International Journal of Scientific & Engineering Research Volume 9, Issue 4, April-2018
ISSN 2229-5518

Comparative Study of Normalized Dynamic Feature and Immune Recognition System in Signature Verification using Artificial Intelligence

[1]AlthafKhan. A, [2]Mr.S.Vijayakumar

Abstract— In this competitive generation security is very important. As like handwritten signature verification is most widely used in any financial and documentation activity but this system is manual verify. So, a more robust system is required for verification through online and offline. In this article showing the comparative study of normalized feature and immune recognition system are implemented. It is for both offline and online. In artificial intelligence the signature verification has many methods. Signature verification from this comparative study showing the existing technique with digital tablet with digital pen and unique technique that support the artificial immune recognition system and their merits and demerits of these techniques.

Keywords— Artificial Immune Recognition System, Artificial Neural Network, Online signature, Dynamic features, Signature Verification.

1 INTRODUCTION

It took great deal of time for researcher to research into signature verification. Handwritten signature is the most used biometric for any financial activities, authorization of documents etc, this types of biometric are called as behavioral biometric. A biometric is the science which detects person on the basic of their biological or behavioral feature, it is related to behavioral properties of the human being.

An automated signature verification system can either be online or offline. In offline verification, the person sign on the paper that converted into signature image it is less precise but it has large practical application. Other approach online signature verification in which user sign on digital tablet using digital pen and the dynamic data has been captured in real time and saved into the database. In the technique of artificial immune recognition system are biological behavior ways like neural network. This system will protect from any virus, it will detect any foreign substance. This helped to develop system which could solve expert and intelligent system problem like fault and anomaly detection. To comprising the both system with dynamic feature and immune recognition, the technique showing the result the way of finding the genuine otherwise not. There three types of forgeries signature verification system.

1.1 Random Forgery

A random forgery, the person wants to forge the signature only knows about the name of the person to whom which he wants to forge the signature but does not know the exact signature.

1.2 Unskilled Forgery

An unskilled forgery is the person who wants to copy the exact signature are know the way how the exact signature will come after all does not able to reproduce exactly as like the original signature.

1.3 Skilled Forgery

A skilled forgery is the type the person wants to copy the signature knows very well about the way and different variation of genuine signature and the copy well match with the signature.

2 DYNAMIC FEATURE

There are two main phases of the signature verification system.

- Training Phase
- Testing Phase

2.1 Training Phase included the following steps

Take the Signatures of the persons on Wacom bamboo digital pad with pressure pen. Then extract the dynamic properties of the signature i.e., x, y coordinates of signatures and pressure on each pixels of the signatures at the time of signature is being made on tablet. Then extract the 11 different features of the signature from dynamic values of the signature as defined earlier. Then, make a database of the extracted features and train a neural network by back propagation technique using Levenberg-Marquardt (trainlm) training algorithm in MATLAB as shown in Fig.2.1.

- *[1]AlthafKhan. A, II-Year MCA, Priyadarshini Engineering College, Vaniyambadi, Email: althafkhan666@gmail.com*
- *[2]Mr.S.Vijayakumar, Associate Professor& HOD, MCA, Priyadarshini Engineering College, Vaniyambadi, Email: Vijayviswak@gmail.com*

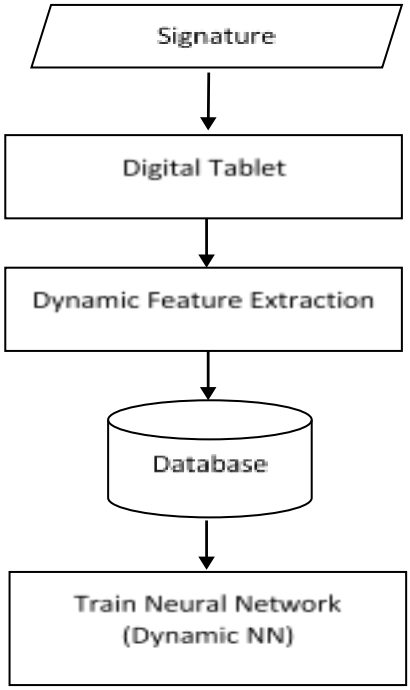

Fig2.1: Training Phase

2.2 Testing Phase included the following steps

Take all type of forge signature (one at a time) i.e., Random forge, Unskilled forge and Skilled forge on digital tablet and extract the same dynamic features that uses in Training phase. Then, test the neural network that train in training phase using the extracted features as shown in Fig. 2.2.

