ISSN (Online): 2456-5717

International Journal of Advanced Research in Basic Engineering Sciences and Technology (IJARBEST)
Vol.3, Issue.4, April 2017

Digital Signature Authentication Using Artificial Neural Network

R.Preethi[1], A.R.Rishivarman[2]
Research Scholar, Mathematics, Theivanai Ammal College for Women, Villupuram, India[1].
Professor, Mathematics, Theivanai Ammal College for Women, Villupuram, India[2].

***Abstract* – In order to deal with security, Authentication plays an important role. Thwarting forgery and ensuring the confidentiality of Information in the field of Information Security is the need of the hour. This paper presents the signature recognition technique and discusses techniques of Signature Authentication by Back-propagation Algorithm of ANN .The purpose of this technique is to ensure that the rendered services are accessed only by a legitimate user, and not anyone else. By using this method it is possible to confirm or establish an individual's identity. This technique is suitable for various applications such as bank transactions, passports and so on, since it is augmented by modern mathematics followed by hardware and software implementation.**

***Keywords*- Artificial Neural Network, Authentication, cryptography, Digital signature, Hash function.**

I. INTRODUCTION

Handwritten signature is one of the most widely accepted personal attributes for identity verification of the person. The written signature is regarded as the primary means of identifying the signer of a written document based on the implicit assumption that a person's normal signature changes slowly and is very difficult to erase, alter or forge without detection. The handwritten signature is one of the ways to authorize transactions and authenticate the human identity compared with other electronic identification methods such as fingerprints scanning and retinal vascular pattern screening. It is easier for people to migrate from using the popular pen-and-paper signature to one where the handwritten signature is captured and verified electronically.

There are two main streams in the signature recognition task. First approach requires finding information and can recognize signature as the output of the system and it is seen that in a certain time interval, it is necessary to make the signature. This system models the signing person and other approach is to take a signature as a static two-dimensional image which does

not contain any time-related information [1].in short, signature recognition can be divided into two groups. Online and offline.

The online signature recognition, where signatures are acquired during the writing process with a special instrument, such as pen tablet. In fact, there is always dynamic information available in case of online signature recognition, such as velocity, acceleration and pen pressure. So far there have been many widely employed methods developed for online signature recognition for example, Artificial Neural Networks (ANN)[2,3] dynamic time warping (DTW)[4,5], the hidden Markov models (HMM)[6,7].

The off-line recognition just deals with signature images acquired by a scanner or a digital camera. In general, offline signature recognition& verification is a challenging problem. Unlike the on-line signature, where dynamic aspects of the signing action are captured directly as the handwriting trajectory, the dynamic information contained in off-line signature is highly degraded. Handwriting features, such as the handwriting order, writing-speed variation, and skillfulness, need to be recovered from the grey-level pixels.

In the last few decades, many approaches have been developed in the pattern recognition area, which approached the offline signature verification problem. Justine,[8] propose an off-line signature verification system using Hidden Markov Model . Zhang, Fu and Yan [9] proposed handwritten signature verification system based on Neural 'Gas' based Vector Quantization. Velez, Sanchez and Moreno [10] propose a robust off-line signature verification system using compression networks and positional cuttings. [11, 12, 13]

The signature recognition & verification system is broadly divided into three subparts

- Preprocessing,
- Feature extraction,
- Recognition & Verification.

II. HASH FUNCTIONS

A hash function is a quick function to compute but whose inverse image is the class of computationally difficult problems (NP class). It transforms a message of arbitrary length into a hash code or message authentication of fixed size, typically 160 bits currently. For safety reasons

there is a tendency to increase the size of the fingerprint[14]. The scheme for calculating a signature using a hash function is as follows:

