Method for Detecting People Who are Trying to Fool Security

Shmuel UR

***Abstract*—This paper was originally submitted to Xinova as a response to a Request for Invention (RFI) focusing on new Decision and Response Techniques for Security Applications. This paper describes a method for distinguishing people who are being evasive.**

In more detail, this describes how to utilize computers to recognize in people in both human-like and machine-like ways, and compare for discrepancies.

I. Abstract

IN the beginning of AI and machine learning, we tried to reason how people do things (play chess, recognize faces), and train computers to do the same. This approach was later discarded. We don't really care how people do that but we train computer to do those things very well. Computers can now play chess better than the best players, and they can also recognize faces very well. The way they do it is very different than the way people do it. In general, the learning is done by giving the computers a large number of samples from which they learn. The algorithm created is usually very different than that which is used by humans.

For example, in http://u.cs.biu.ac.il/~koppel/papers/impostors-journal-revised2-140213.pdf, they discuss "Determining if Two Documents are by the Same Author". The problem is when you write a document, try to disguise your style, or give a different name. They want to detect if it is you. Computers can use a different method for which the fact that you change your style to the best of your ability does not help much. The computer looks at thousands of writing characteristics while you know only how to change ten. The computers are able to recognize the writer well, while people may be fooled.

Instead of training computers to solve a problem, we can train computer to give the same solutions as humans. The difference in the training set would be to give the reply a human would give instead of the correct reply. Sometimes it is the correct reply but sometimes not. For example, assume that you want to train to recognize a face of X. You give the computer a number of examples of X and then asks question Y, that asks if Y is the same as X? When you want to teach the computer to recognize people you will give it the correct reply, so in the training set on a specific question you will indicate if Y is indeed X or not.

If you want to know if people would understand that Y is X, you can ask them. In the training, they are the same examples of X, but now on every Y, instead of saying yes if Y is X we say Yes if people think that Y is X. This will train computers to recognize people in a manner that is similar to people, as the features that people use to recognize people will be prominent.

The fact that different ways of looking at things can be used to detect disguises is not new. For example, in WW2 they used color blind people used to spot camouflage nets as they looked at contrast and not color, different thing than the people hiding them use.

II. Summary of the invention

The invention is a method for recognizing people who try to deceive observers. We try to discover the following cases

1. A person who tries to disguise so he will not be recognized. This is triggered if the computer program that recognize people, recognize him, but the computer program that tries to emulate people recognition does not.
2. Someone who tries to masquerade as a specific person. This is triggered if the computer program that emulate people recognize him, but the generic one does not.

The first case is more common but the second case also has security implications.

The differentiation of recognizing as a person does, or in general, can be for face recognition, gate recognition,

voice or any other method used by computer and people.

III. Detailed Explanation

The invention is composed of two components and the way they are used together to achieve the deception detection task.
The first component is the regular computer algorithm. An example could be a face detection algorithm,

https://en.wikipedia.org/wiki/Face_detection or gait detection biometrics

https://en.wikipedia.org/wiki/Gait_analysis#Biometric_identification_and_forensics or voice detection biometrics

https://en.wikipedia.org/wiki/Speaker_recognition.

In general, those are computer algorithm that reply to one of the two different but similar questions: 1) who is this person or 2) is this person X. The first question happens when you scan a crowd, you see a person and you want to know who it is, and the second is when a person identify as X and you want to know if this is true. In voice you get a voice and is asked who is it (question 1), or you get a voice, you can see the ID on the phone as Shmuel, and you ask is it Shmuel (question 2).

