JOURNAL OF BASIC SCIENCE AND ENGINEERING

SIGNATURE-BASED DOOR LOCK SYSTEM USING KNN ALGORITHM

Kurra Nagasai[1], Dr.Sunil T.D[2], Dr.Eshwawarappa M N[3],

[1]M. Tech, Student, Department of Electronics and Communication, Sri Siddhartha Institute of Technology, Tumakuru, Karnataka, India.

Kurranani75@gmail.com

[2]Associate Professor, Department of Electronics and Communication, Sri Siddhartha Institute of Technology, Tumakuru, Karnataka, India.

suniltd@ssit.edu.in

[3] Professor & Head of Department, Department of Electronics and Communication, Sri Siddhartha Institute of Technology, Tumakuru, Karnataka, India.

eshwarappamn@ssit.edu.in

Abstract: The Signature verification plays a crucial role in authentication of door lock system, which provides a secured door lock system replacing the use of mechanical lock, scanner card, memorizing password and OTP. It also instills more secured feeling in the user's mind. In this paper, the application of the K-nearest neighbors (KNN) algorithm in signature verification has been explored while using canny edge features extracted from signature images. The project has been conducted by preprocessing a dataset of ten individuals' signature images while extracting canny edge features to represent the unique characteristics of each signature. Subsequently, trained the KNN algorithm using a subset of the dataset, memorizing the feature-label associations. During the prediction phase, utilized the trained KNN model to classify new signature images based on the individual canny edge features. In this work, grey image has extracted from the original image, from that grey image will be converted into edge image, from that Histogram of Oriented Gradients (HOG) feature descriptor is used to extract features from the edge-detected image, this will do for both reference image and verification image and mean feature vector will also calculate and then both images will be compared then the authentication process will be done. By comparing the 'K' values of k=1 and k=3, Our findings highlight the significance of 'k' in influencing the accuracy and reliability of signature verification which is crucial to increase the accuracy of door lock security system and there by optimal selection of 'k' for different applications.

Key words: Signature based Door Lock Systems; KNN Algorithm; Canny Edge Detection Technique.

1. Introduction

In our society door have special place which helps by protecting entire house by not allowing unauthorized persons into house. The secured door lock mechanism gives protection form access to unauthorized persons. In olden days traditional lock system is used as lock mechanics like pin tumbler lock but its protection efficiency is very less compared to electronic locks and in traditional locks, it can open lock easily without original lock by using thin screw driver, because of this traditional locking system security is weak compared to electronic lock system. Hence to increase the level of security to door lock system it has shifted to electronic door lock system from traditional lock system. In electronic lock system OTP and RFID type lock system is used which removes the usage of metal lock. In place of metal lock, Scanner card or OTP is used as metal lock, but if card is lost or if forget the OTP, may can't open the door.

Hence Biometric based lock system was introduced to improve this electronic lock system, and in this need not to remember specific and secret password and need not to carry any lock or card but ourselves can become a lock by scanning different biometric fingerprint ridges in fingerprint lock system, iris lock system, face recognition lock system and hand written signature lock system.

In authentication process handwritten signature has an important role in daily life activity, for every formal process like bank cheques, written orders issued, agreements made, etc. This signature authentication is different from other biometric authentication as signature-based authentication has low efficiency compare to other biometric authentication methods. However, signature collection, authentication and storage of signature is less complicated in the signature-based system when compare to other biometrics. In the signature-based system, can keep or write any name in place of user's signature that can't be forged by others and this feature makes signature-based security systems safer when compared to other biometric authentication systems. There are two types of signature-based systems, a) online based signature verification and b) offline based signature verification.

In online based signature verification pressure is applied on touch screen and time taken to make signature and dynamic features are taken as parameters to verify whereas physical features extraction is involved in verification of signature in offline signature verification.

In offline signature verification feature, extraction of signature will be done by using canny edge detection technique, in this it will detect wide range of edges in image as the edge detected image gives critical features of signature which used for classification.

Classification is done through KNN algorithm. During training phase, dataset of signatures is fed to system by authorized persons, and each signature is labeled and stored and used for comparison, when a new or stored/labeled signature is presented the KNN algorithm calculates the distance between the new signature features with that of stored signature features while identifying the closest matches. Access is granted if the new signature closely matches with the signatures of authorized users, ensuring that only legitimate individuals can gain entry.