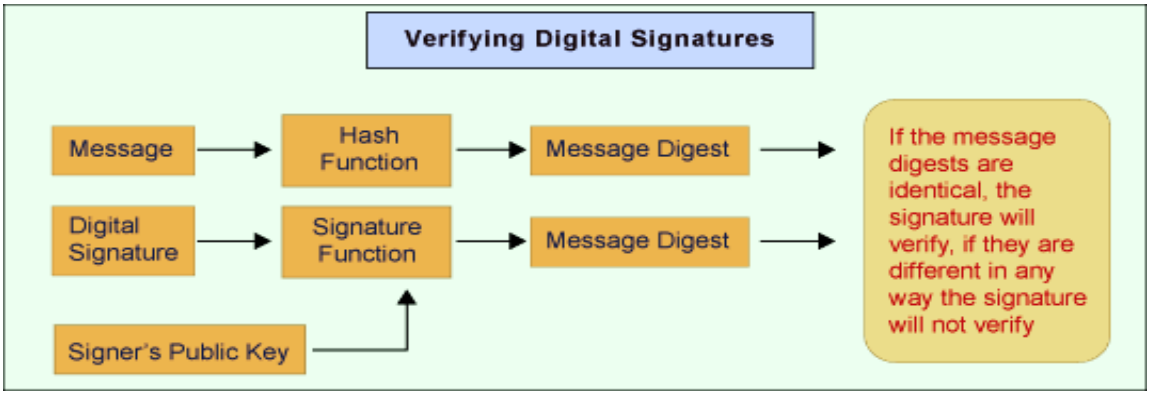

Fig. 1 Operating Principle of Hash Function

The wide use of computer network and wireless devices of digital communication results in a greater need for the protection of transmitted information by using Cryptography. Verifying the integrity and authenticity of information is a prime necessity in computer systems and networks. A one-way hash function is an important element of cryptography. A hash function encodes a plaintext with variable length into a hash value with fixed length, and it is often used in data signature or data authentication. As is known, a secure hash function should satisfy several requirements: one-way, secure against birthday attack and secure against meet-in-the-middle attack.

The one-way property makes it impractical to find a plaintext with the required hash value. The hash function should be secure against birthday attack, which makes it difficult to find two plaintexts with the same hash value. It should also be secure against meet-in-the middle attack, which makes it difficult to find a plaintext whose hash value is same as one of the given plaintexts. Recently, it was reported that widely used Hash functions such as MD5 or SHA-1 are no longer secure. Thus, new Hash function should be studied in order to meet practical applications. Nonlinearity is one of the inherent properties of the neural network, therefore, in this paper Artificial Neural Network is introduced as an alternative to the hash algorithm like MD5 are traditionally used in cryptographic applications

.

III. ARTIFICIAL NEURAL NETWORK

The ANN is inspired by biological neural system. It is composed of several interconnected elements to solve a collection of varied problems. The brain is composed of billions of neurons and trillions of connections between them. The nerve impulse travels through the dendrites and axons, and then treated in the neurons through synapses [15].

This results in the field of ANN in several interconnected elements or belonging to one of the three marks neurons, input, output or hidden. Neurons belonging to layer n are considered an automatic threshold. In addition, to be activated, it must receive a signal above this threshold, the output of the neuron after taking into account the weight parameters, supplying all the elements belonging to the layer $n + 1$. As biological neural system, neural networks have the ability to learn, which makes them useful. The ANN are units of troubleshooting, capable of handling fuzzy information in parallel and come out with one or more results representing the postulated solution. The basic unit of a neural network is a non-linear combinational function called artificial neurons. An artificial neuron represents a computer simulation of a biological neuron human brain. Each artificial neuron is characterized by an information vector which is present at the input of the neuron and a non-linear mathematical operator capable of calculating an output on this vector. The following figure shows an artificial neuron.

