International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 4, Issue 7
July 2017

Evaluating Spoofing Attacks on Biometric Signature Verification System

Farhana Javed Zareen
Jamia Millia Islamia

Suraiya Jabin
Jamia Millia Islamia

ABSTRACT

Biometric systems have become a significant component of present and emerging verification technologies. The aim of a biometric system is to either identify or verify or authenticate an individual using their behavioral or biological characteristics. Although recent biometric systems have reported high-performance rates but many attempts have been reported to fool the biometric system. This paper presents an evaluation of the spoofing attacks on the dynamic signature based biometric system.

KEYWORDS

Biometric, Anti-spoofing, Artificial Neural Network, signatures

INTRODUCTION

Biometrics is by and large generally executed in today's general public to manage the security prerequisite issues [1]. A biometric framework can either do identification or verification. In identification, the biometric framework can build up the personality of a man while check confirms the individual's asserted character from the example put away in the database [3]. Biometric innovation can be isolated into two branches: physiological check and behavioural confirmation. Physiological acknowledgment incorporates discourse, unique handwritten signature, iris and retinal acknowledgment. Physiological acknowledgment is utilized to verify or distinguish an individual while Behavioural acknowledgment looks at the quirks of a person for instance console writing acknowledgment, signature confirmation and so on, these check strategies investigate and perceive how individual signs his handwritten signature or uses a console. Customary verification techniques depend on the information (watchword, Personal Identification Number numbers) or on the ownership of a token (Identification card, keys), which somebody may overlook or can be stolen. This reality puts a great deal of consideration in biometrics as an option strategy for individual verification and recognizable proof [1], [2].

Signature verification has been partitioned into two sorts: offline and online. Offline properties of a handwritten signature manages just the basic qualities though the online elements speak to the basic and also behavioural attributes of a handwritten signature, for example, add up to time taken by the endorser to sign, the weight connected to the pen tip, the speeding up, the pen tip edge and so forth. Programmed signature confirmation is a built up and extremely dynamic research field with essential applications to the approval of checks and other money related archives. This procedure requires a digitizing tablet which is a handwritten signature catching gadget which records the structure of a signature as well as stores the dynamic features of a handwritten signature.

A signature verification system can be checked for accuracy utilizing the accompanying two parameters: The false acceptance rate (FAR), is the measure of how many often a forged signature sample is accepted by the biometric system as genuine. A system's FAR can be typically calculated as the ratio of the number of false acceptances and the number of total attempts. The false rejection rate (FRR), is the measure of how many times a genuine signature sample is rejected by a biometric system as forged. A system's FRR can be calculated as the ratio of the number of false rejections and the number of total attempts.

In this paper, we attempt to explain all types of attacks that can happen on a biometric system and tackle one of the attacks using a novel method.

TYPES OF ATTACKS ON BIOMETRIC SYSTEM

Figure 1 shows different types of attacks that can occur at different levels of a biometric system.

