ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Providing Privacy to Confidential Data Using Novel Fusion Techniques

Y.Sai Sandya Lakhmi
M.Tech Student
Department of CSE
Malla Reddy College of Engineering,
Hyderabad, India.

K.U.Usha
Assistant Professor
Department of CSE
Malla Reddy College of Engineering,
Hyderabad, India.

Abstract

Pattern classification can be defined as "the act of taking in raw data and taking an action based on the category of the pattern". Mainly the pattern classification techniques are used in security applications such as biometrics based person recognition and intrusion detection in computer networks and spam filtering, Goal to discriminate between the legitimate and a malicious pattern class. Biometric tasks are different from classical pattern recognition tasks. Biometric spoof attack using fake fingerprints. Since the pattern classification techniques do not take into account the adversarial nature of recognition, here exhibit performance degradation when used in adversarial setting, namely under attacks. So our proposed models to achieve a good approximation of fake traits score distribution and our method providing an adequate estimation of the security of biometric systems against spoof attacks. Our experimental shows that robustness of the MMBS to spoof attacks strongly depends on the matching algorithms. We deal with the protection of multimodal biometric systems (MMBS), here propose a two novel fusion techniques that be able to increase the protection and performance. The first extension is LLR based fusion scheme and fuzzy logic. the proposed method allows to point out the vulnerabilities of multimodal biometric score fusion rules to spam attacks.

I.INTRODUCTION

In Pattern classification systems machine learning algorithms are used to perform security-related applications like biometric authentication, network intrusion detection, and spam filtering, to distinguish between a "legitimate" and a "malicious" pattern class. The input data can be purposely manipulated by an adversary to make classifiers to produce false negative.

This often gives rise to an arms race between the adversary and the classifier designer. Well known examples of attacks are: Spoofing attacks where one person or program purposely falsifying data and thereby gaining an illegitimate advantage, modifying network packets belonging to intrusive traffic manipulating contents of emails [3], modifying network packets belonging to intrusive traffic. Mainly three main open issues are identified: (i) analyzing the vulnerabilities of classification algorithms, and the corresponding attacks (ii) developing novel methods to assess classifier security against these attacks (iii) developing novel design methods to guarantee classifier security in adversarial environments. Machine learning is used to prevent illegal or unsanctioned activity which are created from adversary. Machine learning is used in security related tasks involving classification, such as intrusion detection systems, spam filters, biometric authentication. Measuring the security performance of these classifiers is an essential part for facilitating decision making.

II.LITERETURE SURVE

In this paper, we address the security of multimodal biometric systems when one of the modes is effectively spoofed. We propose two novel fusion schemes that can expand the security of multimodal biometric systems. The main is an expansion of the

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

likelihood ratio based fusion scheme and alternate uses fuzzy logic. Other than the matching score and example quality score, our proposed fusion schemes additionally consider the natural security of every biometric framework being melded. Exploratory results have demonstrated that the proposed strategies are more vigorous against parody assaults when contrasted and conventional fusion techniques.

In biometric systems, the risk of "spoofing", where a sham will fake a biometric quality, has lead to the expanded utilization of multimodal biometric systems. It is accepted that a fraud must satire all modalities in the framework to be acknowledged. This paper takes a gander at the situations where some yet not all modalities are spoofed. The commitment of this paper is to diagram a strategy for evaluation of multimodal systems and fundamental fusion algorithms. The structure for this technique is depicted and analyses are led on a multimodal database of face, iris, and fingerprint match scores.

An extremely powerful intends to avoid mark based intrusion detection systems (IDS) is to utilize polymorphic methods to produce assault examples that don't impart an altered mark. Anomaly-based intrusion detection systems give great barrier in light of the fact that current polymorphic strategies can make the assault occasions look not quite the same as one another, yet can't make them look like typical. In this paper we present another class of polymorphic assaults, called polymorphic mixing assaults, that can viably sidestep byte recurrence based system anomaly IDS via deliberately matching the measurements of the transformed assault examples to the typical profiles. The proposed polymorphic mixing assaults can be seen as a subclass of the mimicry assaults. We take a methodical methodology to the issue and formally portray the calculations and steps needed to do such assaults. We demonstrate that such assaults are doable as well as break down the hardness of avoidance under distinctive circumstances. We present itemized systems utilizing PAYL, a byte recurrence based anomaly IDS, as a detailed analysis and exhibit that these assaults are without a doubt doable. We additionally give some knowledge into conceivable countermeasures that can be utilized as barrier.