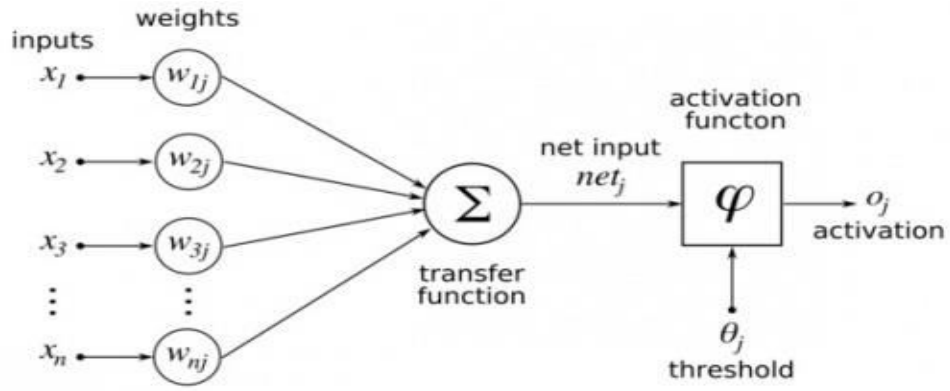

Fig. 2 Artificial Neural

The synapses are W_{ij} (weights) of the J neural; they are real numbers between 0 and1. The function is a summation of combinations between active synapses associated with the same neuron. The activation function is a non-linear operator to return a true value or rounded in the range[0 1]. In our case we use the sigmoid function

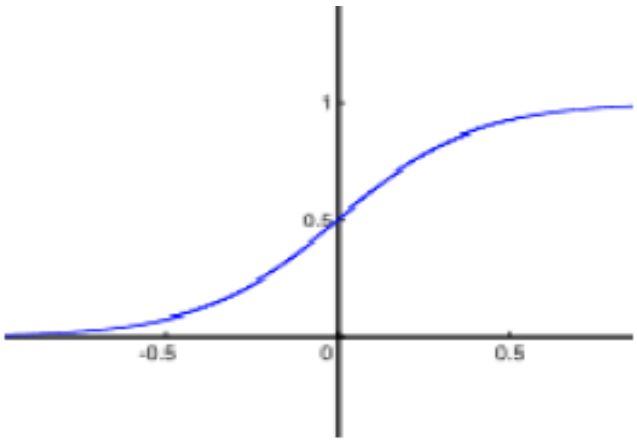

Fig. 3 Sigmoid Function

An ANN is composed by a collection of artificial neurons interconnected among them to form a neuronal system able to learn and to understand the mechanisms. Each ANN is characterized by its specific architecture; this architecture is denoted by the number of neurons of the input layer, the number of hidden layers, the number of neurons in each hidden layer and the neurons number in the output layer. A layer of neurons in a neural network is a group of artificial neurons, with the same level of importance, as is shown in the following figure

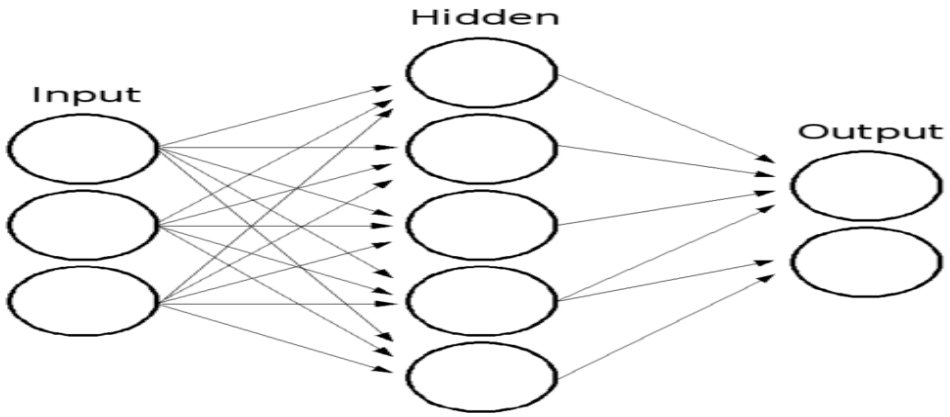

Fig. 4 Multilayer feed forward network

The operating principle of ANN is similar to the human brain; first, it must necessarily pass on the learning phase to record knowledge in the memory of the ANN. The storage of knowledge is the principle of reputation and compensation to a collection of data that forms the basis of learning. We have several algorithms that can teach an ANN as back propagation. The back propagation is a method of calculating the weight for network supervised learning is to minimize

the squared error output. It involves correcting errors according to the importance of the elements involved in fact the realization of these errors: the synaptic weights that help to generate a significant error will be changed more significantly than the weights that led to a marginal error. In the neural network, weights are, first, initialized with random values. It then considers a set of data that will be used for learning.

