

**PERSISTENT AUTHENTICATION BASED ON ECG, PPG, AND GSR
SENSORS ON THE WRIST**

BACKGROUND

[0001] Authentication of a user's identity involves verifying a user is who he or she represents himself or herself to be or has credentials, typically for accessing data or a service. Authentication is particularly useful in computer security to prevent a user from accessing data available via a computer system but for which the user does not have access permission. Biometric authentication techniques may be used. Authentication may be desired on a continuous basis and in a manner which does not interrupt the user's activity in interfacing with an application, computer system or machine controlled by a computer system. For example, distraction caused by interrupting a user to re-enter a password or put his or her eye to a retinal scanning device while engaged in an activity is to be avoided.

BRIEF DESCRIPTION OF THE DRAWINGS

[0002] Figure 1 is a view of the sensors on the caseback of a smart watch. The PPG sensor is shown in the center. The two metal electrodes can be used as ECG and/or GSR electrodes (some devices will have one while other devices will have both types).

[0003] Figure 2 shows an ECG trace obtained using dry electrodes.

[0004] Figure 3 shows a PPG waveform obtained from the brachial artery.

[0005] Figure 4 shows features extracted from both ECG and PPG signals being compared against features extracted from a reference signal to

authenticate the user.

[0006] Figure 5 depicts ECG features obtained in time domain.

[0007] Figure 6 depicts a comparison of ECG signal with a template using dynamic time warping (generated using Matlab algorithm).

[0008] Figure 7 is a flow chart depicting a sequence of tests to determine if the wearer is authenticated or not.

[0009] Figure 8 is a block diagram of an embodiment of a system from a hardware perspective for authentication of a user based on data representing a wrist vein pattern of the user.

DETAILED DESCRIPTION

[0010] Besides security of computer access and data stored by a computer system, biometric authentication may also come in useful in other contexts to verify someone was at a place or is performing an activity such as exercise. Continuous authentication may also be useful, for example in military or other environments requiring high security or monitoring of activity over time. For example, during operations where exposures to chemical and biological threats are possible, a warfighter wears a Military Oriented Protective Posture (MOPP) suit. To allow the warfighter secure and efficient access to networked workstations, continuous authentication of the warfighter in the MOPP suit is desired. Additionally, a wearable wrist contact sensor device (such as a watch or other device – not limited to a watch) communicating with a base station (e.g., computer, smart phone, tablet, laptop, or other computing device) provides authentication without explicit intervention from a user wearing the

wrist contact sensing device. In another example, a user may be exercising on a machine and his or her wrist contact sensing device continuously authenticates the user based on his or her wrist vein pattern. A pulse reading in a military context may insure the wearer of the device has not been killed and his wrist is being used post mortem. In an exercise or health monitoring situation, the additional pulse data can verify a health state of the user based on stored pulse data patterns representing various conditions or stored rules about changes reflected in the data.

[0011] The wrist is the carpus or joint between the forearm and the hand. Eight bones of the carpus and the distal ends of the radius and ulna form a complex articulation that allows three degrees of freedom. In order to provide the articulation while maintaining relative stability, the wrist has a complex configuration of ligaments linking the bones. The wrist also had a readily identifiable neurovascular structure. The primary pulsatile components in the wrist are the radial and ulnar arteries.

[0012] The skin area of the wrist is sufficiently planar or flat so that sensors can be arranged in a planar or nearly planar configuration.

[0013] Technology is described for persistently authenticating a user. The system automatically and continuously determines whether the user is wearing a wrist contact sensor device, automatically (and sometimes continuously) senses and registers ECG and PPG data, determines whether the registered ECG and PPG data matches pre-stored data and, if the registered ECG and PPG data matches the pre-stored data and the user is wearing the wrist contact sensor device, concludes that the user is authenticated. When the user takes off the sensor device, the user is no longer authenticated.

[0014] The wrist based authentication system is based on the sensors used for multiparameter activity and wellness monitoring. The current design will

allow the persistent authentication feature based on detecting unique features of a subject's ECG and PPG signals in conjunction with a reliable, redundant detection of the removal of the device from the wrist.

[0015] PPG is photoplethysmography. It uses light to detect pulse.

[0016] ECG is electrocardiography.

[0017] GSR is galvanic skin response. It measures level of perspiration.