The integration of canny edge detection and the KNN algorithm provides a high level of accuracy in handwritten signature-based door lock security system. Canny edge detection is capable of clear feature extraction and KNN is strong in classification and combination of both helps in increasing the level of accuracy in handwritten signature base door lock security system.

2. Literature survey

Some of the approaches that had been used for signature verification form the heart for handwritten signature-based door lock security system. Ahmed Abdelrahaman et.al [1] This article details that the offline signature is taken and its features are extracted using radon transform and classification is done by using KNN algorithm, extreme points warping algorithm is used to align two signatures, the signature is then classified as genuine or forgery according to the alignment scores. Tushara D1, Shridevi Raddy et.al [2] This article described that online signature is taken and extract the dynamic features of the signature like X, Y coordinate of the signature along with the velocity component and artificial neural network is taken as classifier and compares both the trained/reference signature with verification signature and gives the result as matched/unmatched. Prakash Ratna Prajapati et.al [3] In this Article, offline signature was taken and auto-encoder has been used to compress the image which can be used as forged signature to compare with original image and convolution neural network is used as a classifier. Edson j. r. justinoet.al [4] In this work offline signature was used and Hough transform was used to locate stroke lines in signature image. The Hough transform was used to extract the parameterized Hough space from signature skeleton as unique characteristic feature of signatures. Back Propagation Neural Network was used as a tool to approximate the performance of the proposed method. Yanti Desnita Tasri [5] In this work the aim to implement the canny edge detection method to identify a person’s signature, if it had a similarity percentage of 70% to 100%. Aang Alim Murtopo et.al [6] In this work, offline signature was taken and signature feature were extracted by Harris corner feature extraction method and KNN algorithm was used for classification and in that classification, they used two types of calculation viz., Euclidean distance and Manhattan distance. Eshwarappa M.N et.al [7] In this work, offline signature was taken and for the signature features are extracted by using Discrete Cosine Transform analysis (DCT) as global feature of a signature image and Vertical Projection Profile Analysis (VPP), Horizontal Projection Profile (HPP) are static features of a signature and it compare by Euclidean distance threshold, if the verification image crosses that threshold, then it is taking as matched signature. C. Sridhar Babu et.al [8] In this project, face recognition technology was employed for a door lock security system. The recognition process utilized both the HAAR Classifier and the Local Binary Pattern Histogram (LBPH) methods. When an authorized individual is detected by the system, their name is displayed, and a servomotor is triggered to unlock the door. Conversely, if an unauthorized individual is detected by the webcam, a notification showing "unknown" is displayed on the website. Additionally, an alert email containing the image of the unauthorized person is sent to the owner’s email address.

3. Problem statement

One can manipulate the door lock security systems based on face recognition, fingerprint, speech recognition. For instance, in face recognition even if person is in sleep or unconscious state then also the face recognition may work; Similarly in fingerprint sensor may easily collect fingerprint of persons by collecting the recently used things and further the ridges of fingerprints will become smooth for persons who used to work with hands and by ageing leading to mismatch of finger prints. In speech recognition system also the security system can be manipulated by talking or by voice cloning. So, this handwritten signature-based door lock security system can be adopt to improve the security of door lock system, signature can forge until they know that what signature you have given as reference signature, mostly that will know to the person who's signature is and system only. Thus, the effectiveness of signature-based door locking system in providing safe security to be established by this project.

4.Methodology

The project work has been done in a systematic method by dividing it into five major sections and implementation is done according to the figure.1 (1) collection of data (signatures of Individuals and related works to choose what classifier and features extraction should be used); (2) Image processing, Labeling & features extraction of collected signatures;(3) Training of KNN; (4) verification& image processing; (5) Implementation of circuit for door lock security system. MATLAB, ESP WROOM 32, solenoid lock is used in this project.

