ChikonEye: Open Source Software for Preventing Unauthorized Access to Electronic Devices and Information using Face Recognition

Ashrafur Rahman Minhaj
Britannia University
Cumilla - 3500, Bangladesh

Masum Bakaul
Britannia University
Cumilla – 3500, Bangladesh

ABSTRACT
In this emerging era of technology, ensuring data security is a challenge to be provided for systems of different sizes and types. An open source software is presented to allow authorization to a device having sensitive work-related information. In an exemplification of this project, an unlocked device configured to capture images, analyze the images to see who and how many faces are looking at the device and automatically locks the device if detected faces is not recognized as authorized. The software is implemented using open source computer vision (OpenCV) library for image processing operation. The recognizer has been trained with 100 images of each authorized user to generate a dataset on which the system relies to recognize authorized users using openCV python bindings. Voila-Jones algorithm is used to detect faces in images using the built in camera of a system.

Keywords
Face Recognition; Access Control; Camera; Computer Vision.

1. INTRODUCTION
Information security means protecting digital measures that are applied to prevent unauthorized access to databases, computers and websites. The goal of data security or information security is to provide access to data to authorized users only [1].

Whether it is personal work or completely confidential sensitive information stored in an electronic device needs to be shown on a screen. By looking at from behind the user people might get access to that information as well. For that a third eye was needed to prevent peepers.

Determining identity or authentication is a challenge in this reticulated modern world. Unlike other biometrics systems like voice recognition, typing keystroke, iris, fingerprint / palm print, face recognition has some advantages as images can be captured from a distance without notifying the person being recognized. Also electronic devices such as laptop computers has already a camera built in which is used to capture images in real time.

In this paper, we present a system which prevents peepers from accessing valuable sensitive information as well as the device. The system automatically takes images to analyze and find authorized user. It starts capturing images using its camera when the device is on, finds faces, counts faces in an image and recognize authorized users by matching captured images to previously taken images of a user, if there is no match then it saves the image as burglary image and locks the device instantly to prevent peepers from accessing sensitive information. If any unauthorized user is detected it saves the image with exact date time and locks the system immediately.

2. LITERATURE REVIEW
Lihua Zhao and Richard Tsai invented a system for locking and unlocking mobile device using face recognition [4]. In 2007 Jignesh J. Patoliya and Miral M. Desai published a conference paper "Face Detection based ATM Security System using Embedded Linux Platform" where authors proposed a face recognition based ATM security system using open source computer vision library, the system prevents unauthorized access in ATM machines and locks down the deceiver [5]. Mrutyanjanya Sahini, Subhashree Subudhi, Mihir Narayan proposed a face recognition based home security system using PCA face recognition algorithm [6]. In 2016 Cyrus Azar, George Brostoff invented a method for authorization to electronic devices using face recognition technology and screen gesture where the device is to be oriented in a predetermined position [3]. Anil k. Jain, Arun, Ross and Sharath Pankanti stated in their paper the methods used in biometrics for establishing identity [1].

3. FACE RECOGNITION METHODOLOGY
Face recognition algorithm contains various methodology to detect faces in images. In this system Voila-Jones algorithm is used to detect faces using Haar based cascade classifier. A classifier is trained using lots of positive and negative images. Positive images are images that contain the feature we want to detect (images with faces), and negative images are random images that does not contain positive feature (images without face). Haar like feature sums up the difference between different regions of an image then categorizes subsections of an image. A 24x24 window image results more than 160000 features to check if there is face or not. But in an image most of the pixels contain no face or can be said as non-face region, Paul Viola and Michael Jones proposed to apply some group of features to be checked first instead of applying all the features [2].
No matter how large the image is, it converts into an integral image with only four pixels. At first less feature is checked then if it passes another feature is checked at that region. Thus within a very short time the feature (face) can be detected.

Haar cascade files are supported in openCV is an open source computer vision library to get better knowledge and detect things in images. It supports different programming languages like Python, Java, C++. Here OpenCV with python binding is used to detect faces using the webcam of a computer device.

4. PROJECT OVERVIEW
4.1 GUI
GUI or simply Graphical User Interface provides as the name suggests, it enables developers to include fancy graphical UI (User Interface) to projects. A GUI is developed to provide

user three options after starting the ChikonEye software, which are – Start, Train and Exit. Also live camera reading is showed on a window if Start is selected.

It is made by using a library called PyAutoGUI. It provided all the necessary widgets to build the UI for the project.

4.2 Face Recognition

The project can be divided into three parts Trainer, Detector and Recognizer. The trainer is used to create data set and training the recognizer. It takes 100 photos of a person and saves only the face of that person. As this software is for face recognition the ROI (Region of Interest) is face. After that it converts the images into numpy array and generates a yml file after successful training.

The recognition system follows an algorithm called Voila Jones which follows an approach of training a cascade function using positive and negative images to detect objects in images.

4.3 Flow Chart

After selecting Start the program starts capturing images to identify users or peepers.