[0018] Figure 1 illustrates an embodiment of a wrist wearable device including one or more skin contact sensors positioned by a wristband 101 or wrist strap to contact the user's skin on a palmar side of a user's wrist. The wristband acts as a support structure positioning the wrist contact sensor device against the skin on the palmar side of a user's wrist. In other examples, the support structure may be a bracelet. In some examples, the wrist strap or wristband may include wrist contact sensor device as well as being part of a watch. A support structure or housing of the device, e.g. a plastic support structure, supports the sensor(s) and illuminators and provides a conduit for their electrical circuitry. In some embodiments, a slight curvature of the sensor was designed based on a 3D model of various wrists.

[0019] Figure 1 shows a view of the sensors on the caseback of a smart watch. The PPG sensor is shown in the center. The two metal electrodes can be used as ECG and/or GSR electrodes. The ECG and PPG sensors are used to verify the identity of the individual. The PPG, ECG and GSR sensors are used to reliably, and redundantly detect the removal of the device from the wrist.

[0020] An example of an ECG trace obtained from dry electrodes is shown in Figure 2. The ECG trace provides several unique features that can be compared in both the time and frequency domains.

[0021] An example of a PPG trace (obtained from the brachial artery) is shown in Figure 3.

[0022] During normal operation of the authentication device, the individual wears the device on the wrist(s) and registers the ECG and PPG parameters. For example, the one or more sensors sense ECG and PPG data. This is done by the individual placing a finger on the exposed electrode. During this authentication session, the ECG and PPG signals are obtained simultaneously. The signals are processed and the features extracted from the signals are compared with a secure template (obtained during the enrollment phase) in both time and frequency domains. Additionally, the characteristic phase delay between the ECG and PPG signals are compared.

[0023] The template is obtained during a secure enrollment session during which the user registers the PPG and ECG signals. During the enrollment, the biometric information is recorded and stored. During authentication, the detected biometric information is compared with the stored data.

[0024] Figure 4 illustrates the architecture for extracting the features from both the ECG and PPG signals in both the time and frequency domains. Features extracted from both ECG and PPG signals are compared against features extracted from a reference signal to authenticate the user.

[0025] Some examples of ECG morphological features obtained in the time domain is shown in Figure 5. To extract the time domain morphological features, fiducial points are detected first. Features such as P duration, P amplitude, QRS duration, QRS amplitude, T duration, T amplitude are detected.

[0026] In addition to the morphological features that is found within the R to R interval, there are other features that can be found in the patterns of consecutive heart beats.

[0027] Frequency domain features can be obtained from techniques such as wavelet decomposition, Fourier transformation, or discrete cosine transform.

[0028] Figure 5: ECG features obtained in time domain.

[0029] One example of the comparison of the ECG signal with the template in the time domain is shown in Figure 6. In this example, one cycle of the R to R ECG signal is compared with an R to R ECG template. Dynamic time warping is used to obtain a metric for the closeness of fit between the measured signal and the template.

[0030] One aspect of the authentication system is automatic and periodic (or continuous) detection of the device being worn on the wrist. When the device is removed from the wrist, the signal from the PPG detector is measurably different from when the device is on the wrist. Additionally, when the device is removed from the wrist, the GSR will detect an open circuit since the contact with the skin (with low, but measurable conductivity) is lost. The ECG circuit also detects a characteristic signal when the caseback electrode is not in contact with the skin.

[0031] The persistent authentication system relies on the device continuously being on the wrist after the authentication is made. This allows the device to declare that the wearer's identity is validated. A fail-safe, redundant method of detecting the removal of the device from the wrist is therefore, a key element of the technology. When the device is removed from the wrist, the device will no longer declare authentication or validation of identity. To establish authentication, the device needs to be placed on the wrist and the validation measurements needs to be taken.

[0032] For more critical authentication or identity validation applications, the system can request the user to provide real time ECG and PPG signals during the time of the transaction. The sequence for determining if the wearer is

authenticated or not is shown in Figure 7.

[0033] The wrist-based persistent authentication has a large number of applications. One benefit is that we have irrefutable authentication of the identity of the owner of the token (electronic key). Some additional benefits are (1) enabling of transactions: Transactions based on 2D barcode, NFC, BLE, or other means of communication can be enabled based on the authentication of the wearer; (2) Validation of exercises: Authentication allows verification of the wearer and thus provides evidence that the person receiving the credit for the exercise (e.g. for health insurance or corporate wellness programs) is the authorized person; (3) Access to devices and appliances: Access to laptops, phones, workstation, etc . can be based on persistent authentication; and (4) Access to restricted areas: The addition of persistent authentication to a token (e.g. RFID) provides additional level of security, ensuring that that only the authorized and designated of the token accesses the restricted area. This could be used for secured areas but could also be used for access to paid facilities.

