"Smart Transactional System Using Face Detection Technique"

[1] Vijay Lande, [2] Sujay Shinde
[1,2] Department of computer Technology, JayHind COE, Kuran, Pune

=

Abstract: Now-a-days everyone faces security issues while some online transactions. This problem is increasing rapidly in today's world. So it's necessary to provide security for transactional system. To overcome the problem faced by people regarding transactions "Smart Transactional System Using Face Detection Technique" can be used in future. The major work of this system is to identify the particular person which is doing the transaction for particular things. The Face Detection Algorithm is used to identify the person by the image captured at real-time transactions. This system will automatically identify the person whether he/she is identified user or not. If the system detects that the particular person is not the same as per real-time data. The System will automatically send an E-mail and SMS to the User of that bank account, Bank Sector, and the Investigation (Police). This system will automatically identify the user using face detection technique using real-time data and location of that user.

Keywords: *Fraud Detection, automatically E-mail, SMS*

I. INTRODUCTION

There has been a tremendous increase in electronic transactions during the last decades, due to the popularization of the World Wide Web and e-commerce. Online transactions have gained popularity in the recent years with an impact of increasing fraud cases associated with it. Fraud increases as new technologies and weaknesses are found, resulting in tremendous losses each year. Since the transactions associated with e-commerce are large in number, the dataset associated with them is also large; therefore, it requires fast and efficient algorithms to identify fraudulent transactions. Most of the methods used for fraud detection are rule-based or are systems that require re-training when newer patterns of fraud occur. Detecting fraud as it is happening or within a short time span is not easy and requires advanced techniques. As the demand has arisen for self-learning predictive systems, the main objective is to detect the fraudulent transactions by using Face Detection System, which is a hybrid of neural networks along with fuzzy inference, wherein the system can adapt to newer instances of fraud.

II. PROBLEM STATEMENT

1. Problem Statement:

Recently everyone perform online transactions for everything and at online transaction some security issues are occurred. To overcome the problem faced by people regarding transactions we proposed "Smart Transactional System Using Face Detection Technique" and also identify unauthorized user using phishing or face detection technique.

2. Goals & Objectives:

- ➢ To improve the current manual face detection system.
- ➢ To identify authorized person.
- ➢ To be able to secure transaction.

III. PROPOSED SYSTEM

Recently everyone perform online transactions for everything and at online transaction some security issues are occurred. To overcome the problem faced by people regarding transactions we proposed "Smart Transactional System Using Face Detection Technique". This system proposes a method for online transaction system which

will integrate with the face detection and face recognition technology using Haar Cascade, LBP and GLCM algorithms, respectively. Our solution proposes a technique by which the features extracted from the image clicked during the payment made by user on ecommerce portal will be compared to the features from the training dataset of the respective user. Features extracted from the Images stored in administrator database acts as the training data set for authentication purpose. Further security approaches of online transaction have been focused on, and have been improved using phishing site detection.

A. SYSTEM ARCHITECTURE

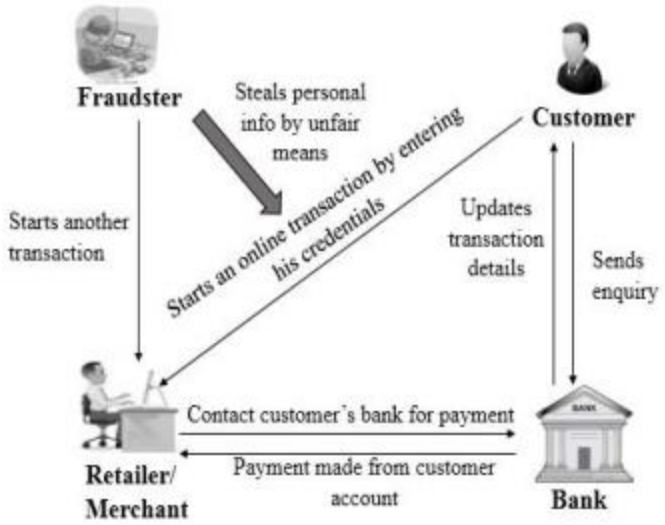

Fig.: System Architecture

B. REQUIREMENTS SOFTWARE AND HARDWARE:

I. Hardware Requirements Specification:

There should be required devices to interact with software.

- System : Pentium IV 2.4 GHz.
- Hard Disk : 40 GB.
- Ram : 256 Mb.

Software Requirements Specification:

- Operating system : Windows XP/7.
- Coding Language : Python
- IDE : PyCharm / Python 3.7.0
- Web server : Apache Tomcat 7.

IV. CONCLUSION AND FUTURE WORK

This proposed system will help to avoid the corruption in rationing system to a large extent by providing transparency at each level. As there is no manual data stored in books or register, all the data is stored in database. hence it becomes easy for higher authority to cross check the data at any point. So implementing this will be really helpful to targeted poor people.

ACKNOWLEDGMENT

This work is presented as an analysis of computational intelligence techniques used for fraud detection in electronic transactions and also a new technique based on python approach is proposed. Online transactions have gained popularity

in the recent years with an impact of increasing fraud cases associated with it. Fraud increases as new technologies and weaknesses are found, resulting in tremendous losses each year. Since the transactions associated with e-commerce are large in number, the dataset associated with them is also large; therefore, it requires fast and efficient algorithms to identify fraudulent transactions.

REFERENCES

[1] Belhumeur, P. N., Hespanha, J. P., Kriegman, D. J. (1997). Eigenfaces vs. Fisherfaces: Recognition Using Class Specific Linear Projection. IEEE Transactions on Pattern Analysis and Machine Intelligence 19, pp. 711-720. IEEE Computer Society

[2] Brunelli, R., Poggio, T. (1993). Face Recognition: Features versus templates. IEEE Transaction on Pattern Analysis and Machine Intelligence, 15 (10), 1042-1052

[3] Viola, P. and Jones, M. Rapid object detection using boosted cascade of simple features. IEEE Conference on Computer Vision and Pattern Recognition, 2001

[4] P. Viola and M. Jones. Robust Real-time Object Detection, International Journal of Computer Vision, 57(2):137154, 2002

[5] Bureau of Justice Statistics, U.S. Department of Justice, April 1990), pp. 43-66; SEARCH Group, Legal and Policy Issues Relating to Biometric Identification Technologies

[6] J. Cox, J. Ghosn, and P.N. Yianilos, Feature-Based Face Recognition Using Mixture Distance, in IEEE Computer Society Conference on Computer Vision and Pattern Recognition, 1996, pp. 209-216.

[7] G. Wang, H. Chen, and H. Atabakhsh, Automatically Detecting Deceptive Criminal Identities, Comm. ACM, Mar. 2004, pp. 70-76.

[8] Cristinacce, D. and Cootes, T. Facial feature detection using AdaBoost with shape constraints. British Machine Vision Conference, 2003