Simulating Manual Signature using Elman Back Propagation Model to Create Pseudo Digital Signature

Ekta Narwal, Sumeet Gill

Abstract: Manual Signatures are used in authentication worldwide. But they are still not used in VANETs and in ad hoc networks for security. In our research we try to use manual signature in place of Digital Signatures for the security of message and stimulated the same by pattern recalling mechanism of Artificial Neural Network using Elman Back Propagation Algorithm to create pseudo digital signature. These pseudo digital signatures are now used as the identity of message sender in communication. We also maintained the speed of manual signature recognition and verification to stop the delay in identification of the sender.

Keywords: VANETs, Elman Back Propagation Model, Vehicle Privacy, Artificial Neural Network.

I. INTRODUCTION

As the Internet of Things (IoTs) growing rapidly the interest of the society is also growing in the field of Intelligent Transportation System (ITS).[1] VANET is the main component of the ITS and it is the most talk research area in the traffic application now days. In VANETs the security of data and messages which are save on vehicle and transmit during the communication, is the most important concern and all these things depend on the broadcasting channels. But these wireless channels on road are very much prone to data leakage, intrusion and attacks by third parties.[2] There is a great need to construct a trust worthy platform for information and message security for VANETs. Existing technologies mostly focus on the use of techniques which needed third party as an authentication authority and this can also create threat to personal data of the vehicle driver and users. End to End authentication is also not possible in VANETs due to the high speed of vehicles, so the traditional security schemes cannot be applied on vehicle. Thus there is need of some new approaches for vehicular privacy.[1] In this paper we propose a mechanism that is based on use of driver biometric data in form of manual signature to verify the identity of sender whenever a message is sent by him over wireless channel. [3]

II. WHY MANUAL SIGNATURES

Many biometric approaches are widely used in the security of messages in VANETs but in our research we focus on using manual signature for identity verification of sender because of various important features of manual signatures. They are as follows:[2]

- Manual Signatures are minimally intrusive in comparison to other biometric approaches.
- We can change or modify manual signature without any certification authority. So many variations can be possible in manual signatures.[4]
- We can create public or private keys using manual signature, which provides a grid to the users. They can then create pseudo code using that grids and these images can be used to create keys or digital signatures.[5]
- In manual signatures we don’t need a third party certification to verify the signature.

III. EXPERIMENT DESIGN

This section discussed about the setup to convert the manual signatures into pseudo digital signature and then simulate them for verification using Elman Back Propagation Model of Artificial Neural Network [6], [7]. The simulation process is done by using Neural Network Tool Box of MATLAB. The driver produces manual signature on a piece of paper and then these manual signature converted in soft form two ways. First is just clicking the picture and saving that on a particular folder in the vehicle’s computational device. Second by using Image Acquiring Tool Box this application uses device camera for live capturing. The images captured through this mechanism are also stored in the particular place in the memory system. These images are now converted into some new format by applying various morphological techniques. The formatted images are unrecognizable and will be used as pseudo digital signature to verify the message sender identity in VANETs. After that, network trained by using Elman Back Propagation Model of Artificial Neural Network so that verification process did not take much time.

The system learnt the pseudo digital signatures and verifies them just in no time.[8]

Revised Manuscript Received on December 30, 2019.
***** Correspondence Author

Ekta Narwal*, Department of Mathematics, Maharshi Dayanad University,Rohtak. India. Email: ekta_narwal@yahoo.com

Sumeet Gill, Department of Mathematics, Maharshi Dayanad University,Rohtak. India. Email: drsumeetgill@gmail.com

The flowchart of the complete process is given in Figure-1.We used four manual signatures during our research displayed in Figure-2. All these signatures are converted into pseudo digital signatures shown in Figure-3. Table I shows the parameters used in our experiment during training.