IV. SIGNATURE AUTHENTICATION USING ANN

The transfer function of a neuron in a neural network is the main processing function. It is utilized for limiting the amplitude of the output of a neuron. Also activation function is referred to as a squashing function as it squashes (limits) the permissible amplitude range of the output signal to some finite values.

There are many types of activation functions available to use in MATLAB, Particularly the popular sigmoid function. In this work, it uses Neural Network Toolbox for signature Authentication.

When the application launches, it waits for the user to determine whether he wishes to train or verify a set of signatures. At the training stage, based on the back propagation neural network algorithm, the user gives five different signatures as input, of which the real input to the network are the individual pixels of the images. When input is confirmed and accepted, it passes through the back propagation neural network algorithm to generate an output which contains the network data of the trained images. The back propagation artificial neural network simply calculates the gradient of error of the network regarding the networks modifiable weights. In this paper it is implemented a multi-layer neural network with backpropagation, specifically a three-layer neural network, which consists of:

- ***Input layer*** – It consists of all the input data that has been supplied to the network.
- ***Hidden layer*** – It consists of all the passive inputs that have been supplied by the preceding layers.
- ***Output layers*** – It contains the outputs of the neural network.

V. ALGORITHM & FLOWCHART

This section offers algorithm for the offline signature verification system in which artificial neural network is used to confirm the genuineness of signature.

- ✓ **Input** = Signature Image
- ✓ **Output** = Conformation from system whether signature is genuine or counterfeit.

A. Algorithm

Step 1: Acquire signature image from the database

Step 2: Create the Neural network index

Step 3: Select any one signature from the given five samples.

Step 4: Retrieving.

Step 5: Normalized the feature vector for further processing.

Step 6: Apply this normalized feature vector to the neural network for training purpose.

Step 7: Perform pattern matching with the test data set present in the hidden layer of neural network

Step 8: Do the classification

Step 9: Using outcome produced by the output layer of the neural network announce signature as True or False.

B. Flowchart

This diagram shows how the whole system works till the result whether signature is genuine or counterfeit.

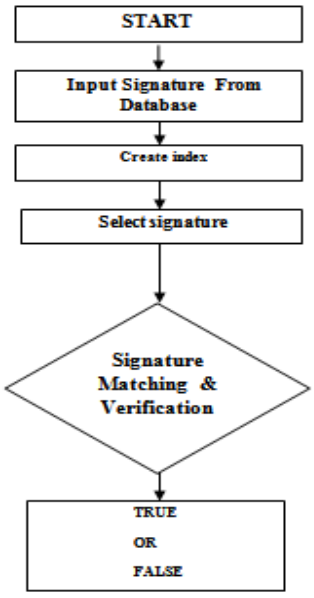

Fig 5: Flow diagram for signature recognition& verification system

ISSN (Online): 2456-5717

International Journal of Advanced Research in Basic Engineering Sciences and Technology (IJARBEST)
Vol.3, Issue.4, April 2017

VI. TRAINING AND TESTING

The recognition phase consists of two parts, training and testing respectively which is accomplished by back propagation neural network. Under normal (correct) operation of the back propagation neural network, only one output is expected to take a value of "1" indicating the recognition of a signature represented by that particular output. The other output values must remain zero. The output layer used a logic decoder which mapped neuron outputs between 0.5 – 1 to a binary value of1. If the real value of an output is less than0.5, it is represented by a "0" value. The back propagation neural network program recognized all of the 5 signatures correctly. This result translates with 100% recognition rate.