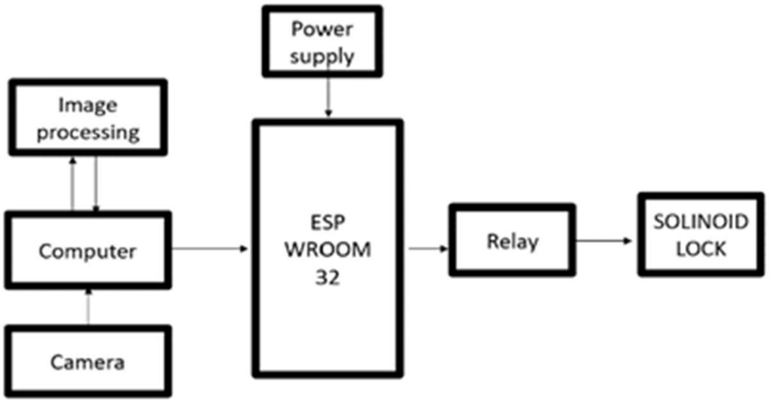


Fig 1. Block Diagram of Handwritten Signature based Door lock security system

4.1 Collection of data:

Collected 10 Individual's signatures for door lock authentication purpose to use as a reference signature of 5 samples from same person.

4.2 Image processing, Labeling & features extraction of collected signatures

Algorithm: Image processing, Labeling & features extraction of collected signatures

STEP 1: Load Reference Image Dataset:
STEP 2: Prompt the user to select the folder containing images of person 1.
STEP 3: Read all image files in the selected folder.
STEP 4: Count the number of reference images.
STEP 5: Extract Features from Reference Images (Person 1):
STEP 6: For each reference image: Read the image.
STEP 7: Resize the image to a standard size (60x120 pixels).

STEP 8: Convert the image to grayscale.
STEP 9: Extract features using the Canny edge detection method.
STEP 10: Calculate the mean value of the feature vector.
STEP 11: Append the mean feature value to the features array.
STEP 12: Assign the label 1 to the reference image and append it to the labels array.
STEP 13: END

Same process will be repeated for 2nd individual and so on for 'n' number of individuals.

In this process the collected reference images will be placed in allotted persons folders and folders of 1 person (or 'n' number of persons) will be selected and form into reference folders and images in this folder will be read and counted and then all the reference images will be converted into stranded image. This stranded image will be converted into greyscale image as shown in the figure 2.

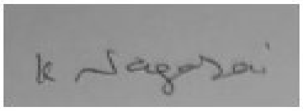


Fig 2. Converted form original image to grey image.

Form this grayscale image the features will be extracted (number of edge pixels, edge density, histogram of edge orientations, normalize the histogram this feature will be extracted) and edge image as shown in figure 3, form this extracted features the mean value of the feature vector will be calculated and given to features array and it assign the label '1' or '2' or '3' in labels array according to the reference folder.

In this canny edge the image will be smooth and noise will be eliminated with Gaussian filter

$$I_{S}(x,y) = \sum_{u=-k}^{k} \sum_{v=-k}^{v} \square\, I(x-u, y-v)G(u,v)$$

(1)

k defines the extent of the convolution operation for the Gaussian blur, impacting the size of the region around each pixel that contributes to the blurred result. K=-1 to 1.

where $G(u,v)G(u,v)$ is the Gaussian kernel.

Gradients represents the rate of change in intensity at each pixel of an image gradient in the X-direction measures the change in intensity form left to right, gradient in the Y-direction measures the change in intensity from top to bottom.

Mathematically, this can be represented as

$$G_x = \frac{\partial I}{\partial x}$$

(2)

$$G_y=\frac{\partial I}{\partial y}$$

(3)

Gradient magnitude (G*):* $G=\sqrt{G^2{}_x+G^2{}_y}$ (4)

Gradient Direction*(θ):* $\theta=arctan2(G_{x,}\,G_y)$ (5)

The direction represents the orientation of the edge. Orientation Binning is a process of quantizing the range of gradient directions into a fixed number of intervals or bins. This helps in creating a histogram that represents the distribution of edge directions in the image. Histogram of edge orientation will be calculated; it represents distribution of edge directions in an image. When edge detection is performed, not only identify the location of edges but can also determine the directions of those edges at each pixel.

$$H_{(k)}=\sum_{x=1}^{m}\sum_{y=1}^{n} 1[\text{Ø}(x,y)\text{€}\{\frac{2k\pi}{k}-\pi,\frac{2(k+1)\pi}{k}-\pi\}]$$