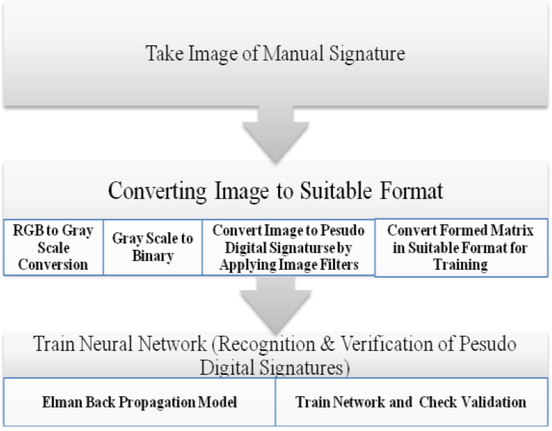
Take Image of Manual Signature
Converting Image to Suitable Format
RGB to Gray Scale Conversion
Gray Scale to Binary
Convert Image to Pesudo Digital Signatures by Applying Image Filters
Convert Formed Matrix in Suitable Format for Training
Train Neural Network (Recognition & Verification of Pesudo Digital Signatures)
Elman Back Propagation Model
Train Network and Check Validation

Figure 1 Simulation of Manual Signature

PARAMETER	VALUE			
Neurons in Input Layer	100			
Number of Hidden Layers	2			
Neurons in Hidden Layer	20	30	40	50
Neurons in Hidden Layer	100			
Training Model	Elman Back Propagation			
Data Division	Random			
Training Function	Traingdx			
Performance	Mean Square Error			
Minimum Gradient	1e-05			
Maximum Number of Epochs	1000			
Maximum Fail (Validation of Training)	06			
Time Delay	Between 0 and 1			

Table I- Parameters for the Network

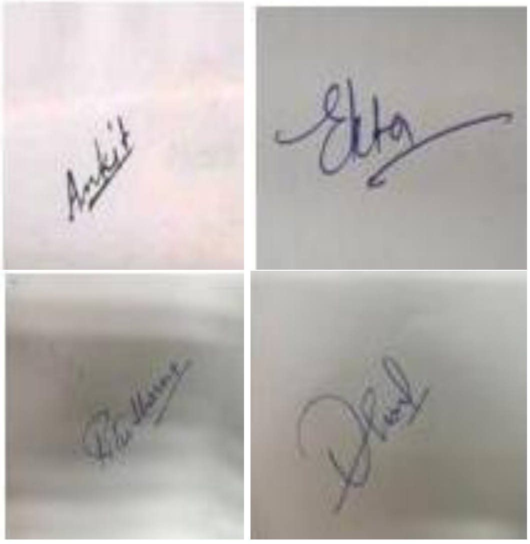

Figure 2 Original Images after Cropping (Size 100X 100) Used for Training

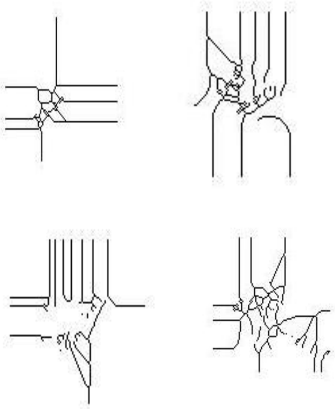

Figure 3- Morphed Images prepared to be used as Pseudo Digital Signature

All pseudo digital signatures are then converted into 100X100 matrices to feed them in the Neural Network Tool Box. All the values in the matrix are in binary form. Input and the target of the network are same. During first training 20 neurons, in second 30 neurons, in third 40 neurons and in forth training 50 neurons kept in the hidden layer of the network. Input and target matrices were of size 100X100 for every network.

IV. RESULTS AND FINDINGS

Four experiments were performed using 20, 30, 40 and 50 neurons respectively in hidden layers.

Table II to Table V show the various network parameters like epochs taken by each training, time taken by each and mean square error during each learning process of various pseudo digital signatures. Figure 4 and figure 5 depict the comparisons of performances of various networks on the basis of time, epochs and neurons used in hidden layers.

