IMPRESSION OF DIGITAL SIGNATURE WITH NEURAL NETWORK

[1]Dr. Aruna J. Chamatkar, [2]Prof. Sachin Y. Zade & [3]Dr. Pradeep K .Butey

[1]Associate Prof., [2]Assistant Prof & [3]HOD, Department of Computer Science

[1]MCA Department, [2]MCA Department, [3]Department of Computer Science

[1]aruna.ayush1007@gmail.com

[1,2,3]Kamla Nehru Mahavidyalaya, Nagpur,Maharashtra, India

Abstract : Signature plays an important role in authentication. Identification and verification of hard written signature from images is very difficult. As even human eye does not have that much visual ability to identify every detail of the in handwritten. Signature changes every time so it is difficult for humans to identify the original and fake ones. Digital signatures are most widely used in various fields of documentation activities for authorization of identity of any human, we can consider that handwritten signature verification system are mainly based on manual verification, in which a person looks and compare the given signature with the test signature, so a better system is required which can be computer based classification. The use of an advanced digital signature as proof of authenticity and integrity for electronic records. So in this paper we mainly focus on, how neural network uses the refined is digital configured replica of human brain, we can identify the fake done in signature with higher accuracy.

Index Terms: PKI, Neural Network, authentication, and security.

I. INTRODUCTION

A digital signature is a mathematical technique used to validate the authenticity and integrity of a message, software or digital document. It's the digital equivalent of a handwritten signature or stamped seal, but it offers far more inherent security. A digital signature is intended to solve the problem of tampering and impersonation in digital communications.

Digital signatures can provide evidence of origin, identity and status of electronic documents, transactions or digital messages. Signers can also use them to acknowledge informed consent. Security is the main benefit of digital signatures. Security capabilities embedded in digital signatures ensure a document is not altered and signatures are legitimate.

Digital signatures are not to be confused with digital certificates. A digital certificate is an electronic document that contains the digital signature of the issuing certify authority. It binds together a public key with an identity and can be used to verify that a public key belongs to a particular person or entity. Most modern email programs support the use of digital signatures and digital certificates, making it easy to sign any outgoing emails and validate digitally signed incoming messages. Digital signatures are also used extensively to provide proof of authenticity, data integrity and nonrepudiation of communications and transactions conducted over the internet. While authenticated digital signatures provide cryptographic proof a document was signed by the stated entity and the document has not been altered, not all e-signatures provide the same guarantees.

It would be a better option to verify the signatures using this model rather than visual recognition through human eye which have a high chances of making a mistakes. So In this paper we study the how neural network useful in verification of digital signature.

II. WORKING OF DIGITAL SIGNATURE

Digital signatures are the public-key primitives of message authentication. In the physical world, it is common to use handwritten signatures on handwritten or typed messages. They are used to bind signatory to the message. Similarly, a digital signature is a technique that binds a person to the digital data. This binding can be independently verified by receiver as well as any third party. It is a cryptographic value that is calculated from the data and a secret key known only by the signer.

Digital signatures are based on public key cryptography, also known as asymmetric cryptography. Using a public key algorithm, such as RSA (Rivest-Shamir-Adleman), two keys are generated, creating a mathematically linked pair of keys, one private and one public.

Digital signatures work through public key cryptography's two mutually authenticating cryptographic keys. The individual who creates the digital signature uses a private key to encrypt signature-related data, while the only way to decrypt that data is with the signer's public key. If the recipient can't open the document with the signer's public key, that's a sign there's a problem with the document or the signature. This is how digital signatures are authenticated.

