



US 20160360998A1

(19) **United States**

(12) **Patent Application Publication**
JUN

(10) **Pub. No.: US 2016/0360998 A1**

(43) **Pub. Date: Dec. 15, 2016**

(54) **SYSTEM, TERMINAL, AND METHOD FOR
DIGITAL ELECTROCARDIOGRAM
AUTHENTICATION**

A61B 5/0456 (2006.01)

A61B 5/0408 (2006.01)

A61B 5/04 (2006.01)

(71) Applicant: **Moon-Seog JUN**, Seoul (KR)

(52) **U.S. Cl.**

CPC *A61B 5/117* (2013.01); *A61B 5/04085*

(2013.01); *A61B 5/04012* (2013.01); *A61B*

5/0456 (2013.01); *A61B 5/681* (2013.01)

(72) Inventor: **Moon-Seog JUN**, Seoul (KR)

(21) Appl. No.: **15/178,415**

(22) Filed: **Jun. 9, 2016**

(57)

ABSTRACT

(30) **Foreign Application Priority Data**

Jun. 11, 2015 (KR) 10-2015-0082898

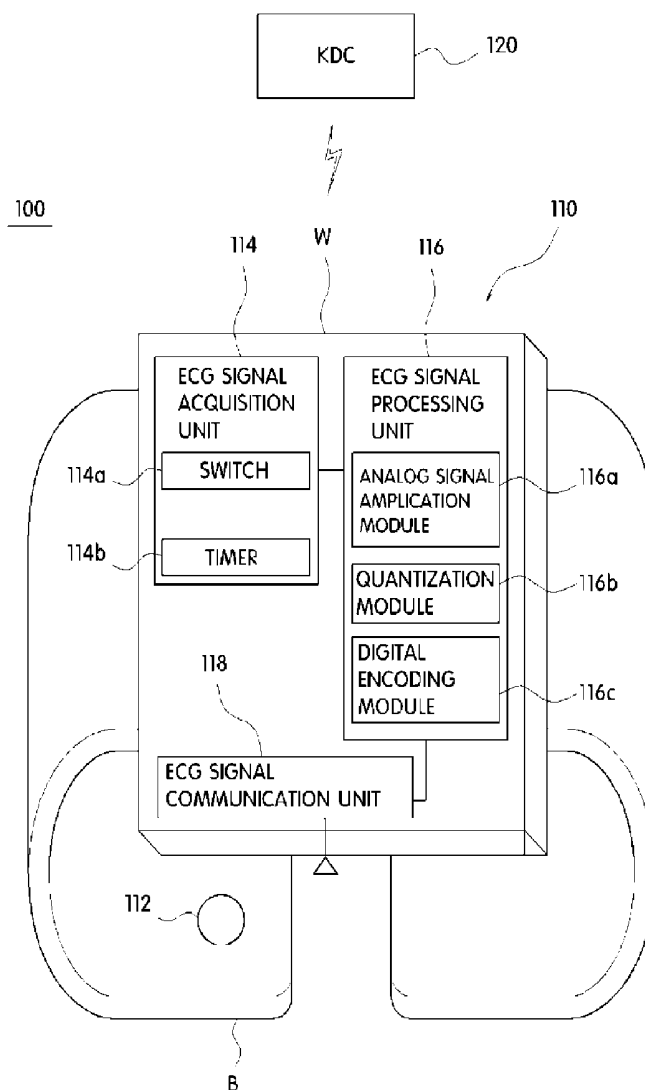
Publication Classification

(51) **Int. Cl.**

A61B 5/117 (2006.01)

A61B 5/00 (2006.01)

Provided is an electrocardiogram (ECG) biometric authentication system that performs biometric authentication using biometric information having unique values for each client includes one or more client terminals and a key distribution center (KDC) that uses ECG information of the one or more client terminals to issue a digital certificate. According to the configuration of the electrocardiogram biometric authentication system, security is enhanced.