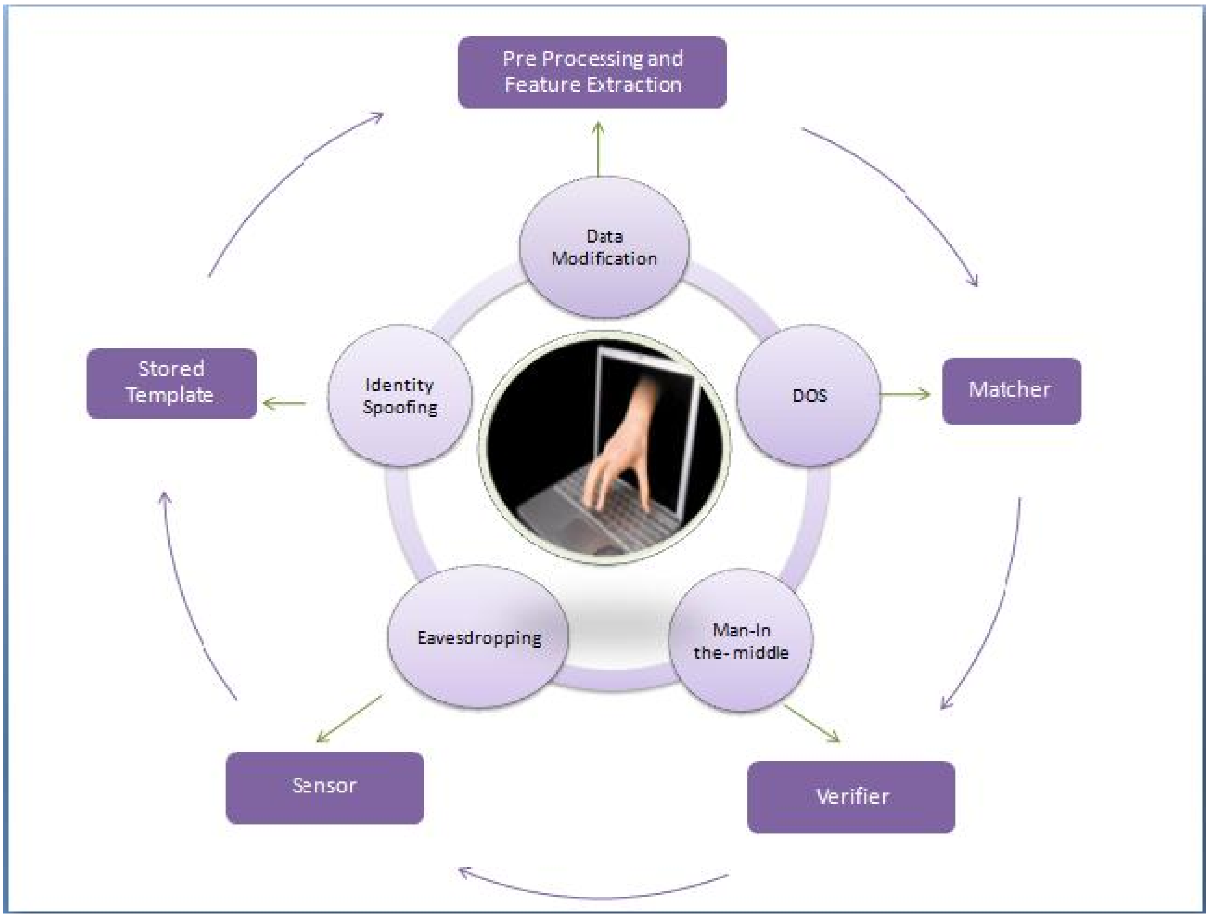

Figure 1: Attacks at different levels of a biometric system

Eavesdropping: It occurs at the data capture level where a sensor is used to capture biometric data. Eavesdropping allows an attacker who has gained access to the biometric system to listen to or read the data that is being captured. When an attacker is eavesdropping on the sensor, it is called sniffing or snooping. The attacker reads the data and stores it to later use it to break into the system using the stolen data.

Data Modification: It occurs at the data pre-processing and feature extraction level. Once the data has been read from the system the next step would be to alter the data. An attacker will modify the data of which the user and the system have no knowledge of. If the sample data is modified in the process then the system will surely fail.

Denial of service (DOS): This occurs at the matcher level where a learning algorithm is required to perform training of the data. Since these algorithms may run on third party servers, instant services are required. An attacker may use DOS attack to prevent normal use of these resources and as a result, the whole system might come to a halt.

Identity spoofing: This occurs at stored template level where the trained samples are stored for verification. An attacker tries to forge the user's signature by posing as the user. Since he has the trained data, he can use it to authenticate himself posing as someone else.

Man in the middle attack: This occurs at the verifier level where the test sample is tested against the stored sample to verify the user. An attacker can sit in between the user and the verifier and manipulate the results by either making the genuine user to be forged or vice versa.