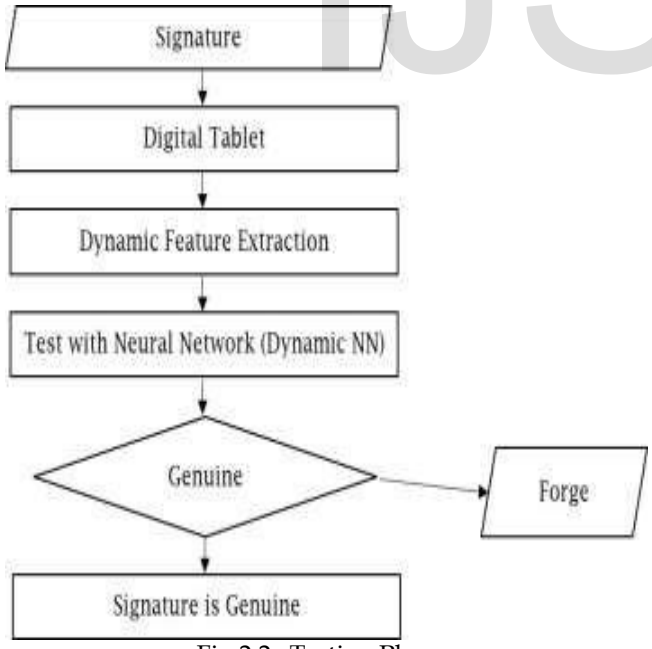

Fig 2.2: Testing Phase

All financial transactions for authorization of identity of human but still this authentication system is based on by comparing the signature with authorized signature manually. So, a system is required which is based on computer based classification. This system 10 signatures of 5 different persons are taken on digital tablet using digital pen and from that a database of x, y coordinate and pressure values at different points are extracted, from which 11 different specific feature set is calculated, which is used to train a neural network using MATLAB software and a digital tablet of WACOM is used called WACOM bamboo with pressure sensitive pen as shown in Fig. 3, For data acquisition a this tablet is interfaced with computer with the help of C# code and a GUI has been developed in C# language.

Fig 2.3: digital tablet for signature

2.3 Advantages

- Systematic signature verifications are one of the major advantages.
- Enrolment is intuitive and fast.
- Signature verification is independent of the native language user.
- Very high comparisons rate doesn't affect shape of the signature.
- Signature is stored in database system so it is more save and secure.
- Through the digital pen signature, it is easier to find whether the signature is forgery or original.
- A signature will process under training phase and testing phase after it store in database and train neural network.

2.4 Disadvantages

- For digital signature verification, account holder and employee need to spend money for buy software.
- Some people have palsies, while other do not have enough fine motor coordinate to write consistently.
- Where signature is store in database system is attack by the hacker.
- In immune recognition system, a unknown person may forgery to the signature through neural network.

3 Artificial Immune Reorganization System

An artificial immune recognition system, in field of artificial immune system(AIS) is concerned with abstracting the structure and function of the immune system to computational system and investigating the application of these system towards solving computational problems from mathematics, engineering, and information technology. It has various applications

like feature generation, pattern recognition, machine learning and data mining. AIRS are algorithm which mimic immune symbols or parameters like antibody antigen binding, affinity maturation, colonel selection process, resource completion and memory cell acquisition. Each training or test sample is antigen. Antibodies which constitute data of each class are called memory cells (MC) of the system. As B-cell in AIRS is called as artificial recognition Balls (ARB) these corresponds to feature vector of an antibody with its class label and resource number. When train then AIRS develops new antibodies (or MC) which describes the different classes of interest. As like, we will collect the scanned images of signature of different persons, basically we collect the 10 scanned images of individuals' actual signatures and their forged signatures. These images are stored in a database which we are going to use in training & testing of ANN and to use an interface with scanner for getting an image and These images are stored in a database. After pre-processing all signatures images from the database, features extraction will be used to extract various features of signature that can distinguish signatures of different persons. These are used for training and testing of neural network.

3.1 Neural Network

It is a fully connected network with three layers as shown in Fig. 4, Neural networks are highly reliable when trained using a large amount of data. They are used in applications where security is highly valued. For signature recognition and verification several steps must be performed. The capability to learn by adjusting its weights which connecting one neuron in one layer to other neuron in other layer comparing the result output this is called supervise learning we have to use an interface with scanner for getting an image and These images are stored in a database. After pre-processing all signatures images from the database, features extraction will be used to extract various features of signature such as stroke, moment invariants, GLCM, color dominant, histogram that can distinguish signatures of different persons.