[0034] Figure 8 illustrates an example system embodiment in which a wrist contact sensor device is communicatively coupled to a computer system (301, 314) over a communication network. In this example, the wrist contact sensor device 201 is networked via a wireless communication link to a base station 301 computer system. In other examples, a wire may connect the wrist contact sensor device 201 and a base station. For example, a contact sensor device 201 may be wired to a base station controlling access to a room or other device. This system embodiment and other system embodiments described below may be used for one-time authentication or for continuous authentication during user activity.

[0035] In other examples, a radio communication range between a wearable wrist contact sensor device 201 and the base station 301 may be engineered to provide a well defined region of operation. Since the wearable device, e.g.

wristband device, is physically bound to the user, the limited radio range of the device 201 ensures that the user is within a secured region around the base station. When the link between the base station and the wearable device is broken, the base station recognizes that the user is absent and notifies one or more applications requesting authentication. For example, an application executing on the base station or a computer system 314 in communication with the base station 301 may cut off access to sensitive data. An identifier token may be used to establish a communication link between the contact sensor device 201 and the base station 301.

[0036] In this example, contact device 201 includes a computer system 206 including a processing unit 202 including one or more central processing units (CPU) or microcontrollers and a memory 204 which may include volatile memory 205 (such as RAM), non-volatile memory 907 (such as ROM, flash memory, etc.) or some combination of the two. Additional memory storage 210 (removable and/or non-removable) may also be included on the sensor device for access by the computer system 206. One or more communication module(s) 212 include one or more network interfaces and transceivers which allow the wrist contact sensor device 201 to communicate with other computer systems typically wirelessly but also through wire if a wire interface is included. In some instances, direct memory access (DMA) such as to a buffer in the optional additional memory storage 210 may be supported for an interface of at least one of the communication modules 212. Input devices like a touch screen and buttons on a watch display also attached to a wearable support structure positioning the wrist contact sensor device 201 and output devices 209 like a display on collocated on the same wearable support structure may also communicate with the processing unit 202 and memory 204.

[0037] The wrist contact sensor device 201 also comprises illumination drive circuitry 228 which drives the one or more illuminators 203 with current

or voltage under the control of the processing unit 202. Sensor interface circuitry 218 is coupled to the sensors 220 for converting their analog detection signals to digital data which are stored by the processing unit 202 in memory (205, 207, 210). The processing unit 202 may process the digital data further to be in a format usable by a pattern recognition technique for determining an identity of a user. The processing unit 202 may also monitor the operational status of the illuminators and sensors based on monitoring detected data and component status data received from the sensor interface circuitry 218 and the illumination drive circuitry 228.

[0038] The base station 301 also includes a computer system 306 with a memory 304 which may include volatile 305 and non-volatile 307 memory components. Additional storage 310 is available. Similarly, the base station 301 includes one or more communication module(s) 212 which include one or more network interfaces and transceivers which allow the base station to communicate with the wrist contact sensor device 201 and other computer systems 314 over wire or wirelessly or in both manners. The base station also includes input and output (I/O) devices like a display and buttons, touchscreen or a keypad, pointing device, keyboard or the like.

[0039] To avoid cluttering the drawings, a power supply and power bus or power line is not illustrated, but each of the system embodiments illustrated from a hardware perspective also includes or has access to a power supply and a power bus to which the various components using power connect for drawing power. An example of a power supply are a battery. Larger computer systems such as the base station and other networked computer systems may also have a power cord connection.

[0040] The example computer systems illustrated in the figures include examples of computer readable storage devices. A computer readable storage device is also a processor readable storage device. Such devices may include

volatile and nonvolatile, removable and non-removable memory devices implemented in any method or technology for storage of information such as computer readable instructions, data structures, program modules, software or other data. The software or instructions are used to program one or more processors to perform the methods described above. Some examples of processor or computer readable storage devices are RAM, ROM, EEPROM, cache, flash memory or other memory technology, CD-ROM, digital versatile disks (DVD) or other optical disk storage, memory sticks or cards, magnetic cassettes, magnetic tape, a media drive, a hard disk, magnetic disk storage or other magnetic storage devices, or any other device which can be used to store the information and which can be accessed by a computer.

[0041] Although the subject matter has been described in language specific to structural features and/or methodological acts, it is to be understood that the subject matter defined herein is not necessarily limited to the specific features or acts described above. Rather, the specific features and acts described above are disclosed as example forms of implementing the disclosed technology.