A. MODEL OF DIGITAL SIGNATURE

In real world, the receiver of message needs assurance that the message belongs to the sender and he should not be able to repudiate the origination of that message. This requirement is very crucial in business applications, since likelihood of a dispute over exchanged data is very high. The model of digital signature scheme is depicted in the following illustration

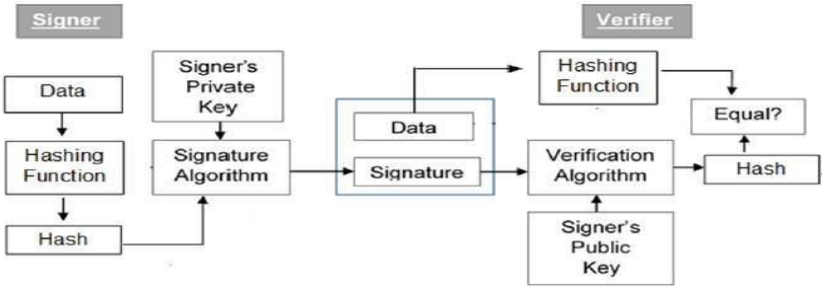

Fig. 1: Model of Digital Signature

- Each person adopting this scheme has a public-private key pair.
- Generally, the key pairs used for encryption/decryption and signing/verifying are different. The private key used for signing is referred to as the signature key and the public key as the verification key.
- Signer feeds data to the hash function and generates hash of data.
- Hash value and signature key are then fed to the signature algorithm which produces the digital signature on given hash. Signature is appended to the data and then both are sent to the verifier.
- Verifier feeds the digital signature and the verification key into the verification algorithm. The verification algorithm gives some value as output.
- Verifier also runs same hash function on received data to generate hash value.
- For verification, this hash value and output of verification algorithm are compared. Based on the comparison result, verifier decides whether the digital signature is valid.
- Since digital signature is created by 'private' key of signer and no one else can have this key; the signer cannot repudiate signing the data in future.

B. IMPORTANCE OF DIGITAL SIGNATURE

The digital signature using public key cryptography is considered as very important and useful tool to achieve information security. Apart from ability to provide non-repudiation of message, the digital signature also provides message authentication and data integrity.

- **Message authentication** − When the verifier validates the digital signature using public key of a sender, it is assured that signature has been created only by sender who possess the corresponding secret private key and no one else.
- **Data Integrity** − In case an attacker has access to the data and modifies it, the digital signature verification at receiver end fails. The hash of modified data and the output provided by the verification algorithm will not match. Hence, receiver can safely deny the message assuming that data integrity has been breached.
- **Non-repudiation** − Since it is assumed that only the signer has the knowledge of the signature key, he can only create unique signature on a given data. Thus the receiver can present data and the digital signature to a third party as evidence if any dispute arises in the future.

C. ENCRYPTION WITH DIGITAL SIGNATURE

In many digital communications, it is desirable to exchange encrypted messages than plaintext to achieve confidentiality.

In public key encryption scheme, a public (encryption) key of sender is available in open domain, and hence anyone can spoof his identity and send any encrypted message to the receiver.

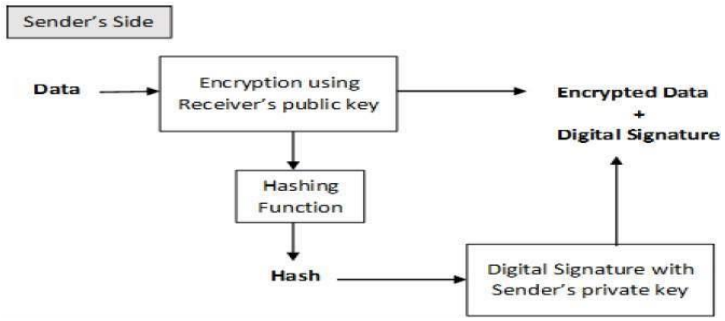

Fig. 2: Encryption with Digital Signature

The receiver after receiving the encrypted data and signature on it first verifies the signature using sender's public key. After ensuring the validity of the signature, he then retrieves the data through decryption using his private key. The most distinct feature of Public Key Infrastructure (PKI) is that it uses a pair of keys to achieve the underlying security service. The key pair comprises of private key and public key. Since the public keys are in open domain, they are likely to be abused. It is, thus, necessary to establish and maintain some kind of trusted infrastructure to manage these keys.

