STRUCTURAL DIGITAL SIGNATURE FOR IMAGE AUTHENTICATION: USING ARTIFICIAL NEURAL NETWORKS

[1]G.SANGEETHA,[2]A.SENTHIL KUMAR

[1]Research Scholar, Dept.of.Computer Science, Tamil University, Thanjavur-613010.

[2]Asst.professor, Dept.of.Computer science, Tamil University (Established by the Govt.of.Tamilnadu), Thanjavur-613010.

ABSTRACT

The digital data verification methods are able to detect regions that have been tampered with, but are too fragile to resist incidental manipulations. A new digital signature scheme which makes use of an image's contents (in the wavelet transform domain) to construct a structural digital signature (SDS) for image authentication. Identification and verification of hard written signature from images is major issue. This 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 forged ones. By using deep learning which uses the sophisticated is digital configured replica of human brain, we can identify the forgery done in signature with higher accuracy.

Keywords: Authentication, digital signature, deep learning, digital configured replica, forgery, signature

I. INTRODUCTION

Because of the easy-to-copy nature of digitized media, it is very easy for one to tamper with digital data without leaving any clues. Under these circumstances, integrity verification has become an important issue in the digital world. Conventionally, the methods used for media verification can be classified into two kinds: digital signature-based [2], [4],and watermark-based [5], [7], [10]. A digital signature is a set of features extracted from a media, and these features are stored as a file, which will be used later for authentication. A very important characteristic of a digital signature is that it sufficiently represents the content of the original media.

Digital Signature Digital signature which is some sort of cryptographic is a mathematical scheme for demonstrating the authenticity of a digital message or document. Digital signatures are commonly used for software distribution, financial transactions, and in other cases where it is important to detect forgery or tampering. They also act as checksums which are depended on the time period during which they were produced [1].

SIGNATURE VERIFICATION

2.1 Offline Signature Verification:

Verification of signatures with features which are already present is called as offline signature verification. The features are very simple and basic and the image scanned through a camera should follow certain methods for verification. Design of these kind of systems is difficult as there will be less features available.

2.2 Nature of Human Signature:

Human signatures are generally generated by the inbuilt functions of the human neuromuscular area which induces rapid movements. This system will largely consist of neurons and muscle and fibers which make us know that the velocity of the hand produces the equation. So signatures for every person are unique. In this model we can assess the person who will give the signature and train our model accordingly.

2.3 Types of Forgeries:

Forgeries of signatures are classified into three types as mentioned below and we will solve and try to prevent all this forgeries in our model.

2.3.1 Random forgery:

A signature which is forged and it maybe the genuine signature of other person**.**

1.3.2 Casual Forgery :

A signature forgery in which the one who is doing the forgery will know the name of the victim

1.3.3 Skilled Forgery:

As the name suggests a person who is skilled professional is forging signatures is involved in forging the signatures.

IV.CONCLUSIONS

we description of new NIDS framework using anomaly detection agent, is presented which based on multi agent approach as well as Adoptive Threshold Algorithm, in order to form efficient NIDS system which will deals with anomaly from intruder. So; using multi-agent and Adoptive Threshold Algorithm technology in developing intrusion detection Systems provides many features that improve the performance of these systems. Collaborative multi-agent between them and information sharing may thus improve the overall rate of detecting intrusions. For the anomaly detection system used multiagent and Adoptive Threshold Algorithm is implemented in order to achieve accurate identification unknown attacks. Also improved Network Intrusion Detection System is to achieve less complex structure and faster system response time, and to provide a stronger protection to the system from all types of intrusion attacks with less system processing time.

V.REFERENCES

[1] Wang. H., Zhang.D., and Shin.K.G., "Detecting syn flooding attacks" , In Proceedings of IEEE INFOCOM (2002).
[2] Thottan, M, and Ji, C., "Anomaly detection in ip networks", In IEEE Trans. Signal Processing (Aug. 2003), pp. 2191 { 2204.
[3] Deri, L., Suin, S., and Maselli, G., "Design and implementation of an anomaly detection system: An empirical approach", In Proceedings of Terena TNC, 2003.

[4] M. Williams, Immense network assault takes down Yahoo, in: CNN.COM, 2000.
[5] C.S. Institute, F.B.o. Investigation, in: Proceedings of the 10th Annual Computer Crime and Security Survey 10, 2005, pp. 1–23.
[6] S. Axelsson, Intrusion Detection Systems: A Survey and Taxonomy, Chalmers University, Technical Report 99-15, March 2000.

[7] Gilles Balmisse. Les agents, 2002.
[8] Christophe Pincemaille, Intelligent agent technology, Cork Institute of Technology, 2008.
[9] Fabio Bellifemine1, Agostino Poggi, and Giovanni Rimassa " Developing Multi-agent Systems with JADE",2004, http://www.abdn.ac.uk/~csc232/teaching/CS4027/abdn.only /jade_book.pdf
[10] Muhammad Qasim Ali, Adaptive Thersholding for Anomaly Detection Systems, National University of Sciences and Technology, Pakistan, master thesis, 2009.
[11] Hakan Albag " Network & Agent Based Intrusion Detection Systems" , Istanbul, http://www.model.in.tum.de/um/courses/seminar/worm/WS0 405/albag.pdf
[12] M. Benattou, and K. Tamine, " Intelligent Agents for Distributed Intrusion Detection System ",World Academy of Science, Engineering and Technology, 2005 http://www.waset.org/journals/waset/v6/v6-45.pdf
[13] Vasilios A. Siris , Fotini Papagalou "Application of anomaly detection algorithms for detecting SYN flooding attacks", Institute of Computer Science, Hellas,2004. http://www.ist-scampi.org/publications/papers/sirisglobecom2004. pdf
[14] Allam Appa Rao, P.Srinivas, B. Chakravarthy, K.Marx, and P. Kiran "A Java Based Network Intrusion Detection System (IDS)", Andhra university college of engineering , India, proceeding of the 2006 IJME-INTERTECH Conference.
[15] Kalle Burbeck, "Adaptive Real-time Anomaly Detection for Safeguarding Critical Networks", Sweden, 2006, http://liu.divaportal. org/smash/get/diva2:21588/FULLTEXT01.