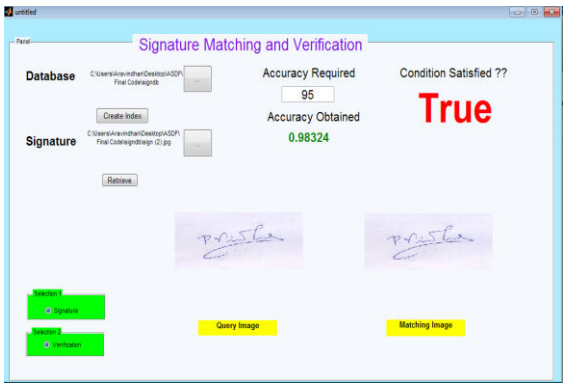

Fig. 6 Signature 1

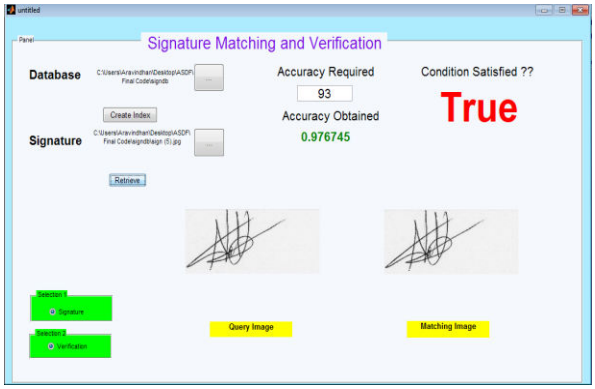

Fig. 7 Signature 2

Fig. 8 Signature 3

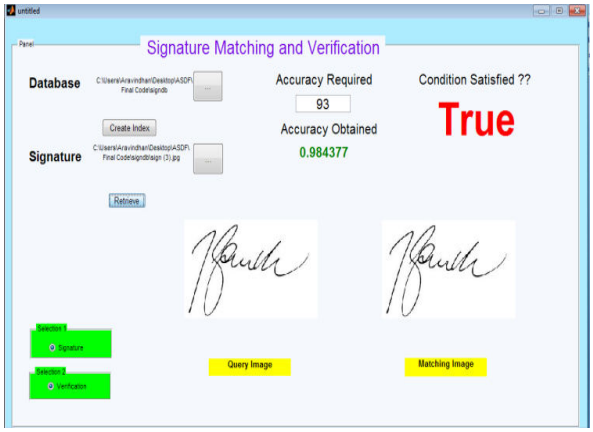

Fig. 9 Signature 4

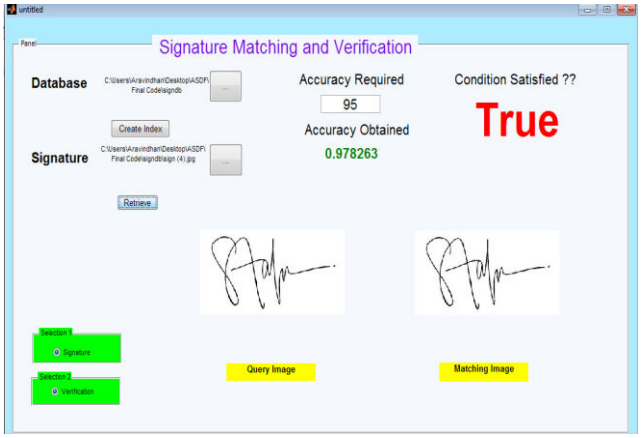

Fig. 10 Signature

VII. CONCLUSION

This paper presents neural network based authentication and verification of individual Digital signature. The use of ANN as hash functions for the digital signature images offer a new approach to protect the integrity of images. This paper provides in detecting the exact personality with cent percent accuracy of verifying signatures. The technique in this discussion intends to mitigate risk of forgery in business and other sensitive transactions. Comparatively, the achievement of authenticity is valid.