D. DIGITAL CERTIFICATE

A digital certificate does the same basic thing in the electronic world, but with one difference. Digital Certificates are not only issued to people but they can be issued to computers, software packages or anything else that need to prove the identity in the electronic world. The process of obtaining Digital Certificate by a person/entity is depicted in the following illustration.

Fig. 3: Generating Digital Certificate

- Digital certificates are based on the ITU standard X.509 which defines a standard certificate format for public key certificates and certification validation. Hence digital certificates are sometimes also referred to as X.509 certificates.
- CA digitally signs this entire information and includes digital signature in the certificate.
- Anyone who needs the assurance about the public key and associated information of client, he carries out the signature validation process using CA's public key. Successful validation assures that the public key given in the certificate belongs to the person whose details are given in the certificate.

III. NEURAL NETWORK

Artificial neural network models are a subpart of the machine learning models which are motivated by the functioning of the brain. A system which does computing and is combines with basic, and highly coincidental processing elements which use the data to get a highly relevant and faster response from the inputs taken Neural networks generally work like the neurons of the brain and the connected neurons will work in a network process to collect and process the data for providing the necessary output. There will be an input layer to the system which consists of all the patterns in which the system should process and also the necessary inputs and it communicates with the hidden layer as shown in the below figure and the hidden layers use the patterns and inputs by the input layer and are used to find out a relevant function for the task to be performed and then they communicate with the output layers to display the final output.

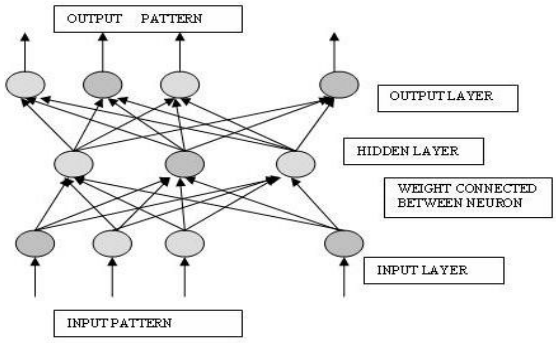

Fig. 4 : Basic structure of Neural Network

IV. DIGITAL SIGNATURE VERIFICATION USING NEURAL NETWORK

Signatures can be viewed as an image and recognized using image processing. Sample QR code Connected components labeling used in and the similarity between the features was calculated by the Manhattan distance method.

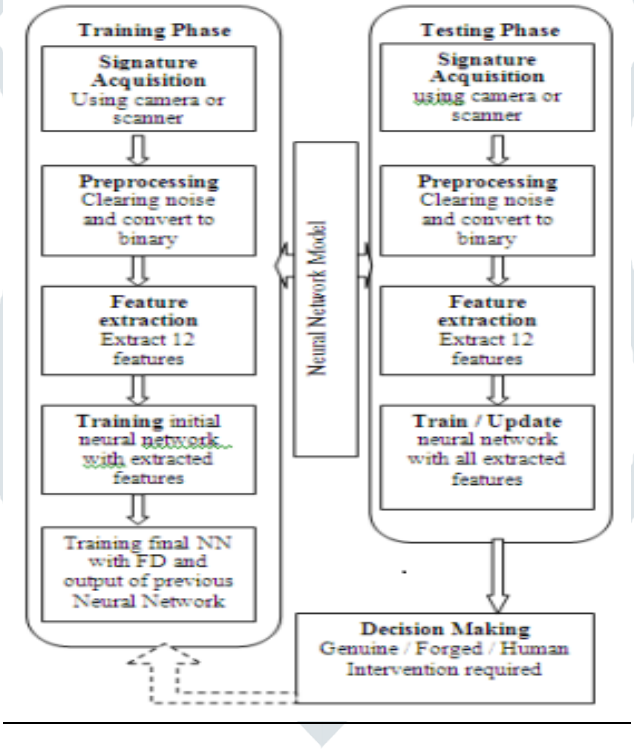

Fig. 5 : Process of verification Model

The features extracted are fed to natural network as inputs. Before that the networks are trained with data sets.

