Multi-Biometric Dynamics Authentication System

Sujit Barnwal[1], Anjali Gajakosh[2], Bharti Singh[3], Sachin Desai[4]

[1]BE Student, computer Engineering, Smt. Indira Gandhi College of Engineering, Navi Mumbai, Maharashtra, India
[3-4]Professor, Department of computer Engineering, Smt. Indira Gandhi College of Engineering, Navi Mumbai, Maharashtra, India

---***---

Abstract - *This paper represents a model for authentication using biometrics like Keystrokes, iris scan and voice recognition. This Biometric Authentication not only reduces the risk of forgetting user's passwords and PINs but also enables users to authenticate incredibly easy and quick through it. This paper propose a joint end-to-end model, which uses a deep neural network to generate feature extraction from biometrics given by user to authenticate while login user. For this purpose, the multitask features learning deep model mines rich information such as human attributes, iris scan, actions interactions, and information from a voice to produce password. This information is taken out through a CNN, which is fine-tuned for these specific tasks. Our experiments show that our models execute well on standard datasets. This representation will not only save processing time but will also save storage space.*

***Key Words*: Keystroke, Biometric, Iris Authentication, Voice Authentication.**

1. INTRODUCTION

The days of using your PIN every time you make a payment or unlock your Device/phone might soon become a thing of the past. Security concerns are one of the most important reasons why biometric authentication has become the need of the hour. People are already switching to biometric identification techniques such as Iris, voice recognition to validate the authenticity of the user. From maintaining the attendance of employee's to combating the challenges of online and offline fraudulence, biometric recognition systems have outsmarted every other security measure. With biometric authentication, you are able to eliminate payment fraud activities such as card skimming, chip switching and shoulder surfing, etc. After its popularity in other environments, it is now gaining ground in financial payment systems. Biometric payment cards are already available and are gathering customer interest and engagement with every passing day.

1.1 Keystroke Dynamics

Keystroke dynamic biometric is based on typing pattern, rhythm and speed. Every user has a certain way of typing that separates him from other users like how long does a user press the keys, how much time between consecutive key presses, etc. Keystroke dynamics is the detailed timing information which describes exactly when each key was pressed and when it was released as a person is typing at keyboard. The main motivation behind this effort is due to the fact that keystroke dynamics is economical and can be easily integrated into existing computer system with minimal alteration and user intervention. Compare to another biometric system the keystroke dynamic is providing high security to users.

Dynamics :

1. Key down hold time (H Time),
2. Keydown–keydown time (DD Time),
3. Time from when a key was released to when another key was pressed (UD time).

1.2 Iris scans

The iris is an externally visible, yet protected organ whose unique epigenetic pattern remains stable throughout adult life. The iris is the colored part of the eye. Each iris is unique, and even irises of identical twins are different. Iris scanning can be used quickly for both identification and verification Applications because of its large number of degrees of freedom. Iris recognition is regarded as the most reliable and accurate biometric identification system available.

Dynamics :

1. IRIS ACQUISITION - Image acquisition is the action of retrieving an iris image from source
2. IRIS LOCALIZATION & SEGMENTATION
3. Unique patterns in iris
4. The colored circles in people's eyes
5. Set of pixels containing only the iris.

1.3 Voice recognition

At the time of enrollment, the user needs to speak a word or phrase into a microphone. Vocal tract is not affected by a cold. This is necessary to acquire speech sample of a candidate. Individual's voice is based on the shape and size of their vocal tracts, mouth, nasal cavities, lips, etc. There are two different types of voice/speaker recognition system, i.e. text dependent and text independent systems. A text-dependent system verifies the identity of an individual on the basis of the utterance of a fixed predetermined phrase, such as the person's name. A text-independent system verifies the identity of a speaker regardless of what he or she says. Text- independent voice recognition is more difficult than text-dependent verification but offers more protection against fraud.