III. EXISTING SYSTEM:

Pattern classification systems based on classical theory and design methods do not take into account adversarial settings; they exhibit vulnerabilities to several potential attacks, allowing adversaries to undermine their effectiveness.

A systematic and unified treatment of this issue is thus needed to allow the trusted adoption of pattern classifiers in adversarial environments, starting from the theoretical foundations up to novel design methods, extending the classical design cycle of. In particular, three main open issues can be identified:
(i) Analyzing the vulnerabilities of classification algorithms, and the corresponding attacks.
(ii) Developing novel methods to assess classifier security against these attacks, which is not possible using classical performance evaluation methods.
(iii) Developing novel design methods to guarantee classifier security in adversarial environments.

DISADVANTAGES OF EXISTING SYSTEM:

1. Poor analyzing the vulnerabilities of classification algorithms, and the corresponding attacks.
2. A malicious webmaster may manipulate search engine rankings to artificially promote her1 website.

IV. PROPOSED SYSTEM:

In this work we address issues above by developing a framework for the empirical evaluation of classifier security at design phase that extends the model selection and performance evaluation steps of the classical design cycle .We summarize previous work, and point out three main ideas that emerge from it. We then formalize and generalize them in our framework. First, to pursue security in the context of an arms race it is not sufficient to react to observed attacks, but it is also necessary to proactively anticipate the adversary by predicting the most relevant, potential attacks through a what-if analysis; this allows one to develop

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

suitable countermeasures before the attack actually occurs, according to the principle of security by design. Second, to provide practical guidelines for simulating realistic attack scenarios, we define a general model of the adversary, in terms of her goal, knowledge, and capability, which encompasses and generalizes models proposed in previous work. Third, since the presence of carefully targeted attacks may affect the distribution of training and testing data separately,We deal with the protection of multimodal biometric systems(MMBS), here propose a two novel fusion techniques that be able to increase the protection and performance. we also propose an algorithm for the generation of training and testing sets to be used for security evaluation,which can naturally accommodate application-specific and heuristic techniques for simulating attacks.

ADVANTAGES OF PROPOSED SYSTEM:

1. Prevents developing novel methods to assess classifier security against these attack.
2. The presence of an intelligent and adaptive adversary makes the classification problem highly non-stationary.

V. IMPLEMENTATION

Implementation is the stage of the project where the theory is accepted and initiation of process to convert theory into working system. Hence it can be considered to be the most important stage in achieving a successful new system and in giving the user, so that the new system will work and be effective.

The implementation step involves cautious planning, analysis of the current system and it's constraints on implementation, we can achieve barter and evaluation of changeover methods by using designing methods.

MODULES:

1. Attack Scenario and Model of the Adversary
2. Pattern Classification
3. Adversarial classification:
4. Security modules

MODULES DESCRIPTION:

Attack Scenario and Model of the Adversary:

Although the definition of attack scenarios is ultimately anapplication-specific issue, it is possible to give generalguidelines that can help the designer of a pattern recognition system. Here we propose to specify the attack scenarioin terms of a conceptual model of the adversary that encompasses, unifies, and extends different ideas from previouswork. Our model is based on the assumption that the adversary actsrationally to attain a given goal, according to herknowledgeof the classifier, and hercapabilityof manipulatingdata. This allows one to derive the corresponding optimalattack strategy.

Pattern Classification:

Multimodal biometric systems for personal identity recognition have received great interest in the past few years. It has been shown that combining information coming from different biometric traits can overcome the limits and the weaknesses inherent in every individual biometric, resulting in a higher accuracy.

Moreover, it is commonly believed that multimodal systems also improve security against Spoofing attacks, which consist of claiming a false identity and submitting at least one fake biometric trait to the system(e.g., a "gummy" fingerprint or a photograph of a user's face). The reason is that, to evade multimodal system, one expects that the adversary should spoof all the corresponding biometric traits. In this application example, we show how the designer of a multimodal system can verify if this hypothesis holds, before deploying the system, by simulating spoofing attacks against each of the matchers.

Adversarial classification:

Assume that a classifier has to discriminate between legitimate and spam emails on the basis of their textual content, and that the bag-of-words feature representationhas been chosen, with binary features denoting the occurrence of a given set of words

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Security modules:

Intrusion detection systems analyze network traffic to prevent and detect malicious activities like intrusion attempts,ROC curves of the considered multimodal biometric system under a simulated spoof attack against the fingerprint or the face matcher. Port scans, and denial-of-service attacks.When suspected malicious traffic is detected, an alarm is raised by the IDSand subsequently handled by the system administrator.