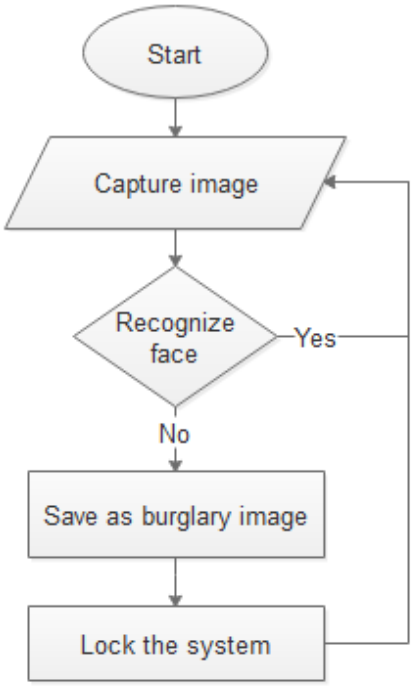

Fig 1: Flowchart

The recognizer does the crucial part. It detects faces and based on the data from the trained yml file it recognizes the authorized users. It decides whether to lock the system or not.

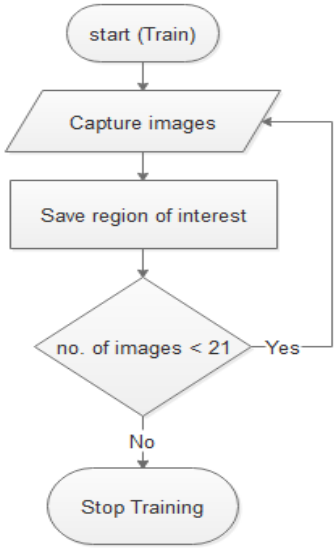

Fig 2: Training Procedure

5. RESULT AND DISCUSSION

The software is realized by a python3.7.1 script running on a laptop computer. The laptops built in camera is used to continuously take images. After running the program, it shows 3 options to Train, Start, Exit.

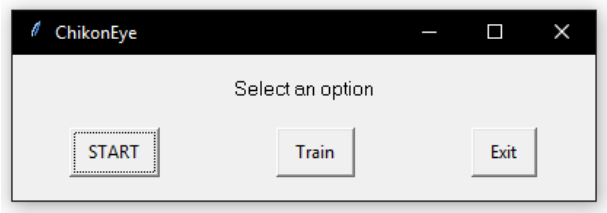

Fig 3: Beginning Window

If Start is selected the software starts recognition process.

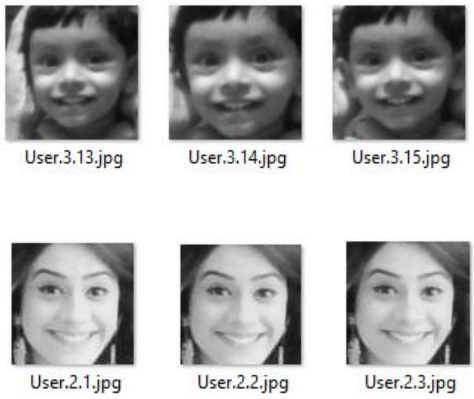

Fig 4: Data Set

Training takes 100 photos of a user and stores it as authorized user image and trains a model to generate a yml file. The test database is created with images of five people (authorized users).

The system can detect faces and recognize authorized users

Figure 5. Detecting Faces

Also if any unauthorized person tried to peep to the computer screen, the system takes a photo and saves the image and locks the computer automatically.

In addition, if exit is selected the software starts recognizer, if authorized person is detected it takes the command else locks the computer preventing unauthorized access to the computer and information.

6. IMPLICATION

The project works well with high accuracy. However, identifying twins has always been a challenge in computer vision. The software does suffer in that other than that, the project is promising in securing access to information and devices.

7. ACKNOWLEDGMENTS

Our thanks to OpenCV (Open source computer vision) library for that image processing has become easier and faster with python bindings.

8. REFERENCES

[1] Anil k. Jain, Arun, Ross and Sharath Pankanti, Biometrics: A Tool for Information Security, June 2006, IEEE Transations on Information Forensics and Security, VOL. 1, NO. 2, DOI = https://doi.org/10.1109/TIFS.2006.873653

[2] Cascade Classifier. (2019). Retrieved July 2019 from https://docs.opencv.org/trunk/db/d28/tutorial_cascade_classifier.html. [Accessed: 10- Jun - 2019]

[3] Cyrus Azar, George Brostoff, System and method for disabling secure access to an electronic device using detection of a predetermined device orientation. 2016. Patent no. 9,519,769 B2. Issued December 13. 2016.

[4] Lihua Zhao, Richard Tsai. 2015. Locking and unlocking a mobile device using facial recognition. (March. 2015). Patent no. 8,994.499 B2. Filled Mar 16, 2011, issued Aug. 2015.

[5] Jignesh J. Patoliya, Miral M. Desai . Face Detection based ATM Security System using Embedded Linux Platform, 2017. 2nd International Conference for Convergence in Technology.

[6] Mrutyanjanya Sahini, Subhashree Subudhi, Mihir Narayan. Design of Face Recognition based Embedded Home Security System. 2016. Ksii transactions on internet and information systems Vol. 10, no. 4.