CLAIMS

What is claimed is:

1. A method of persistently authenticating a user based, comprising:
 - (a) performing enrollment to establish and store pre-stored data as a baseline for comparison;
 - (b) automatically sensing and registering ECG and PPG data;
 - (c) determining whether the registered ECG and PPG data matches pre-stored data;
 - (d) if the registered ECG and PPG data matches the pre-stored data, concluding that the user is authenticated and reporting to a client device that the user is authenticated;
 - (e) if the registered ECG and PPG data does not match the pre-stored data, concluding that the user is not authenticated and reporting to a client device that the user is not authenticated;
 - (f) automatically and continuously determining whether the user is wearing a sensing device;
 - (g) if the user has been authenticated and continues to wear the sensing device then concluding that the user is still authenticated and (optionally) reporting to a client device that the user is authenticated;
 - (h) if the user has been authenticated and is detected to stop wearing the sensing device then concluding that the user is not authenticated and reporting to the client device that the user is not authenticated;
 - (i) while the user is continuing to wear the sensing device, repeating steps (f) – (h).

2. A method of persistently authenticating a user based, comprising:

- (a) performing enrollment to establish and store pre-stored data as a baseline for comparison;
- (b) automatically and continuously determining whether the user is wearing a wrist sensing device;
- (c) automatically and continuously sensing and registering ECG and PPG data by the wrist sensing device;
- (d) determining whether the registered ECG and PPG data matches pre-stored data;
- (e) if the registered ECG and PPG data matches the pre-stored data, concluding that the user is authenticated and reporting to a client device that the user is authenticated;
- (f) if the registered ECG and PPG data does not match the pre-stored data, concluding that the user is not authenticated and reporting to a client device that the user is not authenticated;
- (g) while the user is continuing to wear the wrist sensing device, repeating steps (b) – (f).

3. A system for persistent authenticating of a user, comprising:
a wrist contact sensor device comprising one or more sensors for sensing ECG and PPG data, one or more processors local to the one or more sensors for processing the ECG and PPG data and a first transmitter local to the one or more sensors; and

a base station having a second transmitter relatively removed from the one or more sensors;

wherein the system automatically and continuously determines whether the user is wearing a sensing device, automatically senses and registers ECG and PPG data, determines whether the registered ECG and PPG data matches

pre-stored data and, if the registered ECG and PPG data matches the pre-stored data and the user is wearing the wrist contact sensor device, concludes that the user is authenticated.

ABSTRACT

Technology is described for persistently authenticating a user. The system automatically and continuously determines whether the user is wearing a sensing device, automatically senses and registers ECG and PPG data, determines whether the registered ECG and PPG data matches pre-stored data and, if the registered ECG and PPG data matches the pre-stored data and the user is wearing the wrist contact sensor device, concludes that the user is authenticated.