(6)

where k ranges from 0 to -1
Number of edge pixels marked as edges (non-zero pixels in the edge-detected image E)

$$N_{edges}=\sum_{x=1}^{m}\sum_{y=1}^{n} 1[\text{€}(x,y)>0]$$

(7)

where 1 is the indicator function

Edge Density*:* $D_{edges}= N_{edges}/mxn$

(8)

Mean value of a feature vector derived from canny edge detection for signature feature extraction can be calculated using the same principle as any other feature vector. The feature vector might include different aspects such as edge pixel count, edge density, Histogram of edge orientations.

$$\text{Mean(f)} =\frac{1}{n}\sum_{i=1}^{n} fi$$

(9)

where n is the number of features in the vector.

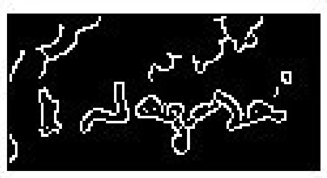


Fig 3. grey image is converted to edge image.

4.3 Training of KNN:

Load preprocessed features (features) and corresponding labels (labels) from a data file. Train a K-nearest neighbors (KNN) classifier (knn Model) using the loaded features and labels It is simple and instance-based learning algorithm used for classification tasks.

In training phase, want to select the reference folders where the training dataset is stored. To make a prediction for a new instance, the algorithm calculates the Euclidean distance and by assigning ‘k’ value the prediction will be done for if k=1 the instance is simply assigned the label of the nearest neighbor.

4.4. Image processing & verification:

Algorithm: Image processing & verification

STEP 1: Load preprocessed features (features) and corresponding labels (labels) from a data file.

STEP 2: Train a K-nearest neighbors (KNN) classifier (knn Model) using the loaded features and labels.

STEP 3: Select Verification Image:

STEP 4: Prompt the user to select an image for verification.

STEP 5: Preprocess Verification Image: Read the selected image.

STEP 6: Resize the image to a standardized size (60x120 pixels).

STEP 7: Convert the image to grayscale.

STEP 8: Extract Features from Verification Image:

STEP 9: Apply the Canny edge detection method to extract edge features from the grayscale image.

STEP 10: Use the Histogram of Oriented Gradients (HOG) feature descriptor to extract features from the edge-detected image.

STEP 11: Predict Label Using KNN Model:

STEP 12: Feed the extracted features of the verification image into the trained KNN model to predict the label.

Same process will be repeated for all images extracted signatures

For verification a new signature through camera will be given and that image will also go under feature extraction through canny edge.

4.5 Implementation of circuit for door lock security system

Algorithm: Implementation of circuit for door lock security system

```
STEP 1: Verify Access and Control Door Lock
STEP 2:  Compare the predicted label with the expected label (authorized person's label).
STEP 3:  If the predicted label matches the expected label:
STEP 4:  Unlock the door by sending a signal through a serial port (COM3).
STEP 5:  If the predicted label does not match the expected label: Keep the door Locke
```

If the verification image matches with reference image than the door will be unlocked, through ESP wroom 32 to relay to solenoid lock, like shown in figure 1, if the verification image is not matches with reference image than the door will be remains locked.

5. Results and Discussion

The Results obtained at the end of the experiment are in accordance with stipulated algorithms. All samples of individuals gave consistent results confirming the correctness of Algorithms. When the authorized user display signature in front of camera same will be processed as per figure 1 block diagram and algorithm then door will open inferring that the signature given is matched with reference signature stored in the system like shown in figure 5. The door remains locked if the given signature is not matched with the stored one like shown in figure 4. This can be implemented in real time to door like shown in figure 6. In this project, K-nearest neighbors (KNN) has been used for classification which a simple, instance-based learning algorithm. KNN is easy to use. By using the canny edge for feature extraction and KNN algorithm it got accurate result for handwritten signature-based door lock security system.

The results signify that the signature-based door lock systems are more secured systems as they are less prone to forgery. The user can use Signature, or name or code of words in the place of signature and only authorized user can knows the encryption of signature that stored in the system for authentication. Hence, breaking of security of signature-based system is not possible for any unauthorized person without knowing the signature stored in system.

