Biometric Authentication Exemptions using Pattern Exceptions

By: Jeffrey Nickerson

Introduction

Biometric authentication systems may be enabled to recognize and react to biometric pattern exceptions. The results can be used to identify whether the scanned individual is exempt from true authentication and further security checks. System processing may include: obtaining biometric authentication data from a biometric reader, analyzing the biometric authentication data, identifying from the biometric authentication data that the biometric authentication data contains a biometric pattern exception, responding to identification of the biometric pattern exception, and performing specialized exemption processing including determining a set of alias authentication credentials to be associated with the individual and/or suppressing any security alarms. The biometric pattern exception may be used for multiple exempt individuals.

Background

Current biometric authentication systems have become capable of authenticating individuals using multiple types of biometric data, such as ocular scanning of the eyeball or iris, fingerprint scanning, 3D-facial scanning, and other methods become available as one of ordinary skill in the art would appreciate.

In these systems, the biometric authentication occurs by obtaining biometric authentication data from a biometric scanning of some sort. In ocular scanning, for instance, an iris may be scanned to create a set of authentication data. This authentication data is then analyzed to determine a set of authentication credentials, or the identity, associated with the scanned individual.

However, these biometric authentication systems have advanced in such a way that they can identify when an individual is attempting to circumvent the system. For instance, the systems have verification checks in place to ensure that only a single identity or a single set of authentication credentials maps to a single unique set of biometric authentication data. That is, the system assumes a particular set of biometric authentication data can be linked to a unique

human existing on earth, and therefore only allows each unique biometric authentication data to represent a single identity. Individuals of the system cannot map to multiple identities.

Furthermore security measures to prevent biometric spoofing are implemented in newer biometric authentication systems. Some of these prevention techniques include determining whether the scanned individual is wearing contact lenses (spoofing ocular authentication data), or whether the scanned individual is wearing gel fingertips (spoofing fingerprint authentication data). Thus it is difficult for a scanned individual attempting to be identified by the authentication system as an alias (an identity that is not the true identity of the scanned individual), to use spoofing items that identify the scanned individual as the alias.

Government agents that typically use multiple aliases to cross country borders may be limited to only one alias if the biometric authentication system requires his or her ocular authentication data to map to a single authentication credential or identity. And if the agent attempts to spoof the biometric system with contact lenses or fingerprint gels, the system will raise a security alarm.

Thus there exists a need for enabling individuals with good intentions to be exempt from biometric authentication, and to link only certain individuals to an alias identity or alias authentication credential, all without security operators being aware that the individuals are using an alias that is not their true identity.

Objective of System

To configure a biometric authentication system for use, the system may be accessed either during manufacturing or after deployment in order to alter its operating methods to include authentication exemptions. One objective of the system is to alleviate any concerns of a security officer operating the biometric authentication system. Another objective is to ensure the biometric authentication system and security officer identify the scanned individual as an alias that is not the scanned individual's true identity. A further objective of the system is to ensure no security alarms are raised based on the scanned individual's true identity or alias identity.

Overview of Operation

The biometric authentication system, like a normal one, obtains authentication data and analyzes it. Unlike a normal one, however, it attempts to identify a biometric pattern exception. If the system doesn't detect a biometric pattern exception, the biometric authentication system performs processing as normal. This may include identifying the true identity of the scanned individual, presenting the true identity of the scanned individual as the identity of the scanned individual to a security officer, and/or raising a security alarm based on the identified true identity.

If, however, the biometric authentication system does detect a biometric pattern exception, the system will perform specialized processing. This specialized processing includes further analyzing the biometric authentication data for hidden data, and identifying the hidden data. The identified hidden data is then used to either: i) generate a set of biometric, authentication, or identity information that is not the true identity of the scanned individual (ie, an alias); or ii) if a preferred alias is already within the biometric authentication system (for instance a database of individuals), the system may merely map the hidden data to an already-existing alias identity or credential. The system may also ensure that no security alarms are triggered based on the scanned individual's true identity or alias identity by overriding software functions that trigger such alarms.

Biometric Spoofing

Biometric spoofing is presenting biometric information to the biometric authentication system that is not the true biometric information of the scanned individual. Biometric spoofing items may be used to present this information to the system discreetly, so that no individuals are aware of the spoofing except for the scanned individual. A biometric spoofing item would be used for carrying the biometric pattern exception and embedded hidden data. This may be a removable biometric spoofing item, such that the scanned individual can easily dispose of it, and so that the individual's true biometric information is not accidentally read. Ideally, such spoofing may be done so that it is not identifiable as a spoofing item to a security officer that is visually inspecting the biometric spoofing item or the scanned individual without aid of a computing device.