Figure 1

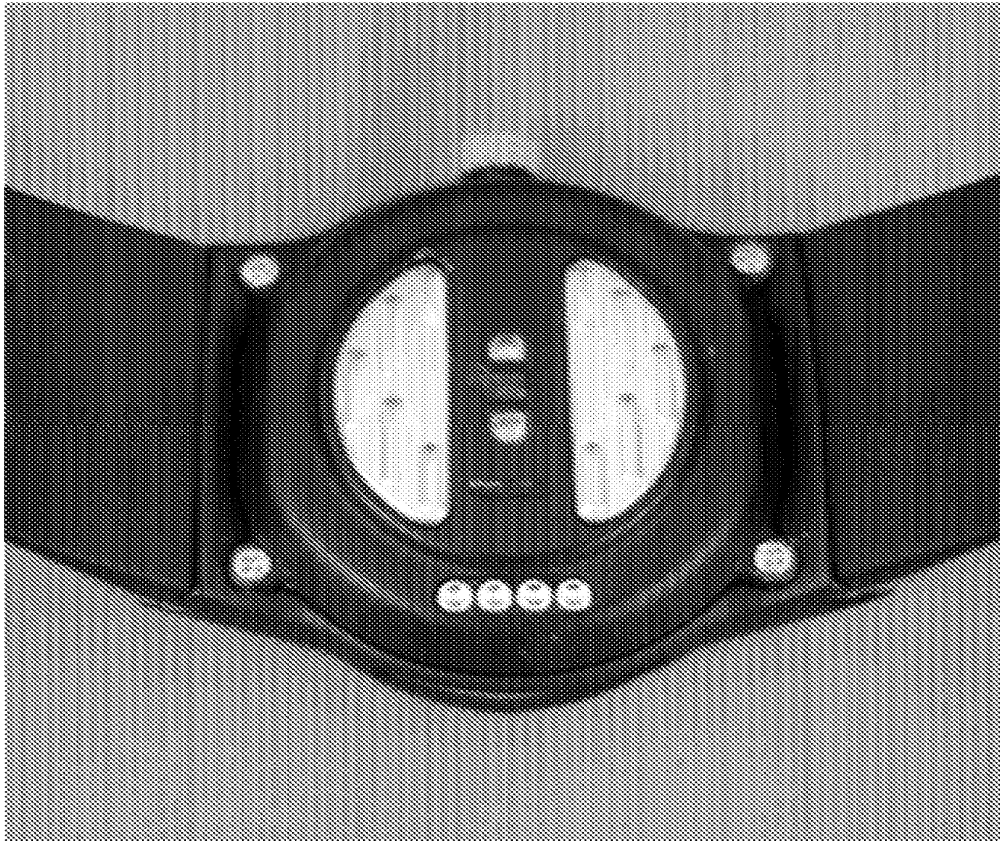


Figure 2

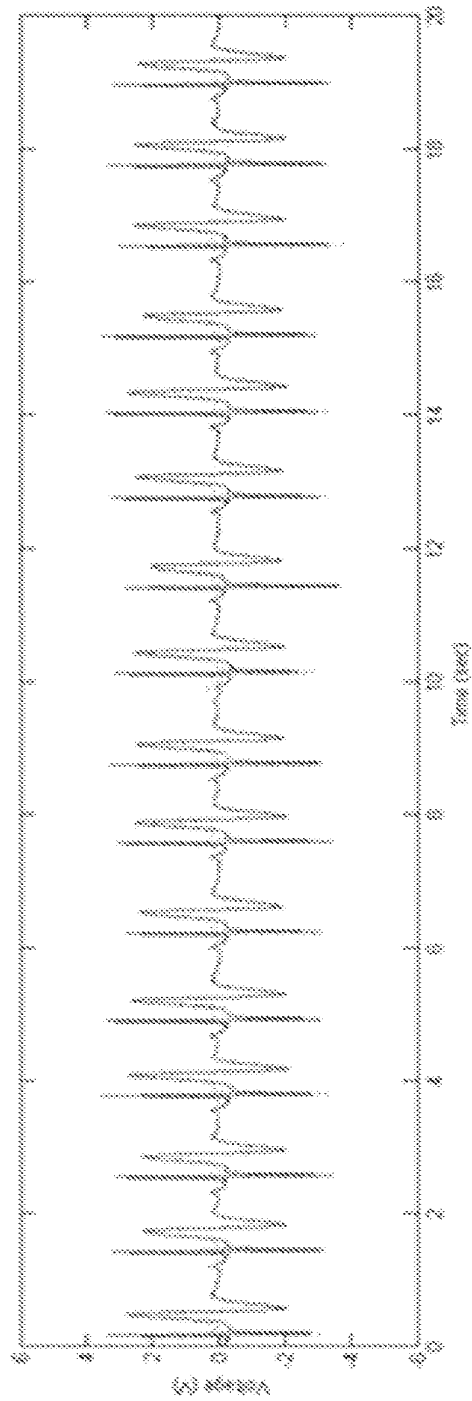


