International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-4, November 2019

Simulation of Biometric Data in VANETs using Layer Recurrent Model

Ekta Narwal , Sumeet Gill

Abstract: ***Biometric identification methods like fingerprints are used throughout the world for authentication such methods are now being researched worldwide for VANETs too. Normally such data are stored in respective files in a computer machine but normally such data from servers/computers are crack-able. There is a need of improving security of such data from intruders as this data contains private information of the driver on road. In this paper we proposed to design and simulate the storage of such biometric data in the form of network parameters of a Neural Network. The simulation of the network is done by using recurrent model and the parameters are saved in place of original biometric images which makes the images impossible to crack. There by providing much more security to the biometric data.***

Keywords: VANET, Biometric, Fingerprints, Recurrent Neural Network, Artificial Neural Network

I. INTRODUCTION

VANETs (Vehicular Ad Hoc Networks) provide many important services to the users in the ad-hoc environment and the personal information of the users like their geo locations, their account details etc. are attached with them. If any suspicious activity occurs in the environment, creates many destructive consequences. Whenever a vehicle wants to convey any message it joins the ad hoc group and for security reasons it goes through some security parameters. One of these security parameters is authentication of vehicle in which vehicle goes through the identity check. There are many user authentication schemes present in VANETs some of them are based on biometric like fingerprints and face recognition of user. An authentication scheme which uses driver's fingerprint as biometric data and it also uses biometric encryption schemes to produce bioscrypt at data link layer produces an effective method to encrypt plaintext stored in the memory related to biometric and uses only bioscrypt for authentication purpose. This bioscrypt tries to protect biometric template from tempering.[1] All biometric parameters store in the authentication server (AS) of the VANETs. Therefore, it is very much necessary to secure these AS with high security parameters because if once they got tampered it is easy for spammers to use identity of other devices/vehicles to spread false messages. So in this paper we will basically focus on the security of biometric data stored in AS using Artificial Neural Networks (ANN). But before doing that process it is necessary to know about the biometric identification, the methods of authentication based on biometric identification in VANETs and also the flaws in security of data stored in AS.[2]

Manuscript published on November 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

II. PRELIMINARIES

A. Biometric Identification Methods

Biometric identification methods base on the biometric features, which are provided by the users for recognition or identification. These features then compare with stored features to authenticate only the matched features. Depending upon the physical and behavioral aspects of the users biometric identification methods can be of two types- Behavioral and Physiological. Attributes of both these methods are used to distinguish one person from other. So the security provided by biometric methods is more powerful than by the normal graphical passwords, as there is no need to keep remembers biometric data.[3]

B. Commonly used Biometrics

Physiological Biometric

Physiological biometric is directly related to the physical parts of human body which remain steady over a large time interval. A person has to remain present physically for such type of identification methods. Some of physiological biometric methods are as follows:

- Iris recognition
- Vascular pattern recognition
- Face recognition
- Retina recognition
- Fingerprint recognition
- Facial thermograph
- Ear geometry based recognition
- Hand geometry based recognition
- Palm print based recognition

Behavioral Biometric

Behavioral Biometric is depend upon the behavior of the users over a time interval, for such type of biometrics users need not to be present physically so these techniques are said to be user friendly. But on the low side these have less uniqueness in comparison to the physical biometric[3]. They are more transparent but less accurate too. Some of behavioral biometric methods are:

- Gait recognition
- Voice recognition
- Keystroke analysis based authentication

- Mouse Dynamics
- Signature Recognition

In this paper we will take example of fingerprint identifications as these are used in VANETs for driver identity verification purpose.

Fingerprints are the patterns of furrows and ridges present on the fingertips. They are unique for all human beings whether they are identical twins or not. These patterns are used for identification from centuries and they have higher matching accuracy too. Biometric data templates related to fingerprints are stored on the hardware devices in form of bitmap images or plaintext. One example of such storing is android device HTC one max in which fingerprints are stored in form of bitmap with size of multiple of 4 bytes by padding and every row of bitmap is start with 0xFE01. 0xFE01 represents it is a fingerprint data. In such devices kernels are responsible for all interactions whether it is with fingerprint sensor or with fingerprint libraries. If the attacker is successful in rooting the device then he/she can easily steal the biometric data[1].They can also modify the templates or replace them with new templates to get unauthorized access to the system or to the network[4].

III. AIMS OF BIOMETRIC DATA PROTECTION SCHEMES

- **Security:** It is necessary that biometric data should hard to obtain from the secured database means it should prevent physical spoofing.
- **Performance:** Biometric data protection should not lower the FAR (False Acceptance Rate) and FRR (False Recognition Rate) of biometric identification systems.
- **Revocability:** The system can rescind any template and can create new one for the same biometric data at any time.
- **Diversity:** The system should not allow cross-matching with in database or outside database for providing privacy to its users.