SIGNATURE BIOMETRIC

A biometric signature authentication system is a behavioural biometric system for individual authentication that can be used to perform automated transactions or gaining entry to a protected access [4]. The urgency of implementing an automated handwritten signature authentication system has lead to the introduction of handwritten signature's dynamic information [5]. Handwritten signatures are considered to be ballistic motion. It's a motion which is driven by the brain and does not require any feedback and it cannot be done slowly [6]. Thus a signature or the way of signing never changes with place or time and therefore can be used efficiently for authentication purposes. The signature dynamics are captured using a digitizing tablet, that not only captures the structural property of a signature but also the dynamic features of a signature [7],[8]. The dynamic features of a signature are captured using a tablet is given by equation 1.

$$S_i^j = \{x_i^j, y_i^j, p_i^j, v_i^j, {}^{-}{}_i^j\} \quad (1)$$

Where, S_i^j is the ith signature of the jth signer and $x_i^j, y_i^j, p_i^j, v_i^j, {}^{-}{}_i^j$ are x, y coordinates, pressure with which a person is signing, the velocity of the pen, and the pen angle respectively. There are many other dynamic features that can be captured; it depends on the tablet which is being used to capture the signature. Fig. 2 shows the x coordinates plotted against the timestamp at which the signature was taken.

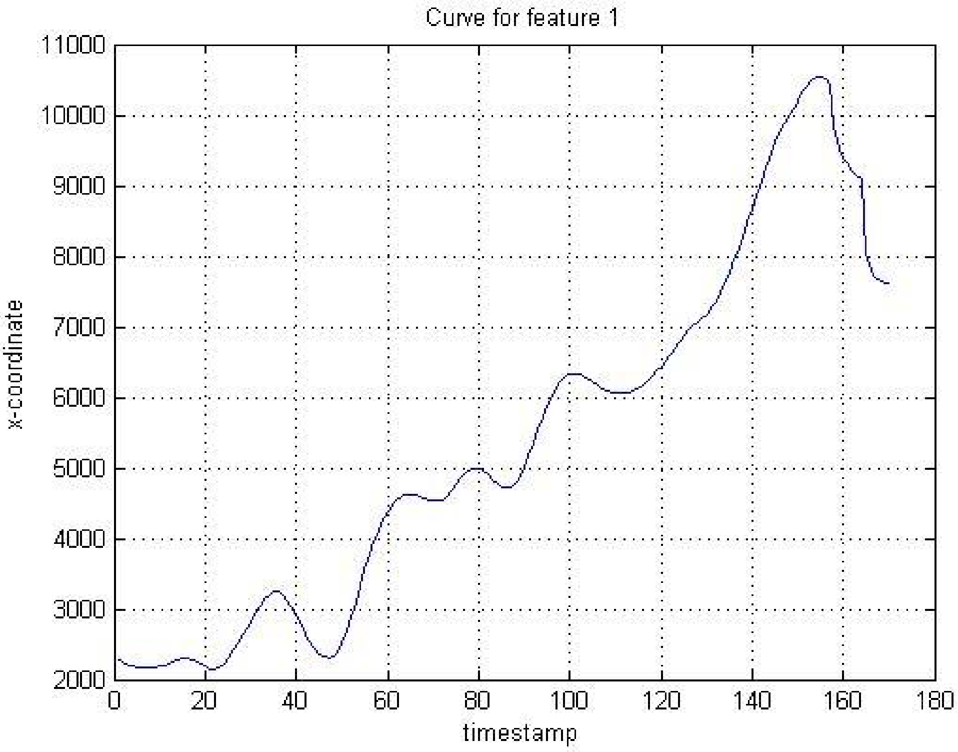

Fig. 2. The x-profile of a signature sample

A signature authentication system is checked using the following three parameters:

False acceptance rate (FAR): FAR measures the accuracy of the biometric system by providing the probability of the cases when the system accepts an incorrect output (forged sample), FAR can be represented using the terms false positives (FP) and true negatives (TN) as given in equation 2.

$$FAR=\frac{FP}{FP+TN} \qquad (2)$$

False Rejection rate (FRR): FRR measures the accuracy of the biometric system by providing the probability of the cases when the system rejects a correct output (genuine sample), FRRcan be represented using the terms false negatives (FN) and true positives (TP) as given in equation 3.