Figure 3

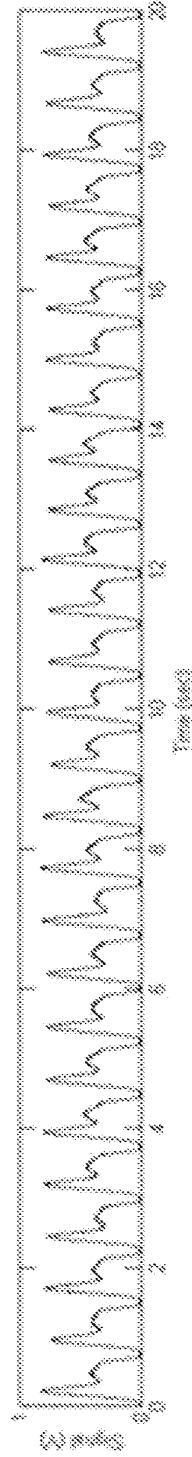


Figure 4

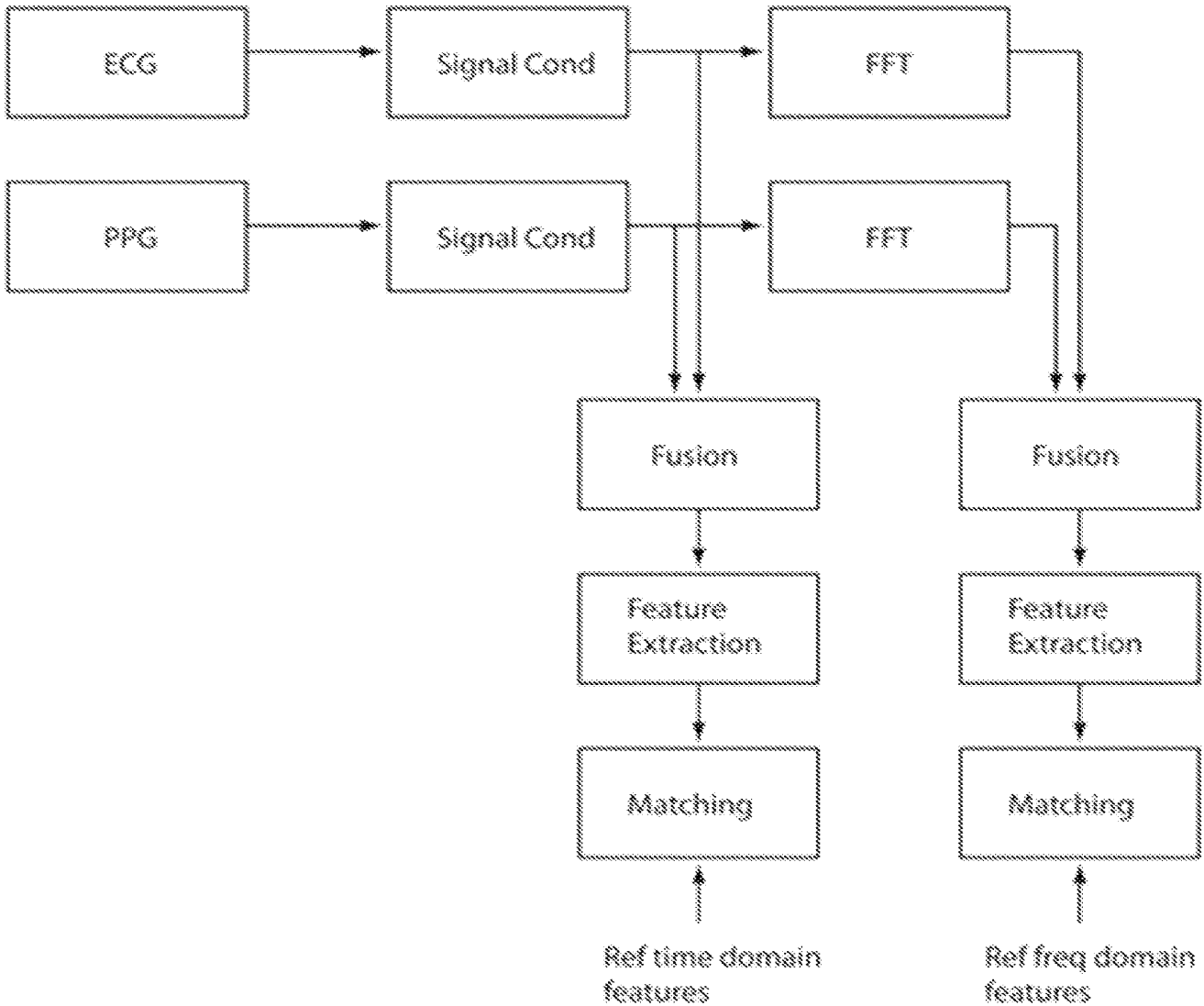


