of factors that impact face recognition performance when processing large scale face datasets. In Securing Social Identity in Mobile Platforms: Technologies for Security, Privacy and Identity Management. Springer International Publishing, 61–76.
[3]Lijun Z., Xiaohu S., Fei Y., Pingling D., Xiangdong Z., et al. 2019. Multibranch face quality assessment for face recognition. In Proceedings of the 19th International Conference on Communication Technology (ICCT). IEEE, 1659–1664.
[4]Rose J. and Bourlai T.. 2019. Deep learning based estimation of facial attributes on challenging mobile phone face datasets. In Proceedings of the International Conference on Advances in Social Networks Analysis and Mining (ASONAM). ACM, 1120–1127.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.379

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