100-20-100

Training	Epochs	Time	MSE
Training-1	114	0.01	0.22571
Training-2	118	0.1	0.22863
Training-3	133	0.01	0.36431
Training-4	119	0.02	0.15173

Table II- Training Results from first network

100-30-100

Training	Epochs	Time	MSE
Training-1	129	0.04	0.09565
Training-2	114	1.51	0.12025
Training-3	114	0.01	0.12025
Training-4	139	0.1	0.08984

Table III- Training Results from second network

100-40-100

Training	Epochs	Time	MSE
Training-1	118	0.27	0.15114
Training-2	123	1.05	0.20692
Training-3	133	0.01	0.3315
Training-4	134	0.01	0.14387

Table IV-Training Results from third network

100-50-100

Training	Epochs	Time	MSE
Training-1	134	0.01	0.056518
Training-2	115	0.37	0.2605
Training-3	119	0.01	0.10033
Training-4	122	0.01	0.045638

Table V-Training Results from forth network

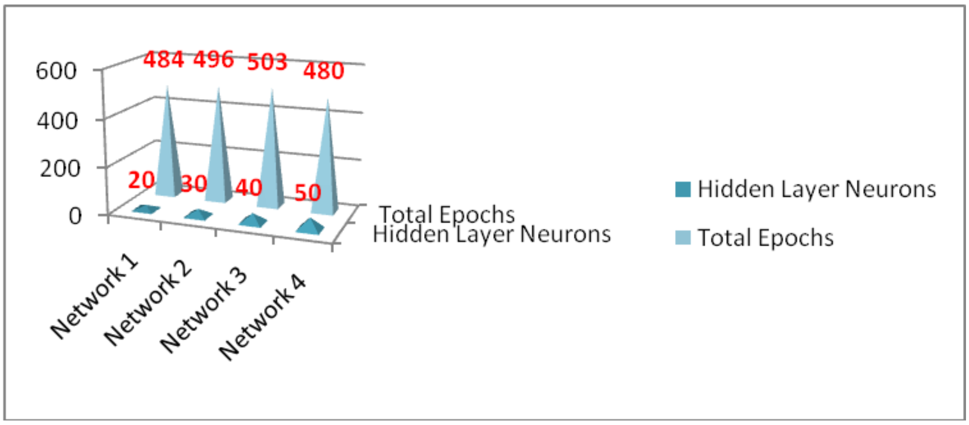

Figure 4- Comparison of total epochs and number of neurons in hidden layers of various networks

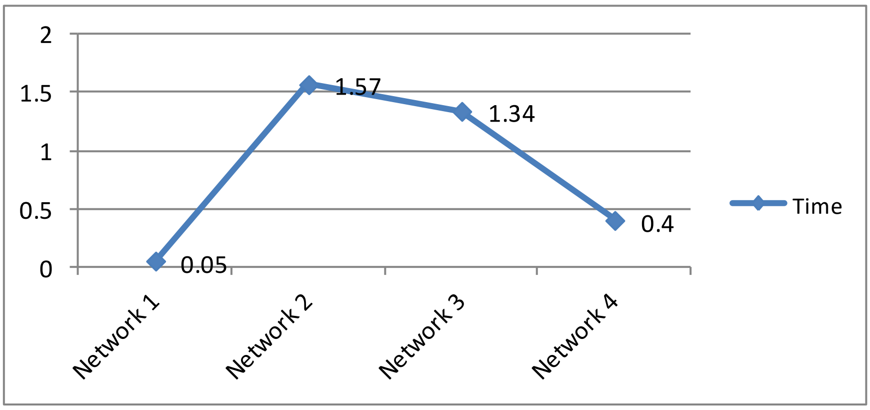

Figure 5- Comparison of time taken by trainings of various networks

Comparison of various networks on the basis of time and epochs shows that the network which has lowest number of neurons in hidden layers takes less time in training and the network which has highest number of neurons needed lowest number of epochs to train the network to achieve the target.

V. CONCLUSION

If any intruder wants to intrude the security of vehicle by forge the pseudo digital signature, it needs to create the manual signature and then needs various network and filters to convert the manual signature into pseudo digital signature. But this is nearly impossible because network once trained will never produce same parameters for exactly same image or data. Only thing intruder can obtain are weights and bias values produced during training of network. Therefore, the attacker cannot forgery the manual signature from a vehicle's memory.