Two main kinds of IDSs exist: misuse detectors and anomaly-based ones. Misuse detectors match the analyzed network traffic against a database of signatures of known malicious activities.The main drawback is that they are not able to detect never-before-seen malicious activities, or even variants of known ones. To overcome this issue, anomaly-based detectors have been proposed. They build a statistical model of the normal traffic using machine learning techniques, usually one-class classifiers,and raise an alarm when anomalous traffic is detected. Their training set is constructed, and periodically updated to follow the changes of normal traffic, by collecting unsupervised network traffic during operation, assuming that it is normal (it can be filtered by a misuse detector, and should).

Novel fusion security Algorithms

1. Algorithm ImageMatch(T, P)

Input text ***T*** of size ***n*** and pattern
P of size ***m***
Output starting index of a
substring of ***T*** equal to ***P*** or -1
if no such substring exists

for $i \leftarrow 0$ **to** $n - m$
{ test shift i of the pattern }
$j \leftarrow 0$
while $j < m \wedge T[i + j] = P[j]$
$j \leftarrow j + 1$
if $j = m$
return i {match at i}
else
break while loop {mismatch}
return **-1** {no match anywhere

}

2. Algorithm BoyerMooreMatch(T, P, S)

$L \leftarrow$ ***lastOccurenceFunction***(P, S)
$i \leftarrow m - 1$
$j \leftarrow m - 1$
repeat
if $T[i] = P[j]$
if $j = 0$
return i { match at i }
else
$i \leftarrow i - 1$
$j \leftarrow j - 1$
else
{ character-jump }
$l \leftarrow L[T[i]]$
$i \leftarrow i + m - \min(j, 1 + l)$
$j \leftarrow m - 1$
until $i > n - 1$
return -1 { no match }

VI. CONCLUSION AND FUTUREWORK

In this paper we focused on empirical security evaluation of pattern classifiers that have to be deployed in adversarial environments, and proposed how to revise the classical performance evaluation design step, which is not suitable for this purpose.

Our main contribution is a framework for empirical security evaluation that formalizes and generalizes ideas from previous work, and can be applied to different classifiers, learning algorithms, and classification tasks. It is grounded on a formal model of the adversary, and on a model of data distribution that can represent all the attacks considered in previous work; provides a systematic method for the generation of training and testing sets that enables security evaluation; and can accommodate application-specific techniques for attack simulation. This is a clear advancement with respect to previous work, since

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

without a general framework most of the proposed techniques (often tailored to a given classifier model, attack, and application) could not be directly applied to other problems.

REFERENCES

1. R.N. Rodrigues, L.L. Ling and V. Govindaraju "Robustness of Multimodal Biometric Fusion Methods against Spoof Attacks", J.¿¿Visual Languages and Computing, vol. 20, no. 3, pp.169 -179 2009

2.P. Johnson, B. Tan and S. Schuckers "Multimodal Fusion Vulnerability to Non-Zero Effort (Spoof)Imposters", Proc. IEEE Int¿¿¿l Workshop Information Forensics and Security, pp.1 -5

3.P. Fogla, M. Sharif, R. Perdisci, O. Kolesnikov and W. Lee "Polymorphic Blending Attacks", Proc. 15th Conf. USENIX Security Symp.,

4. G.L. Wittel and S.F. Wu "On Attacking Statistical Spam Filters", Proc. First Conf. Email and Anti-Spam,

5. D. Lowd and C. Meek "Good Word Attacks on Statistical Spam Filters", Proc. Second Conf. Email and Anti-Spam,

6. A. Kolcz and C.H. Teo "Feature Weighting for Improved Classifier Robustness", Proc. Sixth Conf. Email and Anti-Spam,

7.D.B. Skillicorn "Adversarial Knowledge Discovery", IEEE Intelligent Systems, vol. 24, no. 6, 2009

8. D. Fetterly "Adversarial Information Retrieval: The Manipulation of Web Content", ACM Computing Rev., 2007

9. R.O. Duda, P.E. Hart and D.G. Stork Pattern Classification, 2000 :Wiley-Interscience Publication

10.N. Dalvi, P. Domingos, Mausam, S. Sanghai and D. Verma "Adversarial Classification", Proc. 10th ACM SIGKDD Int¿¿¿l Conf. Knowledge Discovery and Data Mining, pp.99 -108.