$$FRR=\frac{FN}{FN+TP} \qquad (3)$$

Equal Error Rate (EER): The value when both FAR and FRR becomes equal is the EER of the system. It can be represented using equation 4.

$$EER=FAR\,|_{FAR=FRR}=FRR\,|_{FRR=FAR} \qquad (4)$$

ANTISPOOFING SYSTEM

In this paper, we have attempted to tackle the forgery at the stored template level which is called the identity spoofing, where an attacker steals the stored samples of a user and tries to forge that sample during the verification phase in order to authenticate himself to grant access in the system posing as someone else. We have implemented a system that minimizes any efforts of forgery from an attacker's side by providing a secured signature biometric authentication system. We have used different algorithms on datasets that contain both genuine and forged samples in order to achieve a system with low error rates.

DATASETS

The datasets taken for the experiment is SVC which consists of 100 sets of signature samples. There are 20 samples for each user out of which 20 samples are genuine and other 5 samples are forged. Theses samples have been taken in two different sessions with a gap of atleast 7 days. Each of this signature sample represents seven features that are x coordinate, y coordinate, time stamp, button status, azimuth angle, altitude, and pressure.

EXPERIMENTAL SETUP

A no. of experiments were performed with different network topologies and combination of different learning and transfer functions. Here, we are reporting only the experiments with best results. We use two network topologies and five methods for our experiment. The two topologies used are 106-10-200 and 106-10-5-200. The first topology has 106 input neurons, 10 neurons in hidden layer, and 200 output neurons. Out of 200 output units, 100 units indicate correct class labels of 100 genuine signers, and next 100 units indicate class labels corresponding to 100 forged signers. The second topology has 106 input neurons, 2 hidden layers with 10 and 5 neurons respectively and 200 output neurons. We apply Levenberg-Marquardt Backpropagation, Conjugate Gradient Backpropagation, Resilient Backpropagation, Bayesian Regularization and Gradient Descent method on the database for both the topologies.

EXPERIMENTAL RESULTS

We can see the results that are obtained in our experiments in Table 1 and Table 2. For the network topology 106-10-200, Bayesian regularization method is providing the best results as we can see in Table 1. Whereas Levenberg-Marquardt Backpropagation method's performance is also good with EER 5%. In Table 2, we can see that Levenberg-Marquardt Backpropagation is providing the best result for the topology 106-10-5-200 and Bayesian Regularization gives the second best result. Thus, we can conclude that Bayesian Regularization and Levenberg-Marquardt Backpropagation provide the best results in both the topology as we can see from fig.3.

Table 1. Performance of the system with Network topology 106-10-200

Training Function	Network Topology	Performance (EER%)
Levenberg-Marquardt Backpropagation	106-10-200	5
Scaled Conjugate Gradient Backpropagation	106-10-200	50
Resilient Backpropagation	106-10-200	30
Bayesian Regularization	106-10-200	2.6
Gradient Descent Backpropagation	106-10-200	30

Table 2. Performance of the system with Network topology 106-10-5-200

Training Function	Network Topology	Performance (EER%)
Levenberg-Marquardt Backpropagation	106-10-5-200	5
Scaled conjugate gradient Backpropagation	106-10-5-200	43.4
Resilient Backpropagation	106-10-5-200	25
Bayesian regularization	106-10-5-200	6
Gradient descent Backpropagation	106-10-5-200	15