REFERENCES

1. R. Al-Mutiri, M. Al-Rodhaan, and Y. Tian, "Improving vehicular authentication in VANET using cryptography," *Int. J. Commun. Networks Inf. Secur.*, vol. 10, no. 1, pp. 248–255, 2018.
2. X. Wang, S. Li, S. Zhao, Z. Xia, and L. Bai, "A vehicular ad hoc network privacy protection scheme without a trusted third party," *Int. J. Distrib. Sens. Networks*, vol. 13, no. 12, 2017.
3. L. G. Hafemann, R. Sabourin, and L. S. Oliveira, "Offline handwritten signature verification - Literature review," *Proc. 7th Int. Conf. Image Process. Theory, Tools Appl. IPTA 2017*, vol. 2018-January, pp. 1–8, 2018.
4. J. Zhang, "A survey on trust management for VANETs," *Proc. - Int. Conf. Adv. Inf. Netw. Appl. AINA*, pp. 105–112, 2011.
5. A. Rathi, D. Rathi, and P. Astya, "Offline handwritten Signature Verification by using Pixel based Method," *Int. J. Eng. Res. Technol.*, vol. 1, no. 7, pp. 7–10, 2012.
6. M. Mikki, Y. M. Mansour, and K. Yim, "Privacy preserving secure communication protocol for vehicular Ad Hoc networks," *Proc. - 7th Int. Conf. Innov. Mob. Internet Serv. Ubiquitous Comput. IMIS 2013*, pp. 188–195, 2013.
7. N. L. M. Shuib, A. S. M. Noor, H. Chiroma, and T. Herawan, "Elman neural network trained by using artificial bee colony for the classification of learning style based on students preferences," *Appl. Math. Inf. Sci.*, vol. 11, no. 5, pp. 1269–1278, 2017.
8. D. A. Hahn, A. Munir, and V. Behzadan, "Security and Privacy Issues in Intelligent Transportation Systems: Classification and Challenges," *IEEE Intell. Transp. Syst. Mag.*, no. May 2019, pp. 2–17, 2019.

AUTHORS PROFILE

Ekta Narwal, B.Sc. (Computer Science, Mathematics, Physics), M.C.A., Pursuing Ph.D. in Computer Science and Applications. She has total five Paper publication till now. She is working as Assistant Professor Computer Science in Department of Mathematics, Maharshi Dyanand University, Rohtak (Haryana) India from last 7 and half years. Previously she worked as Guest Lecturer, Computer Science, Department of Mathematics, M.D.University Rohtak for one year. Her major research areas are Network Security and Artificial Neural Network. She has research experience of 4 years and teaching experience of nearly 9 years.

Dr Sumeet Gill, B.Sc., M.Sc.(Computer Science),M.Sc. (Physics), S.S. Plasma Astro Physics Diloma from Indian Institute of Science, Banglore, and PhD. He is working as Associate Prof. Computer Science, Department of Mathematics, Maharshi Dayanand University, Rohtak from 17th Dec. 2016 to till date. He worked as Assistant Professor Computer Science, Department of Mathematics, Maharshi Dayanand University, Rohtak from 22nd July 2010 to 16 Dec. 2016, lecturer, Computer Engineering, Group B, Gazetted,.Department of Technical Education, Government of Haryana, 17 Dec. 2004 to 21 July 2010, Lecturer and Coordinator (Training & Placement), Department of Information Sciences & Technology, University College, M.D. University, Rohtak-124001 from 9th February 2001 to 16th December, 2004. Counselor Post Graduate and Under Graduate Courses in Computer Science, Indira Gandhi National Open University, New Delhi, Study Center No.1005 from 1st October 2001 to 31st, December 2007, Guest Lecturer, Department of Computer Science and Applications, M.D. University, Rohtak from 27th July 2002 to 30th April 2003 and lecturer, Department of Physics, Vaish College, Rohtak from 24th July 2000 to 31st Jan. 2001. He has 18 years of Research Experience in the field of system security and network security. He has published 29 research papers.