Dynamics :

1. Duration - measures the minutia of the voice
2. Intensity
3. Tone
4. Pitch

2. PROBLEM STATEMENT

Biometrics is the science and technology of authentication by identifying the living individual's physiological or behavioral attributes. The first and most common thing that comes to mind when speaking of unique features is the fingerprint, which is a physical characteristic. But there are other characteristics that are more of behavioral in nature, like the way we speak, the way we type on a keyboard, the iris recognition, and several others. Keystroke dynamics leverage the fact that people follow a definite pattern while typing on a keyboard or keypad. Keystroke dynamics is a behavioral measurement and it utilizes the manner and rhythm in which each individual types. In the human eye, the iris is the colored portion in the shape of a ring. If you look closely, you will find it is made of many asymmetric thick thread- like structures. These thread-like structures are the muscles that help adjust shape of the pupil and only allow appropriate amount of light in the eye. By measuring the unique folds of these muscles, biometric authentication tools can confirm identity with incredible accuracy. The way a person says something – movement variations, tone, pace, accent, and so on – is also unique to each individual. The most important properties used for speech authentication are nasal tone, fundamental frequency, inflection, cadence. Combining data from both physical and behavioral biometrics creates a precise voiceprint.

Project Objectives

1. Keystroke dynamics biometrics offer a way to continuously validate the legitimate identity of a user.
2. Iris pattern is formed by 10 months of age, and remains stable throughout one's life. Full enrollment with instruction can take less than 2 minutes. Authentication takes very less seconds.
3. The voice recognition aims at understanding and comprehending WHAT was spoken.
4. To ensure the authentication of a correct user i.e. to avoid fraud user from authentication.
5. Lower the entry barrier to this field by providing a comprehensive reference for novices.

Related Work

In recent years, biometric authentication has been an active area of research due to its low cost and ease of integration with existing security systems. Various researchers have used different methods and algorithms for data collection, feature representation, classification, and performance evaluation to measure the accuracy of the system, and therefore achieved different accuracy rates. Although recently, the support vector machine is most widely used by researchers, it seems that ensemble methods and artificial neural networks yield higher accuracy. Moreover, the overall accuracy of KB is still lower than other biometric authentication systems, such as fingerprint. The objective of this paper is to present a detailed survey of the most recent researches on Biometrics dynamic authentication, the methods and algorithms used, the accuracy rate, and the shortcomings of those researches.

3. METHODOLOGY

In this section, we have discussed the methodology for Biometric Dynamics Extraction using deep neural network-based models. We have introduced a few related works with models that jointly deal with feature extraction and image pre-processing for iris. The initial phase is a the selection of collecting various time details for keystrokes biometric and collecting the scanned pre-processed image of iris for iris scan and extraction of voice features from the voice samples at every samples given by user. We have used the ANN. To the train the model we have to extract the details dynamics stated above [1]. We need to convert it to key value pair as id and password before giving to model. Then the model will find the pattern using various sample passwords and save this pattern in database. And at the time of registration model will extract the dynamics and then matches with previous data stored in the same id given by user. If the model finds it or it fits properly then model will give further access of the system to user or else it will redirect user to registration page. This methodology is applied to all the three Biometric system in this project.

4. ALGORITHM

4.1 Algorithm for Keystroke Biometric

After raw data is collected, it needs to be processed, normalized, and stored for classification. s. When a key is pressed, it creates a hardware interrupt to the processor and generates a time stamp, typically measured with microsecond precision. Using the time stamps, the durations of and intervals between keystrokes can be calculated.

When a key is pressed, it creates a hardware interrupt to the processor and generates a time stamp, typically measured with microsecond precision. Using the time stamps, the durations of and intervals between keystrokes can be calculated.

Some pretty powerful open source tools and libraries that does the heavy lifting of capturing keystroke biometrics, create and train NN models. Current shot to crack biometric authentication is based on Keras library which itself is based on TensorFlow library open sourced by Google.

