October 17, 2019

Hyperspectral Data Fusion for Multifactor Face-Based Authentication

Sean Korphi

Vincent Mei

Hyperspectral Data Fusion for Multifactor Face-Based Authentication

Abstract:

This publication describes systems and techniques directed to hyperspectral data fusion for multifactor face-based authentication. The described systems and techniques include a user equipment with electromagnetic wave modules for emitting and/or sensing multiple spectrums of electromagnetic waves. Based on hyperspectral data associated with electromagnetic waves reflected from the face of a person, a data fusion manager application of the user equipment performs computations to authenticate the person. The hyperspectral data is, in effect, a multifactor face-based authentication key.

Keywords:

hyperspectral data fusion, multi-spectral data fusion, face authentication, radar facial-recognition, infrared facial-recognition, visual facial-recognition, electromagnetic waves, radiated energy facial-recognition, face authentication, biometric data, facial feature, image fusion

Background:

Facial authentication techniques are commonly used for security purposes. For instance, a visual camera (*e.g.*, an image sensor) of a laptop computer may sense electromagnetic waves reflected from a person's face to capture an image of the person's face. In this instance, the electromagnetic (EM) waves are within the visual spectrum of the electromagnetic spectrum (*e.g.*, EM waves of a wavelength (λ) in millimeters (mm) that range between $0.0004 \text{ mm} < \lambda < 0.0008$ mm). A security application executing on the laptop computer may then compare the captured image with a stored image for authentication purposes. If the captured image and the stored image "match," the security application may unlock the computer for access.

Description:

This publication describes systems and techniques directed to hyperspectral data fusion for multifactor face-based authentication. The described systems and techniques include a user equipment with EM wave modules for emitting and/or sensing multiple spectrums of electromagnetic waves. Based on hyperspectral data associated with electromagnetic waves reflected from the face of a person, a data fusion manager application of the user equipment performs computations to authenticate the person. The hyperspectral data is, in effect, a multifactor face-based authentication key.

FIG. 1, below, illustrates an example user equipment that supports techniques directed to hyperspectral data fusion.