For instance, the spoofing item may be a fingerprint or iris representation, one that appears as an actual and true fingerprint or iris upon visual inspection. These may be implemented as a contact lens situated on the center of the scanned individual's eyeball, or a fingerprint gel mold that situates on the tip of one's finger.

The biometric spoofing item may contain both the biometric pattern exception and hidden embedded data. Multiple individuals may be able to use the same biometric pattern exception. There may be only one pattern exception used by the system, and thus all individuals wishing to trigger the authentication exemption may have to use a biometric spoofing item with the single pattern exception. The biometric spoofing item may further contain hidden and embedded data. This hidden embedded data may be used to identify a particular alias. The hidden data may just contain only enough data needed to map the authentication data to a particular alias identity already existing within the system. Alternatively, the hidden embedded data may contain all information necessary to create an alias identity within the system.

This enables a single individual to use a first biometric spoofing item containing a first biometric pattern exception and first embedded data to be identified as a first alias identity by the biometric system. And then enables the same single individual to use a second biometric spoofing item containing the first biometric pattern exception and second embedded data to be identified as a second alias by the biometric authentication system.

Biometric Pattern Exceptions

The biometric pattern exception is used to discreetly identify scanned individuals who are exempt from certain authentication processing. The biometric pattern exception is preferably not something that would trigger in any non-exempt scanned individuals by accident. This prevents a normal, non-exempt individual that is not intended for biometric authentication exemption from accidentally triggering the specialized exemption processing. That is, the biometric pattern exception should contain data that no potential scanned individual would possibly have. Such a pattern may be authentication data that is impossible for a human to have. In the case of a fingerprint or iris representation, it may be a representation that (upon being scanned) results in authentication data but cannot possibly be a real human's fingerprint or iris. This may be a particular pigmentation, absolute orientation, size, color, or relative

orientation of biometric information such as a fingerprint's mountains and valleys, or iris and pupil boundaries.

The exception pattern may be a microscopic embedded data item, such as a picture image or a known set of data points (for example, a set of microscopic red data points that are oriented in a particular pattern with respect to each other). Absolute orientation or location of the exception pattern is preferably not used during identification, as the scanned individual is unlikely to orient the biometric spoofing item exactly the same way with every use. Instead, relative orientation of multiple sub-patterns, or merely the existence of an obscure pattern, may be used to confirm the existence of the pattern exception.

Alternatively the exception pattern may just include some individual's true authentication data (perhaps a third party, or the scanned individual themselves), but the spoofing item would also include embedded hidden data. Such true authentication data used as an exception pattern would enable a user to wear a clear or non-altering biometric spoofing item (for example, a contact lens that does not obscure iris readings) but includes hidden embedded data somewhere not in the standard scanning spectrum (contains hidden data points outside the iris).

Hidden Embedded Data

The hidden embedded data contained within the biometric spoofing item can be used to dynamically select a particular alias for the scanned individual. The alias identified by the biometric authentication system is then presented to a security officer operating the biometric authentication system in a normal fashion and as the true identity of the scanned individual. The embedded hidden data, once obtained, may be mapped to an alias already existing within the biometric authentication system. Alternatively, the embedded hidden data may contain all the information necessary to create a full alias identity. In either case the biometric authentication system would ensure no security alarms are associated with the identity to be presented as the scanned individual's true identity.

The hidden embedded data may be matched to a particular identity already within the system. Normally, the biometric authentication system reads biometric authentication data, analyzes the biometric authentication data, and maps the biometric authentication data to a particular identity within the system. After mapping to a particular identity, the system presents the particular identity as the true identity to an operator of the system, such as a security officer.

Sometimes the identity is merely passed to another computing system to perform automated background or criminal checks and no security officer is involved. In the instant system, in one embodiment, the hidden embedded data would be mapped to a particular identity that is not the true identity of the scanned individual. This particular identity would then be presented as the true identity of the scanned individual to either a security officer or further verification computing systems.

Therefore, to a security officer, or administrator of further computing systems, this biometric authentication exemption appears as a normal authentication and an identification of the true identity of the scanned individual.

An exemplary method for operation of the system:

A method comprising:

obtaining biometric authentication data of a scanned individual from a biometric scanning device;

analyzing the obtained biometric authentication data;

determining whether a biometric pattern exception exists based on the analyzed biometric authentication data; wherein determining whether the biometric pattern exception exists includes identifying a predetermined data set from within the biometric authentication data;

in response to determining the biometric pattern exception does not exist, performing biometric authentication as normal including presenting the true identity of the scanned individual as the scanned individual's identity;

in response to determining the biometric pattern exception does exist, performing a biometric authentication exemption including:

identifying hidden data within the biometric authentication data;

identifying, based on the hidden data, an alias that is not the true identity of the scanned individual;

presenting the identified alias as the scanned individual's identity;

if necessary, suppressing any security alarms related to the identified alias or the scanned individual's true identity.