The learning is based on multiple positive sample provided during registering process. Several biometric models were then bench marked for their accuracy by computing their EER.

Keystroke biometrics is evaluating an attention-based neural network (ANN) model (back propagation) and comparing it's accuracy to other NN models that are used in keystroke biometrics.

- Sequence to sequence (s2s) involves mapping (encoding) an input sequence (characters, numbers, words, etc) to a predicted answer (output). Keystroke biometrics, leverages sequence to sequence (s2s) modeling, because the input sequence of keystroke metric features (DU, UD, and DD) can be encoded to produce an output sequence of timestamps.

- This keystroke s2s can be learned by a model and then be used to learn a user's keystroke behavior. To efficiently perform this type of analysis, one can leverage data and task parallelism to speed up the training process. It should be noted that the computing system should have sufficient memory to perform the s2s analysis on large datasets.

4.2 Algorithm for Iris Scan

Back Propagation Neural Network (BPNN) is a systematic method for training multi-layer artificial neural network. The basic structure of the BPNN includes one input layer, at least one hidden layer (single layer / multiple layers), followed by output layer. Neural network works by adjusting the weight values during training in order to reduce the error between the actual and desire output pattern. Load normalized Iris data set (contains feature vector values ranges from 0 to 1 for different subjects).Use this normalized data for training set and testing set by randomly drawing out the data for training and testing. Create an initial NN architecture consisting of three layers, an input, an output and a hidden layer. The number of nodes in the input layer is equal to dimension of the feature vector that characterizes the iris image information. Randomly initialize the nodes of the hidden layer. The output layer contains one node. Randomly initialize all connection weights within a certain range. Train the network on the training set by using Back Propagation algorithm until the error is minimum for a certain number of training epochs specified by the user. Present the test data to the trained network and evaluate the performance.

I. **Iris -** Iris is the most accurate biometric. Iris is the elastic, pigmented, connective tissue that controls the pupil. Iris images are taken by CASIA iris image database. The feature extraction is done by using wavelet transform. Data sets will be prepared using features obtained by the feature extraction technique. These obtained features are fed to the ANN for the classification.

II. **Iris Pre-processing -** In iris pre- processing, the iris is detected and extracted from an eye image and normalized. At first stage, the training of recognition system is carried out using Gray scale values of iris images [5]. Neural network is trained with all iris images. After training neural network performance validation is done.

III. **Segmentation -** The segmentation module detects the pupillary and limbus boundaries and identifies the regions where the eyelids and eyelashes interrupt the limbus boundaries contour. A good segmentation algorithm should involve two procedures, iris localization and noise reduction. The noise reduction process refers to localizing the iris from the noise (non-iris parts) in the image.

IV. **Normalization -** The normalization process is used to transform the iris texture from Cartesian to polar coordinates. The process, often called iris unwrapping yields a rectangular entity that is used for further processing. The variations in eye image due to optical size, position of pupil and the iris orientation change from person to person.

V. **Feature Extractor -** To provide accurate recognition of individuals, the most discriminating information present in an iris pattern must be extracted. The iris images thus obtained are then used for feature extraction. Where, Gabor filter is used to provide the optimal resolution in both the domains [12]. The information about time is lost and its hard to tell where a certain frequency occurs in Fourier Transform. Gabor function best analytical resolution in both domains. Thus feature encoding is implemented by breaking the two-dimensional normalized Iris pattern into one-dimensional wavelets and then these signals are convolved with one-dimensional Gabor wavelet.

VI. **Recognizer -** The coefficients of all the persons are saved in a single matrix. The single value decomposition is applied to these coefficients for comparison to find the best performance [2]. Thus a Neural network tool is used to calculate the best validation performance and plot a graph of mean square error V/s number of epochs.