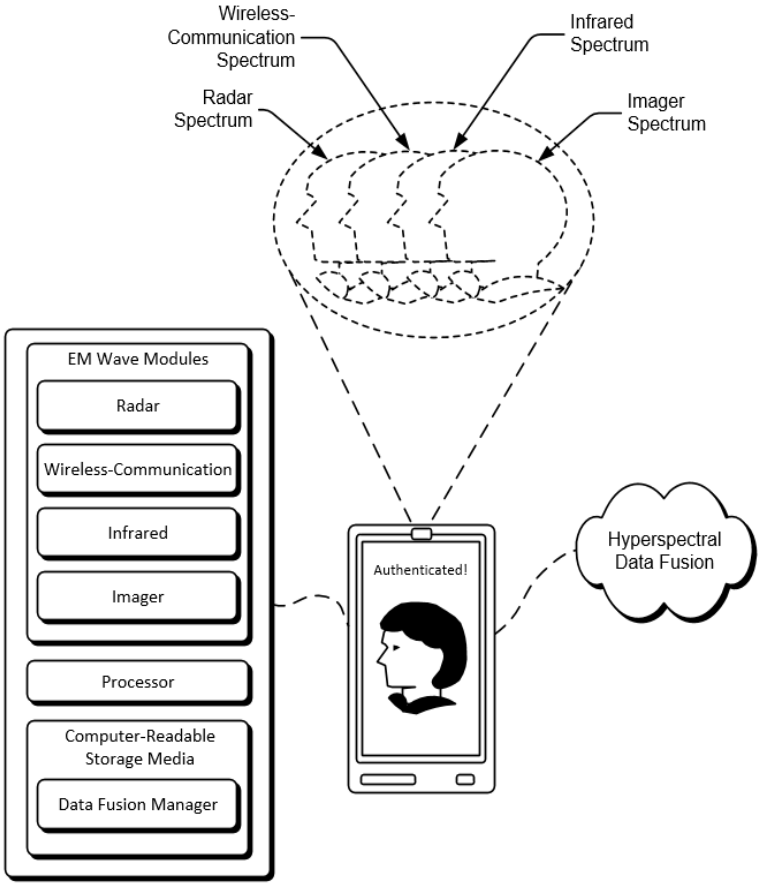

FIG. 1

Although illustrated as a smartphone, the user equipment can be any apparatus device having similar features (*e.g.*, a laptop computer, a home security system, a tablet, an internet-of-things (IoT) device, an automobile). The user equipment includes multiple electromagnetic (EM) wave modules for emitting and/or sensing electromagnetic waves across multiple spectrums of the electromagnetic spectrum. The emitting and/or sensing of the electromagnetic waves, in some instances, can be a combination of active interrogation and passive radiometry. The user equipment includes a radar module (*e.g.*, a module for emitting and sensing electromagnetic waves ranging between 4 mm $< \lambda <$ 6 mm) and a wireless-communication module (*e.g.*, a Fifth-Generation New Radio (5GNR) wireless-communication module for emitting and sensing mmWaves (*e.g.*, electromagnetic waves ranging between 1 mm $< \lambda <$ 10 mm). The user equipment also includes an infrared module (*e.g.*, a module for emitting and sensing electromagnetic waves ranging between 0.01 mm $< \lambda <$ 1 mm) and an imager module (*e.g.*, a module that includes a charge-coupled device (CCD) or complementary metal-oxide semiconductor (CMOS) image sensor for sensing visual, electromagnetic waves ranging between 0.0004 mm $< \lambda <$ 0.0008 mm).

The modules of the user equipment may be "native" to the user equipment and incorporated into the user equipment for purposes other than face-based authentication (*e.g.*, the wireless-communication module may be included for the purpose of communicating with a base station of a cellular network). Although the described modules are associated to select electromagnetic spectrums, it is important to note that the described modules are by way of example only.

The user equipment also includes a processor and a computer-readable storage media including executable instructions of a data fusion manager application. When executed by the processor of the user equipment, the data fusion manager application may cause the user equipment to perform a series of operations, including emitting electromagnetic waves (*e.g.*, scattering, using

one or more of the EM wave modules, multiple spectrums of electromagnetic waves in the direction of a person's face) and collecting hyperspectral data (*e.g.*, detecting, using one or more of the EM wave modules, data associated with the multiple spectrums of electromagnetic waves reflected from the person's face).

In the context of the illustrated user equipment of FIG. 1, collecting the hyperspectral data includes collecting data associated with reflected electromagnetic waves associated with the radar spectrum, the wireless-communication spectrum, the infrared spectrum, and the imager spectrum. The data fusion manager application (being executed by the processor) may then perform hyperspectral data fusion computations for authentication purposes.

FIG. 2, below, illustrates an example of hyperspectral data fusion computations. The example hyperspectral data fusion computations may be performed by the processor of the user equipment executing the instructions of the data fusion manager application.