Figure 5

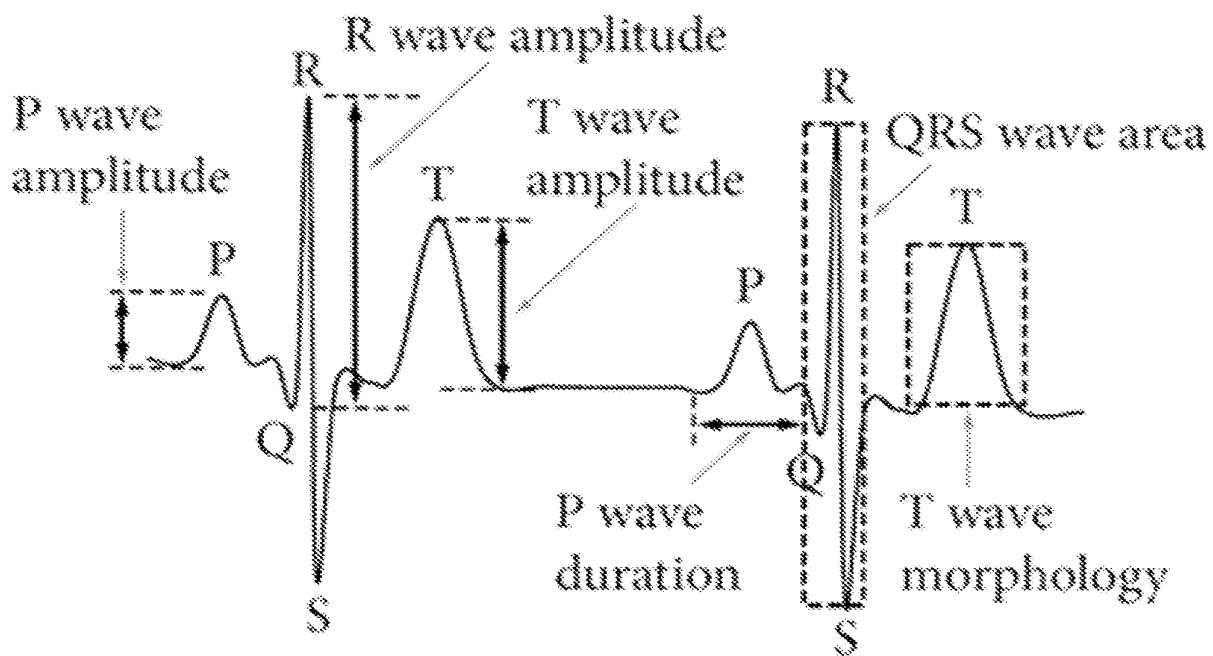


Figure 6