4.3 Algorithm for Voice Recognition

Deep Learning has changed the game in speech recognition with the introduction of end-to-end models. These models take in audio, and directly output transcriptions. Two of the most popular end-to-end models are Deep Speech by Baidu, and Listen Attend Spell (LAS) by Google. Both Deep Speech and LAS, are recurrent neural network (RNN) based architectures with different approaches to modelling speech recognition. Deep Speech uses the Connectionist Temporal Classification (CTC) loss function to predict the speech transcript. LAS uses a sequence to sequence network architecture for its predictions. These models simplified speech recognition by taking advantage of the capacity of deep learning system to learn from large datasets. RNN has succeeded in improving speech recognition performance because of its ability to learn sequential patterns as seen in speech, language, or time-series data. RNNs have challenges in using traditional back propagation technique for training such models. This technique has difficulties in using memory to process portions of a sequence with larger degrees of separation. The problem is addressed with the development of long short- term memory (LSTM) networks that use special hidden units known as "gates" to retain memory over longer portions of a sequence.

I. **Speech -** Speech is the vocalized form of human interactions. In this step, the speech of the speaker is received in waveform. There are many software available which are used to record the speech of humans. The acoustic environment and transduction equipment may have great effect on the speech generated. It can have background noise or room reverberation along with the speech signal which is completely undesirable.

II. **Speech Pre-processing -** Speech pre-processing is intended to solve such problems. It plays an important role in eliminating the irrelevant sources of variation. It improves the accuracy of speech recognition. The speech pre-processing generally involves noise filtering, smoothing, end point detection, framing, windowing, reverberation cancelling and echo removing.

III. **Feature Extractor -** This block transforms the incoming sound into an internal representation such that it is possible to reconstruct the original signal from it. This stage can be modeled after the hearing organs, which first transduces the incoming air pressure waves into a fluid pressure wave and then converts them into a specific neuronal firing pattern. After the first stage, comes the one that analyzes the incoming information and classifies it into the corresponding language.

IV. **Recognizer -** Once the FE(Feature Extractor) block completes its work, its output is classified by the Recognizer module. It integrates the sequences into words. This module sees the world as if it where only composed of words and classifies each of the incoming trajectories into one word of a specific vocabulary.

5. CONCLUSIONS

In this paper, we propose a joint end-to- end model, which uses a deep neural network to generate feature extraction from biometrics given by user to authenticate while login user.

Physiological and behavioral traits can be stored as inputs that are converted into data and stored to unlock in future uses as well as create unique user profiles.

Introducing biometric authentication into the process adds in a road-block for fraudsters that only a real, authorized user can circumnavigate. Additionally, biometrics can only be provided by living, breathing people - at this point in time, a robot would have a hard-time passing an iris scan. For this purpose, the multitask features learning deep model mines rich information such as human attributes, iris scan, actions interactions, and information from a voice to produce password. This information is taken out through a CNN, which is fine-tuned for these specific tasks. This Biometric Authentication not only reduces the risk of forgetting user's passwords and PINs but also enables users to authenticate incredibly easy and quick through it. The abstract neural network (ANN) model is based on biometric attention which is easy to train and produce good results. Our experiments show that our models execute well on standard datasets. This representation will not only save processing time but will also save storage space.

REFERENCES

[1] Methodology for Iris Scanning through smartphones - https://ieeexplore.ieee.org/document/7881460

[2] Biometric Bit String Generation using smartphones microphones https://ieeexplore.ieee.org/document/8659483

[3] https://www.idexbiometrics.com/8-reasons-why-biometric-identification-is-more-than-just-fingerprints/

[4] Recent Advances and Applications of Keystroke Dynamics:

https://ieeexplore.ieee.org/document/9004312

[5] A 3D Iris Scanner from a Single Image Using Convolutional Neural Networks – https://ieeexplore.ieee.org/docume nt/9097841

[6] Iris Recognition : Comparing Visible- Light Lateral and Frontal Illumination to NIR Frontal Illumination - https://ieeexplore.ieee.org/docume nt/8659059

[7] https://www.researchgate.net/publication/294641837 _Keystroke_Biometric_Systems_for_User_Authentication