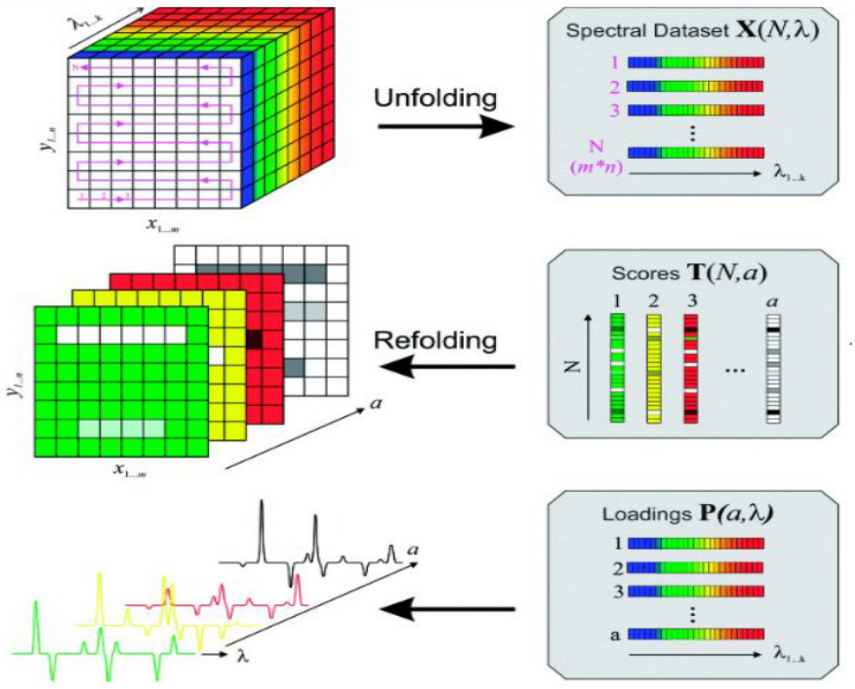

FIG. 2

As illustrated, the hyperspectral data fusion computations rely on hyperspectral data configured in a cubical fashion. The hyperspectral data includes data that is indicative of magnitudes and/or distortions that may be present in reflected electromagnetic waves collected across a reference two-dimensional plane (*e.g.*, an x-y plane) corresponding to respective, reflected electromagnetic wave images of the person's face. As illustrated, the hyperspectral data (*e.g.*, data of the respective, reflected electromagnetic wave images) is arranged in a fashion that is segmented by wavelengths (*e.g.*, wavelengths corresponding to the radar spectrum, the wireless-communication spectrum, the infrared spectrum, the imager spectrum).

The hyperspectral data fusion computations, using principal component analysis (PCA) techniques, can include "unfolding" the respective, reflected electromagnetic wave images to yield a spectral dataset, "refolding" the spectral data set in a series according to computed image scores, and computing loading vectors for the series of images included in the refolded spectral data set. Algorithms supporting the hyperspectral data fusion computations may, in effect, use the hyperspectral data as an authentication key (*e.g.*, verifying the set of loading vectors computed from the hyperspectral data against an expected or stored set of loading vectors). The algorithms may reside in the data fusion manager application of FIG. 1 and, in some instances, evolve using machine learning techniques (*e.g.*, the algorithms may be machine-learned algorithms).

Hyperspectral data fusion computations, as described above, provide a foundation for multifactor face-based authentication techniques having advantages over visual face-based authentication techniques. For example, computations that include electromagnetic waves of the radar spectrum are immune to the effects of visual changes to a person's face that may result from makeup or face painting. As another example, computations that include electromagnetic waves

of the wireless-communication spectrum (*e.g.*, mmWave) are immune to the effects of visual changes to a person's face that may result from facial hair.

Although the techniques above are described in the context of being performed by a user equipment, the techniques may be modified to include aspects of the techniques being performed by a server or a cloud computing device. As an example, the user equipment may perform operations that are effective to provide the hyperspectral data to a banking service provider that is remote from the user equipment (*e.g.*, a user may "log-in" to their banking account by the user equipment transmitting collected, hyperspectral data of the user's face to a complementary data fusion manager application installed at a server of their banking institution).

In general, the described multifactor face-based authentication techniques can provide added levels of security and reliability over visual face-based authentication techniques. Such techniques can be used to not only simply grant access to a user equipment but may also be used to grant access to one or more applications that may reside on the user equipment or be accessible through the user equipment.

References:

[1] Patent Publication: US20100002912A1. Facial feature evaluation based on eye location. Filing Date: January 10, 2005.

[2] Patent Publication: US20050063566A1. Face imaging system for recordal and automated identity confirmation. Filing Date: October 17, 2002.