Each neural network has a corresponding user to it. So a user has two neural networks one with feed forward mechanism and the other with feedback mechanism. The user's features are given as input to both the neural networks and the output is recorded.

The entire system is divided into training and testing phases. The decision making stage is where the human intervention is needed if the neural network shows abnormal results. The update stage has the facility to change or update the signature of a person with proper authorization. That all represented in step by step process in verification model.

V. CONCLUSION

Security capabilities embedded in digital signatures ensure a document is not altered and signatures are legitimate. To avoid fake and ensure the confidentiality of Information in the field of Information Technology we need Security. In this paper we discuss about a technology of signature authentication by using neural network. It is a new approach in the field of signature authentication. In this paper an online signature verification system is proposed which is based on neural network based classification.

VI. ACKNOWLEDGEMENTS

First author would like to acknowledge Dr. P. K. Butey for their cooperation and useful suggestion to research work.

REFERENCES

[1] Digital signatures and electronic records by F. BOUDREZ

[2]Babita P, "Online Signature Recognition Using Neural Network" Journal of Electrical & Electronic Systems 2015.

[3] Gopichand G, Shailaja G, VenkataVinod Kumar, T.Samatha, "Digital Signature verification Using Artificial Neural Networks" International Journal of Recent Technology and engineering(IJRTE) Volume-7 Issue-5S2, January 2019.

[4] Chamatkar et al." Implementation of Different Data Mining Algorithms with Neural Network" IEEE, International conference on International Conference on (ICCUBEA), Pune Feb. 2015

[5] AlisheiKolmatov, BerrinYainkoglu, "Identity authentication using improved online signature verification method, Pattern Recognition letters", volume 26 ,Issue 15, November 2005,pp 2400-2408.

[6] Cemil Oz, "Signature Recognition and Verification with Artificial Neural Network Using Moment Invariant Method" International Symposium on Neural Networks ISSN 2005.

[7] Ashok Kumar and S. Dhandapani, "A Bank Cheque Signature Verification System using FFBP Neural Network

Architecture and Feature Extraction based on GLCM", IJETTCS, vol. 3, no. 3, May – June 2015.

[8] Chalechale, G. Naghdy, P. Pramaratne & Mertins, "Document image analysis and verification using cursive signature",

Proc. IEEE International Conference on Multimedia and Expo(ICME '04), pp. 27-30, June 2004.

[9]H.H. Wai and S.L. Aung, "Feature extraction for offline signature verification system", *IJCCER*, vol. 1, no. 3, pp. 84-87, 2013.

[10] Oladele, K.S.Adewole and A.O.Oyelami, "Forged Signature Detection using Artificial Neural Network", African

journal of Computing and ICT, vol. 7, no.3, 2014.

[11] Sascha Schimke, Claus Vielhauer, Jana Dittmann,"Using Adapted Levenshtein Distance For On- Line

Signature Authentication", 17th International Conference On Pattern Recognition (ICPR'04), Vol.2, 2004, pp.931-934.

[12] Impedovo and G. Pirlo, "Automatic signature verification: the state of the art", *Systems Man and Cybernetics Part C: Applications and Reviews IEEE Transactions on*, vol. 38, no. 5, pp. 609-635, 2008.

[13] Chamatkar and Butey ," Data mining classification methods and different Techniques "International Journal of Computer Application ISSN: 2250-1797 www.rspubliction.com, Issue 4, Volume 4 (July-August 2014**)**

[14]S. Yin, A. Jin, Y. Han, and B. Yan, "Image-based handwritten signature verification using hybrid methods of discrete Radon transform , principal component analysis and probabilistic neural network," Appl. Soft Comput. J.,vol. 40, pp. 274–282, 2016.