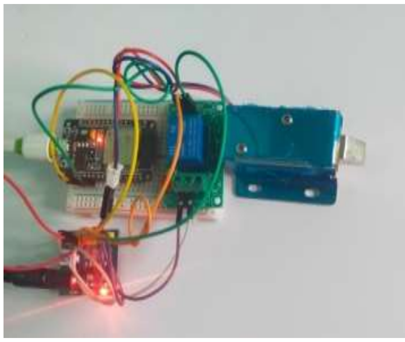


Fig 4. locked position

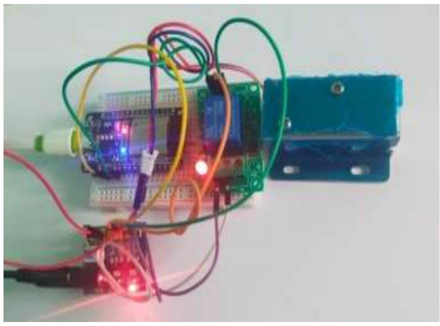
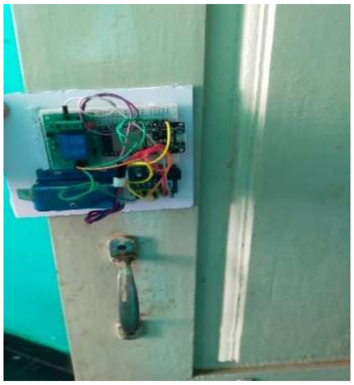


Fig 5. Unlocked position



Fig

6. Door lock setup

6.Conclusion

To ensure the strong security for house and to avoid the carrying of key physically with us or remembering the OTP to get access, we shifted into this biometric door lock system. The signature-based door lock system has a special feature that assures high security. This ease of verifying and matching with more features of stored signature is a significant feature of signature-based door lock system as it provides efficient security to the door lock.

7. References

1. Ahmed Abdelrahaman A. A., Ahmed Abdallah M. E.K-Nearest Neighbor Classifier for Signature Verification System 2013 International Conference on Computing, Electrical and Electronic Engineering (ICCEEE)

2. Tushara D, Shridevi Raddy, Shreya KM, Spoorthy Y, Signature Verification System using Neural Networks International Journal of Engineering Research & Technology (IJERT) Special Issue - 2021 ISSN: 2278-0181 NCCDS - 2021 Conference Proceedings

3. Prakash Ratna Prajapati a, Samiksha Poudel b, Madan Baduwal c, Subritt Burlakoti d, Sanjeeb Prasad Panday, Signature Verification using Convolutional Neural Network and Autoencoder Journal of the Institute of Engineering Volume 16, No. 1 ISSN: 1810-3383 Published: April 2021

4. Edson j. r. justino' Abdenaimel yacoubi' Flavio bortolozzi' Robert Sabourin, An Off-Line Signature Verification System Using Hidden Markov Model and Cross-ValidationIEEE Int. Workshop on Neural Networks for Signal Processing,pp. 859–868, 2000.

5. Yanti DesnitaTasri a,Identification of Signature Images with Edge Detection CannyJournal of Ocean, Mechanical and Aerospace November 30, 2022 -Science and Engineering- 30th November 2022. Vol.66 No.3 © 2012 ISOMAse

6. Aang Alim Murtopo, Bayu Priyatna, Rini Mayasari Signature Verification Using The K-Nearest Neighbor (KNN) Algorithm and Using the Harris Corner Detector Feature Extraction Method, P-ISSN: 2715-2448 | E-ISSSN: 2715-7199 Vol.3 No.2 July 2022 Buana Information Tchnology and Computer Sciences (BIT and CS)

7. Eshwarappa M.N. Dr. Mrityunjaya V. Latte, Multimodal Biometric Person Authentication using Speech, Signature and Handwriting Features (IJACSA) International Journal of Advanced Computer Science and Applications, Special Issue on Artificial Intelligence

8. C. Sridhar Babu, Uttara Nanduri, G. Deepshikha, Sai Sunidhi Pabba, Door Lock System Using Face Authentication and Arduino UNO, international journal of novel research and development (IJNRD)