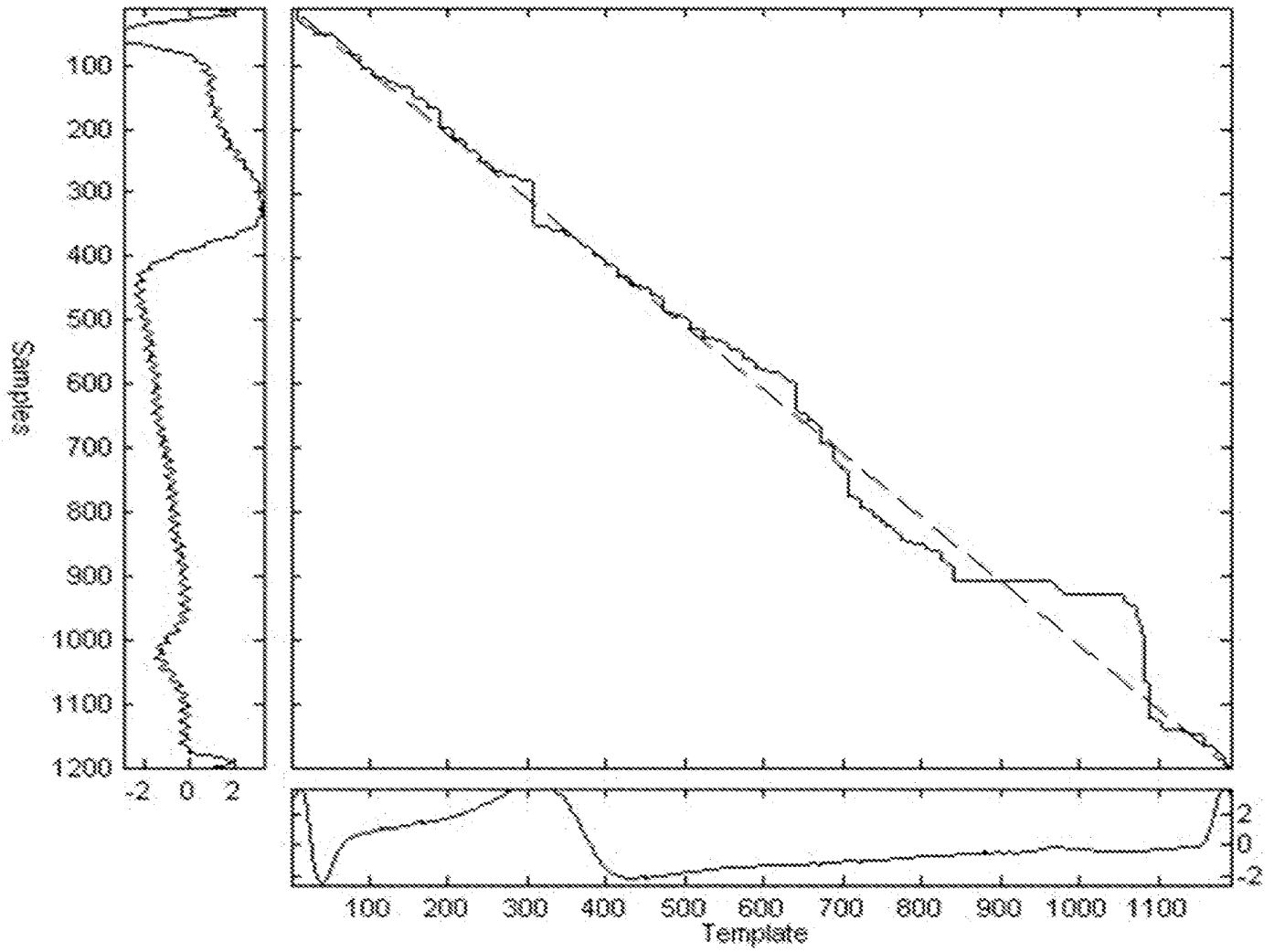


Figure 7

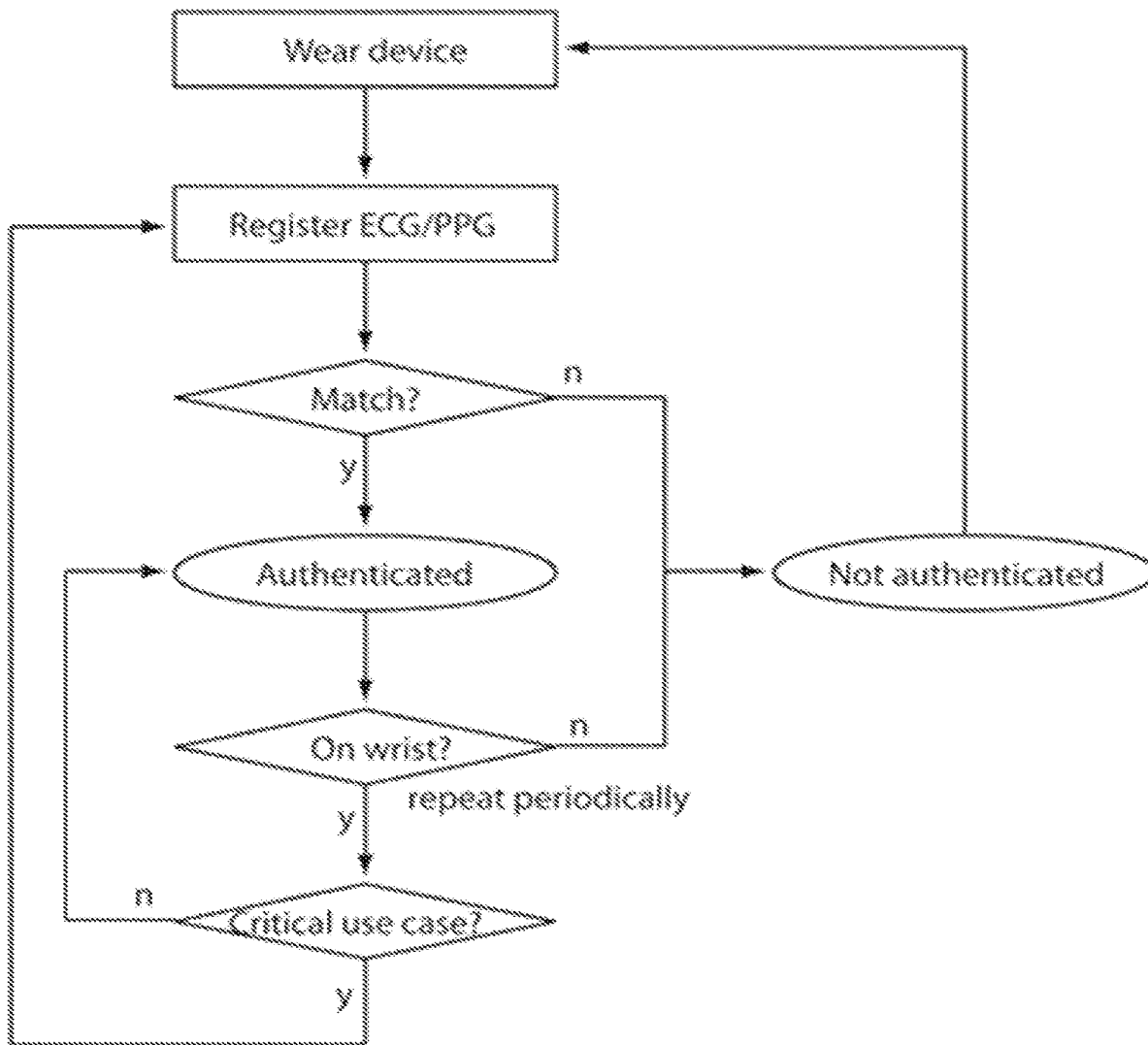


Figure 8