IV. ATTACKS ON BIOMETRIC AUTHENTICATION SYSTEMS

Intrusion refers to the modification of biometric templates and their operating parameters. Intruder may get the illegal access to the system and that results in loss of important data. There are many types of attacks which are present in biometric authentication systems.

1. Adversary Attacks
2. Attacks on user interface
3. Attacks at the interface
4. Attacks on the software modules
5. Attacks on the hardware modules

Attacks on the hardware modules are the most potential damaging attacks because these can damage or retrieve the biometric templates/data stored in the hardware devices[5]. They can create vulnerabilities like:

- Biometric templates can be replaced by other templates to gain unauthorized access.
- To gain unauthorized access physical spoofing can also be done.
- Cross matching can be done to gain unauthorized access.

V. LAYER RECURRENT NEURAL NETWORK

Layer recurrent is the special type of back propagation model which basically depends on time so it is also called back propagation through time [3]. These networks form directed cyclic graph with the help of connections and because of this feature they are used for solving learning problems of sequential data. Recurrent Neural Network (RNN) is good for text and numeric data that is why in our model we change the image of fingerprints into matrix of double data type. RNN have bidirectional flow which make this network different from other neural networks. Forward data flow is chased by backward data flow to affect the learning process, that's why it is called back propagation through time[6].

VI. PROPOSED SCHEME

VANETs use biometric identification methods for identity verification of the message sender[7]. The biometric is saved in the memory of the vehicle computer system. If any hacker or attacker becomes successful in rooting the device then he can easily access these biometric identities. In our design we first convert the fingerprint images in the encrypted from using morphology and then using Recurrent Neural Network these encrypted images are memorized by the system. We used Layer Recurrent Neural Network Model [8] for the simulation. Figure 1 shows the basic flowchart of the experiment.

For simulation, we took 2 inputs of size 50 X 50 generated from two different format images one .jpg and one .png format and 20 neurons in hidden layer of the each network. Parameters used by the various networks are shown in Table I and II. Two types of training functions are used trainbfg and trainrp for training, both with 20 neurons in hidden layer. Input and target values for both the functions are same.

Table I: Parameters used in LRNN when training done using trainbfg training function

Parameters of LRNN	Setting of the Parameters
LRNN Input Neurons	50
LRNN Hidden Neurons	20
LRNN Hidden Layer Activation Function	TANSIG
LRNN Output Layer Activation Function	PURELIN
LRNN Training Function	Trainbfg
Search Function	srchbac
Minimum Gradient	1e-06
Scale_tol	20
LRNN Number of Hidden Layers	2
Maximum Generations/ Epochs	1000

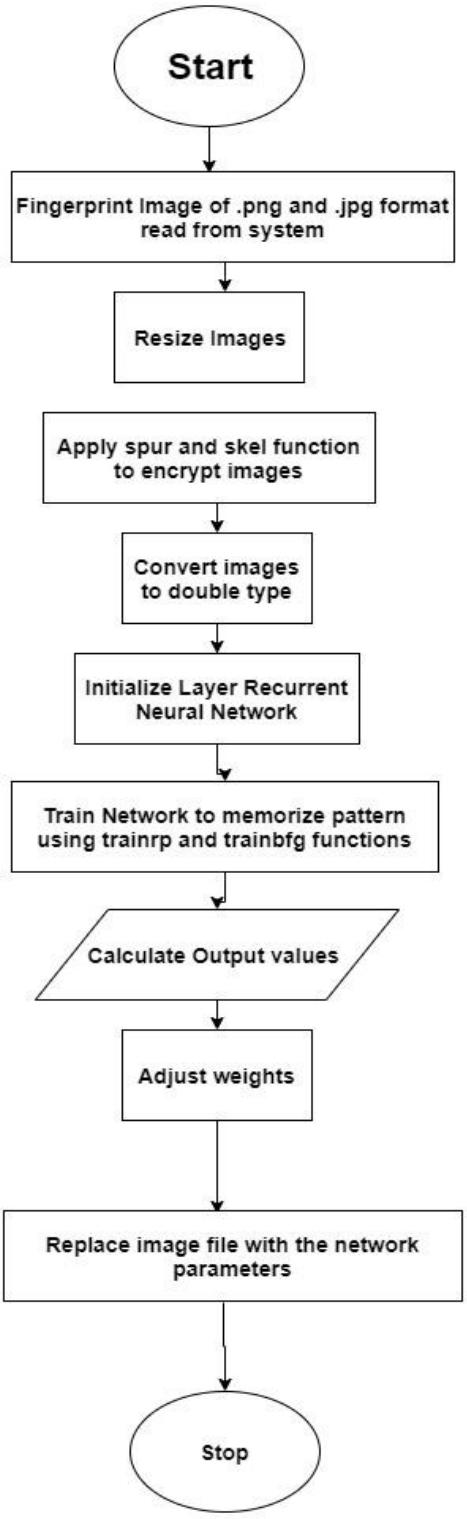

Figure 1- Flowchart to show the simulation mechanism

Table II: Parameters used in LRNN when training done using Trainrp Training Function