ACKNOWLEDGEMENT

The authors are thankful to referees for their valuable comments and suggestions for improving this paper.

REFERENCES

[1] Pacut, A Czajka, "Recognition of Human Signatures", pp. 1560-1564, 2001.

[2] Ronny Martens, Luc Claesen, "On- Line Signature Verification by Dynamic Time-Warping", IEEE Proceedings of ICPR'96 1996.

[3] Quen-Zong Wu, I-Chang Jou, and Suh-Yin Lee, "On-Line Signature Verification Using LPC Cepstrumand Neural Networks", IEEE Transactions on Systems, Man, and Cybernetics—Part B: Cybernetics, 27(1):148-153, 1997.

[4] Pave1 Mautner, OndrejRohlik, Vaclav Matousek, JuergenKempp, "Signature Verification Using ART-2 Neural Network", Proceedings of the 9th International Conference on Neural information Processing (ICONIP'OZ) ,2: 636-639, 2002.

[5] A. Jain, F. Griess, S. Connell, "On-line signature Verification", Pattern Recognition, Vol. 35, No. 12, 2002 .pp.463-465

[6] W. Nelson, W. Turin, T. Hastie, "Statistical methods for on-line signature verification", International Journal of Pattern Recognition and Artificial Intellingence, 8, 1994.pp.356-360.

[7] R. Kashi, J. Hu, W.L. Nelson, W.Turin, "A hidden markov model approch to online handwritten signature verification", International Journal on Document Analysis and Recognition, Vol. 1, No.1, 1998.pp.568-570.

[8] E. J. R. Justino, F. Bortolozzi and R. Sabourin,(2001) "Offline Signature Verification Using HMM for Random, Simple and Skilled Forgeries", ICDAR 2001, International Conference on Document Analysis and Recognition, vol. 1, pp. 105--110.

[9] Zhang, M. Fu and H. Yan (1998), "Handwritten Signature Verification based on Neural 'Gas' Based Vector Quantization", IEEE International Joint Conference on Neural Net-works, pp. 1862-186

[10] J. F. Vélez, Á. Sánchez, and A. B. Moreno (2003) , "Robust Off-Line Signature Verification Using Compression Networks And Positional Cuttings", Proc. 2003 IEEE Workshop on Neural Networks for Signal Processing, vol. 1, pp. 627-636.

[11] Q. Yingyong, B. R. Hunt, "Signature Verification Using Global and Grid Features", Pattern Recognition, vol. 22, no.12, Great Britain (1994), 1621--1629.

[12] Drouhard, J.P., R. Sabourin, and M. Godbout, "A neural network approach to off-line signature verification using directional PDF", Pattern Recognition, vol. 29, no. 3, (1996), 415-424.

[13] G. Rigoll, A. Kosmala, "A Systematic Comparison Between On-Line and Off-Line Methods for Signature Verification with Hidden Markov Models", 14th International Conference on Pattern Recognition - vol. II, Australia (1998), 1755.

[14] William Stallings. Cryptography and Network Security: Principles and Practice.(5th Edition), Prentice Hall, 2010.

[15] Zhang Hong. A Preliminary Study on Artificial Neural Network, IEEE,PP 336-338,2011.

AUTHOR'S BIOGRAPHY

Ms.R.Preethi, Is presently a Research scholar in Mathematics, Theivanai Ammal College for women, Villupuram. She completed her Post Graduate in Mathematics from Theivanai Ammal College for women, Villupuram and did her Under Graduate in Mathematics from Seethalakshmi Ramaswami College, Trichy.

Dr. A. R. Rishivarman, is presently a Professor of Mathematics in Theivanai Ammal College for women, Villupuram. He has been teaching Mathematics to students of B.E, M.E., M.Sc., and M.Phil. For past 16 years. His Current Area of interest include Number Theory, Cryptography, and Mechanics.