The second component is a computer algorithm trained to achieve the same task but to reply as a human observer would. So instead of being trained with the correct replies, it is trained with the replies that humans would give, which are mostly accurate, but sometime mistaken. This is a different use to the paradigm of supervised learning
https://en.wikipedia.org/wiki/Supervised_learning.
"Supervised learning is the machine learning task of inferring a function from labeled training data.[1] The training data consist of a set of training examples. In supervised learning, each example is a pair consisting of an input object (typically a vector) and a desired output value (also called the supervisory signal). A supervised learning algorithm analyzes the training data and produces an inferred function, which can be used for mapping new examples. An optimal scenario will allow for the algorithm to correctly determine the class labels for unseen instances. This requires the learning algorithm to generalize from the training data to unseen situations in a "reasonable" way" to understand the difference assume the following common scenario for face recognition. We have 1000 pictures of Shmuel, in the first algorithm they are all labelled Shmuel. In the second, we take a human and ask him to label the pictures, those he recognizes as Shmuel will be so recognized but some may be called Vlad, or not identified. We know it is Shmuel but it is not identified as Shmuel. The algorithm learns according to the training set, so the second algorithm does not learn to identify Shmuel but to identify the images human observer identify as Shmuel. **The entire concept capitalizes on this difference.** For the learning to be differentiated we need examples in which humans make mistake. Sometimes it is easy, in tasks human are not great at, but in others, like face recognition where humans are good we can manufacture many examples by adding lots of disguised pictures into the training set. Those are easy to find in the right quantities, taken from films, theatre, and many other places. So we need to find examples in which for the same image/voice/whatever the labelling of the human observation and the true labelling are different. Finding examples in which they are the same is generally very easy. This approach will give two algorithms which generally agree but may disagree where a disguise of some kind is used.

The third component is application specific. It uses the first two to achieve a task. The two most common examples are the following:

Example one: There are many people on a suspect list with different priorities, for example, criminals, agitators, extremists. When they are identified in an event a flag may be raised. However, this may not be considered a strong enough indication that requires action. If, in addition, we are told that they are trying to disguise, this is a stronger flag. For example, the following two people in Figure 1 are the same. They have the same face structure, so a computer may not be fooled, but most people would be.

Fig. 1. Same person

In example one, if one computer program recognizes a person on the list, and the second, the "human-like one" does not, we assume he may be up to something and a

stronger warning is given. This is the main use case. This same use case is relevant for a casino. Casino may be watching for professional gamblers. They may be allowed to enter but the casino needs to know what they are doing. Thus, often they use disguise. For example, "Because the Hyland team has been counting cards for so long they are recognized at many casinos. The team has used disguises throughout the years at various casinos." http://www.stjosephpost.com/2013/04/01/professional-gambler-charged-with-hiding-winnings-from-casino-feds/

Example Two: In many places, some of the people are known to the guards, so they can get in with a hand wave. One way to overcome security is to impersonate one of this people. This may be easier than we think it is (but still not the main example of this invention). Impersonators are very good at impersonating voices (over the phone) or gate (walking) or even a face, using make up. It will be good to have a warning on the phone that this may not be the person we expect, or the guard may get a warning that the person walking in, the one that looks familiar, may not be the one who regular comes. In this case, there is a list of the "regulars", if we see a case where a human would recognize someone as one of the regulars (the second component) but the computer does not (the first component) than we give a warning to the guard to validate that person.

An example of this is an Obama impersonator, in Figure 2

Fig. 2. Impersonator and the real person

For example, when I call the bank, the teller recognise my voice (he knows me), so I can give instructions. If he would get a warning that the phone ID and the person do not match, he may be more alert.

Again the learning of voice uses the same supervised learning concept. It is fairly easy to lie to humans, as you know what they are listening to,. It is harder to fool computers as they listen to different things, and it is much harder to fool both.
https://www.youtube.com/watch?v=7TSNdsCtaOA

IV. Conclusion

Could be quite additional applications of the difference between the way computer and people do things. The learning of how people do things, with supervised learning, as appose to the true result is the key thing. In that learning, we need many examples meant to fool people. For example, in face recognition we have a huge set of images from movies, in which actors are disguised and harder to recognise, allows to test and raise the alertness level automatically.

The invention makes use of the fact that people are adept at fooling human observers, but that computers look at things differently. Fooling one and not the other can trigger alerts. This invention:

- Determines the discrepancy between output of what computers recognize, and how humans would (human-like vs. machine-like)
- Can concentrate on feature discrepancies including include face, gait, or other distinguishable characteristics

Acknowledgment

This research was originally submitted to Xinova, LLC by the author in response to a Request for Invention. It is among several submissions that Xinova has chosen to make available to the wider community. The author wishes to thank Xinova, LLC for their funding support of this research.
More information about Xinova, LLC is available at www.xinova.com.