Parameters of LRNN	Setting of the Parameters
LRNN Input Neurons	50
LRNN Hidden Neurons	20
LRNN Hidden Layer Activation Function	TANSIG
LRNN Output Layer Activation Function	PURELIN
Delta increment	1.2
Delta Decrement	0.5
Minimum Gradient	1e-05
LRNN Training Function	Trainrp
LRNN Number of Hidden Layers	2
Maximum Generations/ Epochs	1000

Figure 2 to Figure 3 shows the original images used as input in the network, resized images obtained from algorithm and encrypted images generated after applying morphological function 'spur' and 'skel'.

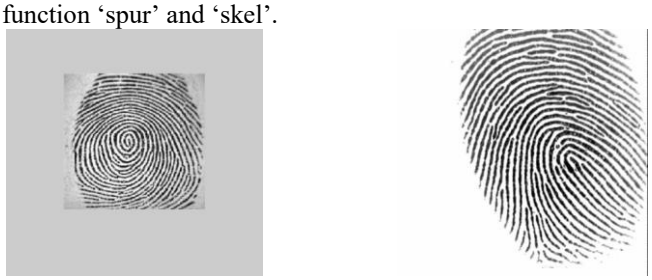

Figure 2- Original Fingerprints used for Training in Different Format Files

Figure 3- Images after Cropping and Resizing

Figure 4- Encrypted Images

VII. RESULTS AND OBSERVATIONS

Network experiments perform different trainings with different learning and transfer functions show different performance for same input values. Table III compares the various performances graphs of the different networks.

It shows that when we use trainbfg training function then network will take more time in comparison to the network trained with trainrp function. Training network with trainrp took more epochs but the time consumption is less. So we can conclude that training with layer recurrent neural network using trainrp training function is the fast method to memorize the patterns. After training the original of the fingerprints are deleted and replaced with the network parameters obtained from the network.

Table III: Comparision of Various Networks

Network	Input	Training Function	Neurons	Epochs	Time
Network 1	Image 1	Trainbfg	20	6	29 sec
Network 2	Image 1	Trainrp	20	33	0 sec
Network 3	Image 2	Trainbfg	20	21	59 sec
Network 4	Image 2	Trainrp	20	28	.02 sec

VIII. CONCLUSION

After the network simulation using recurrent neural network we can conclude that the fingerprints images now can store in the form of network parameters or matrices obtained as result from network which are impossible to reproduce and hence gives more security to the finger print data.

Here are some points which we can carry out after the simulation.

Fresh keys generated each time: The weights and bias for same input and output values will remain different.

Backward Security: Passive adversary cannot guess the old keys because after simulation original fingerprints are removed from the memory only network parameters remain.

Replay Attacks: Random weights are generated during training and all weights remain fresh each time so they deny replay attacks.

Biometric Privacy: When vehicle register with AS then AS stores weights and network parameters in place of bitmap and those network parameters do not reveal any information related to biometric. So they are safe with user or authority.

REFERENCES

1. Y. Zhang, C. Zhaofeng, X. Hui, and T. Wei, "Fingerprints On Mobile Devices: Abusing and Leaking," p. 11, 2015.
2. S. C. Satapathy, A. Govardhan, K. S. Raju, and J. K. Mandal, "Emerging ICT for Bridging the Future - Proceedings of the 49th Annual Convention of the Computer Society of India (CSI) Volume 2," *Adv. Intell. Syst. Comput.*, vol. 338, pp. I–IV, 2015.
3. K. Delac and M. Grgic, "a Survey of Biometric Recognition Methods," no. June, pp. 16–18, 2004.
4. M. Kumar and K. S. Vaisla, "To study of various security attacks against Biometric template in a generic Biometric Recognition System," *Proc. Second Int. Conf. Res. Intell. Comput. Eng.*, vol. 10, pp. 235–240, 2017.
5. L. Yao *et al.*, "Biometrics-based data link layer anonymous authentication in VANETs," *Proc. - 7th Int. Conf. Innov. Mob. Internet Serv. Ubiquitous Comput. IMIS 2013*, pp. 182–187, 2013.
6. A. Rodriguez, J. R. Rabuñal, J. L. Perez, and F. Martinez-Abella, "New Challenges on Bioinspired Applications," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 6687, no. PART 2, pp. 257–266, 2011.
7. I. Buciu and A. Gacsadi, "Biometrics systems and technologies: A survey," *Int. J. Comput. Commun. Control*, vol. 11, no. 3, pp. 315–330, 2016.
8. https://www.sciencedirect.com/topics/computer-science/recurrent-neural-network

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.