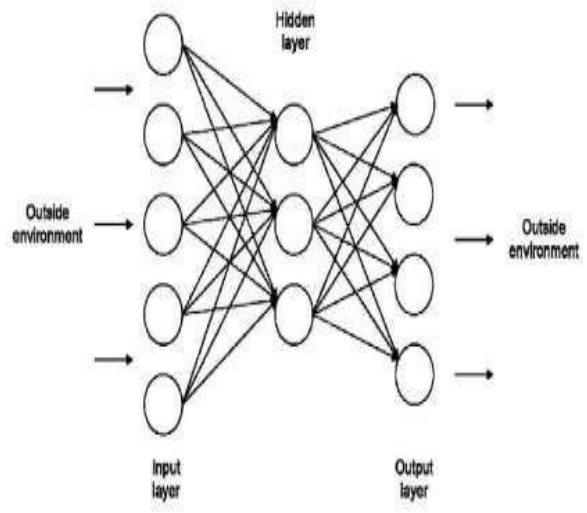

Fig 3.1: Neural Network

3.2 Advantages

- In this immune recognition system are difficult to do forgery work.
- It is simple
- It is efficient (if reasonable of signature)
- It will detect know attacks.
- Signature is stored in database system so it is more save and secure.
- It will know which attack at time of detection.
- A signature will be taken from database than it will be spatial resolution it.

3.3 Disadvantages

- A signature files must have kept up to date.
- A number of signatures may become large amount of data.
- Variation on known attack may not be detected.
- In immune recognition system, a unknown person may forgery to the signature through neural network.
- Signature verification will take more time.
- It is more cost to buy the software.

4 SUGGESTION

Bank has to deal with various documents to their client such as checks, draft, letter approval, transaction etc for all such a major things signature that are most important. We are suggesting in this articles that using a dynamic feature and immune recognition system a signature a store in the database. So, it is difficult of forgery and bank employee comfort with this. A digital signature at the digital pad is needed to identify their itself whether the signature is valid or invalid. In an immune recognition system will fetch the signature from database while at verification time the signature is converted into binary form and it will make image to as a sub image of the signature and through the sub image it will find the valid signature. A digital signature is important to detect forgery work. There are no possibilities of forgery to the signature it has a neural network to find easily with invalid signature.

5 CONCLUSION

This article is present a shorter introduction on Artificial intelligence of signature verification undertaken the comparison of dynamic feature and immune recognition system for verifying signature. As this is new technology for most people and research are still on deep research on this signature verification and I has implementing in major places like banks. Through the digital pen with coordinate x, y pressure values at different point will be extracting. It provides benefit that may improve our lives in such a way by increasing security and efficacy and reduce forgery works. Artificial immune recognition system is method which does the learning mechanism of the natural immune system. It separates the normal behavior in one class and abnormal behavior in another class. AIRS are suitable for detection purpose

like anomaly detection and fault detection than other classifiers in which training grants same processing for all the classes.

REFERENCES

1. Luan L. Lee, Toby Berger and ErezAviczer, "Reliable On-Line Human SignatureVerification Systems", IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 18, no. 6
2. G. Pirlo, V. Cuccovillo, M. Diaz-Cabrera, D. Impedovo, and P. Mignone, "Multidomain verification of dynamic signatures using local stability analysis", IEEE Transactions on Human-Machine Systems, vol. 45, no. 6.
3. Zhan EnqiGuo, JinxuZheng, Jianbin, Ma Chan and Wang Linjuan, "On-line Handwritten Signature Verification Based on Two Levels Back Propagation Neural Network", International Symposium on Intelligent UbiquitousComputing and Education.
4. VahabIranmanesh,harifahMumtazah Syed Ahmad, Wan Azizun Wan Adnan, Fahad Layth and Salman Yussof, "Online Signature Verification Using Neural Network and Pearson Correlation Features", IEEE Conference on Open Systems (ICOS), Sarawak, Malaysia.
5. Ahmed, S.K., Ramasamy, A.K, Khairuddin, A. and Omar, J., "Automatic online signature verification: A prototype using neural networks", IEEE Conference (TELCON 2009), Singapore
6. arzuki Khalid, HamamMokayed, RubiyanYusof and Osamu Ono, "Online Signature Verification with
7. Neural Networks Classifier and Fuzzy Inference", Third Asia International Conference on Modelling & Simulation, Bali, Indonesia
8. Artificial intelligence signature verification in immune recognition-WIKIPEDIA.