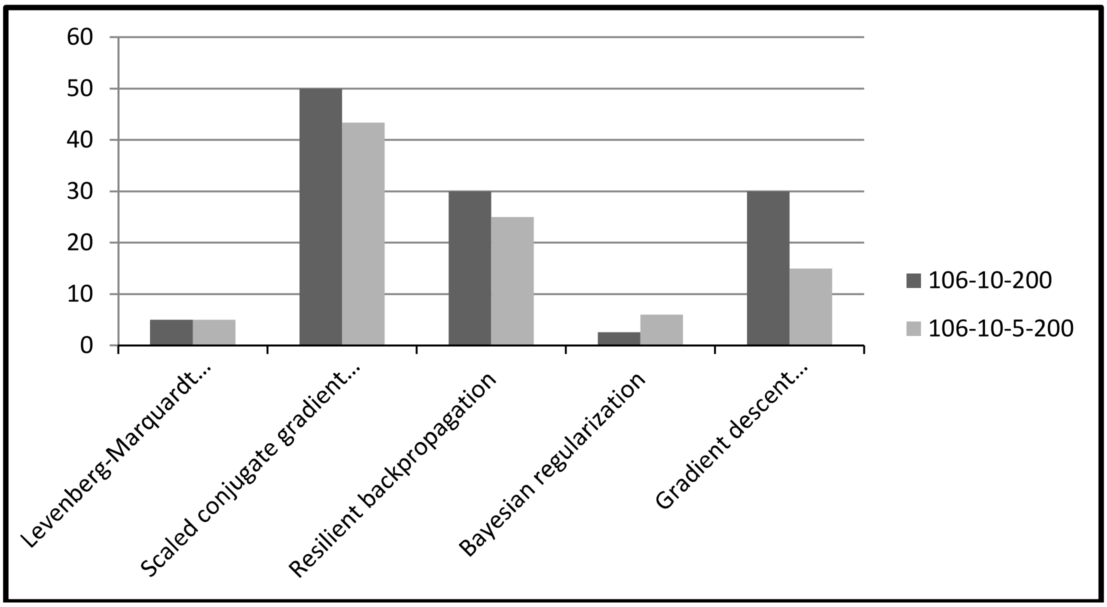

Fig. 3. Comparison of results obtained from experiments

CONCLUSION

The paper provides a comparative analysis of the performance of five different algorithms that can be used to train an artificial neural network for a spoof-proof biometric signature authentication system. It is evident from the experimental results that Levenberg-Marquardt Backpropagation and Bayesian Regularization are the two methods that are giving the best results for dynamic signatures. For network topology 106-10-200, the Bayesian Regularization algorithm outperforms all the other algorithms with minimum equal error rate of 2.6% and Levenberg-Marquardt Backpropagationprovides equal error rate of 5% for network topology 106-10-5-200, Levenberg-Marquardt Backpropagation algorithm provides the best results with equal error rate of 5% along with that we get a close result with Bayesian Regularization algorithm of equal error rate 6%. Through these results, we can conclude that Levenberg-Marquardt Backpropagation and Bayesian regularization algorithm works better for the anti spoofing signature biometric authentication system.

REFERENCES:

[1] S. Garcia-Salicetti and B. Dorizzi, “On using the Viterbi path along with HMM likelihood information for online signature verification,” IEEE Trans. Syst., Man, Cybern. B, vol. 37, no. 5, pp. 1237–1247, Oct. 2007.

[2] E. A. Rúa and J. L. Alba, “Online Signature Verification Based on Generative Models,” IEEE Trans. Syst., Man, Cybern. B, vol. 42, no. 4, pp. 1231-1242, Aug. 2012.

[3] D. Impedovo and G. Pirlo, “Automatic Signature Verification: The State of the Art,” IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS—PART C: APPLICATIONS AND REVIEWS, VOL. 38, NO. 5, SEPTEMBER 2008.

[4] Guru, D. S., Prakash, H. N. (2009). Online signature verification and recognition: An approach based on symbolic representation. Pattern Analysis and Machine Intelligence, IEEE Transactions on, 31(6), 1059-1073.

[5] Van, B. L., Garcia-Salicetti, S., &Dorizzi, B. (2007). On using the Viterbi path along with HMM likelihood information for online signature verification. Systems, Man, and Cybernetics, Part B: Cybernetics, IEEE Transactions on, 37(5), 1237-1247.

[6] Gupta, G. K., & Joyce, R. C. (2007). Using position extrema points to capture shape in on-line handwritten signature verification. Pattern Recognition, 40(10), 2811-2817.

[7] Zareen, F. J., & Jabin, S. (2016). Authentic mobile-biometric signature verification system. IET Biometrics, 5(1), 13-19.

[8] Jabin, S., & Zareen, F. J. (2015). Biometric signature verification. International Journal of Biometrics, 7(2), 97-118.