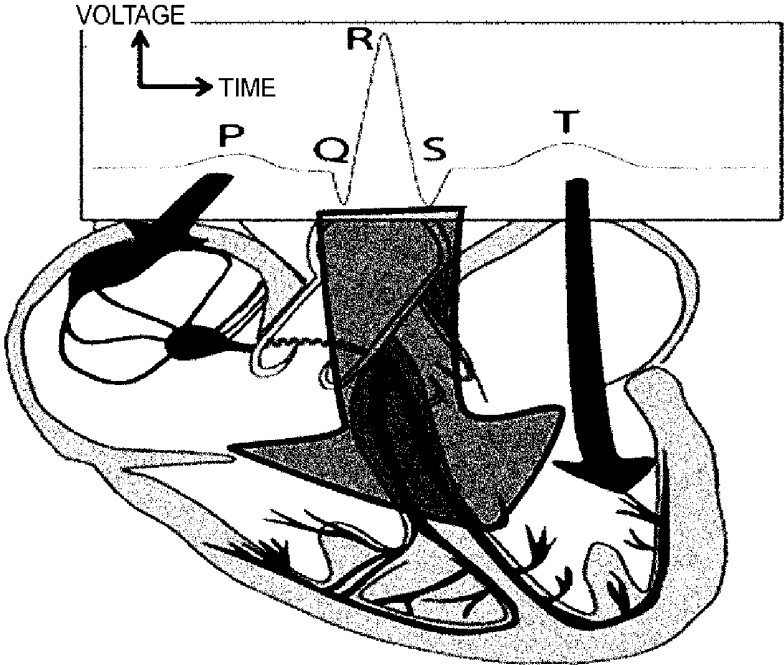


FIG.1

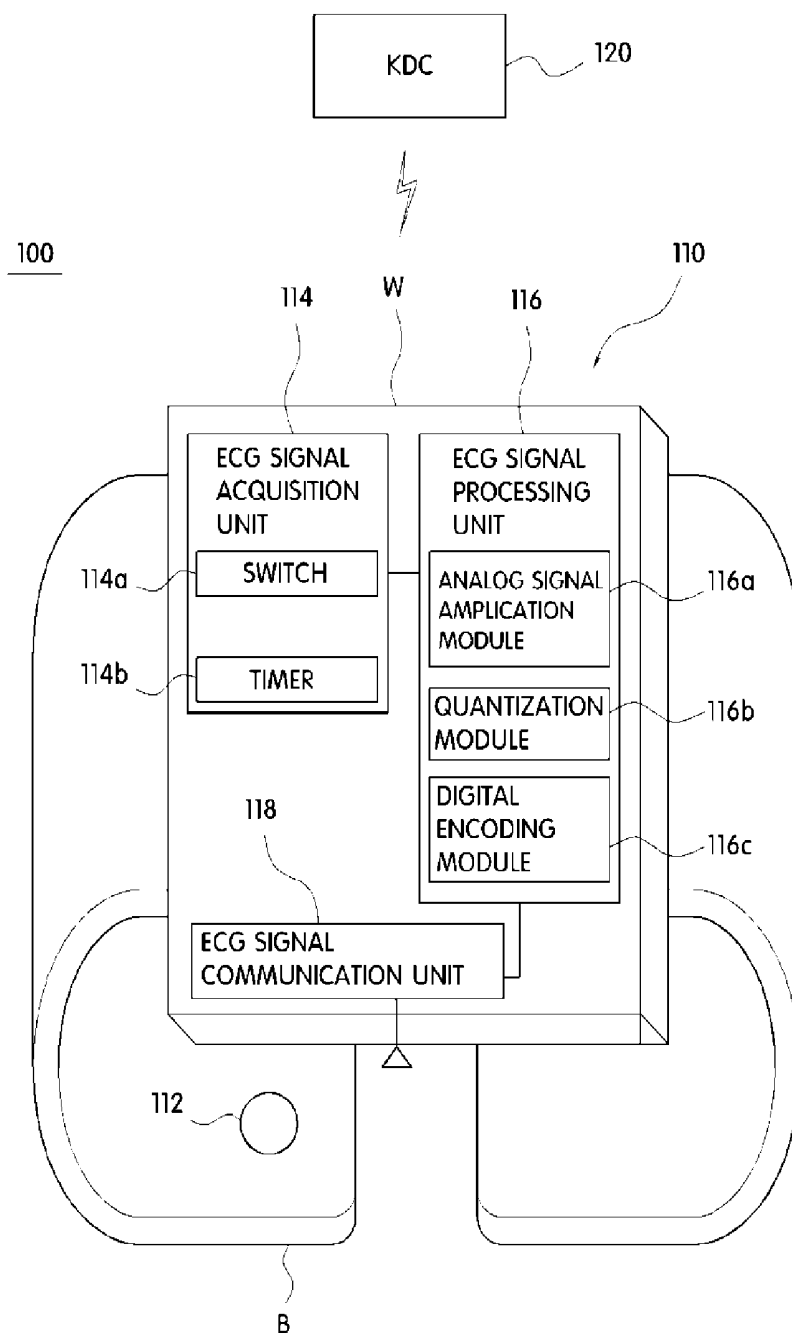


FIG.2

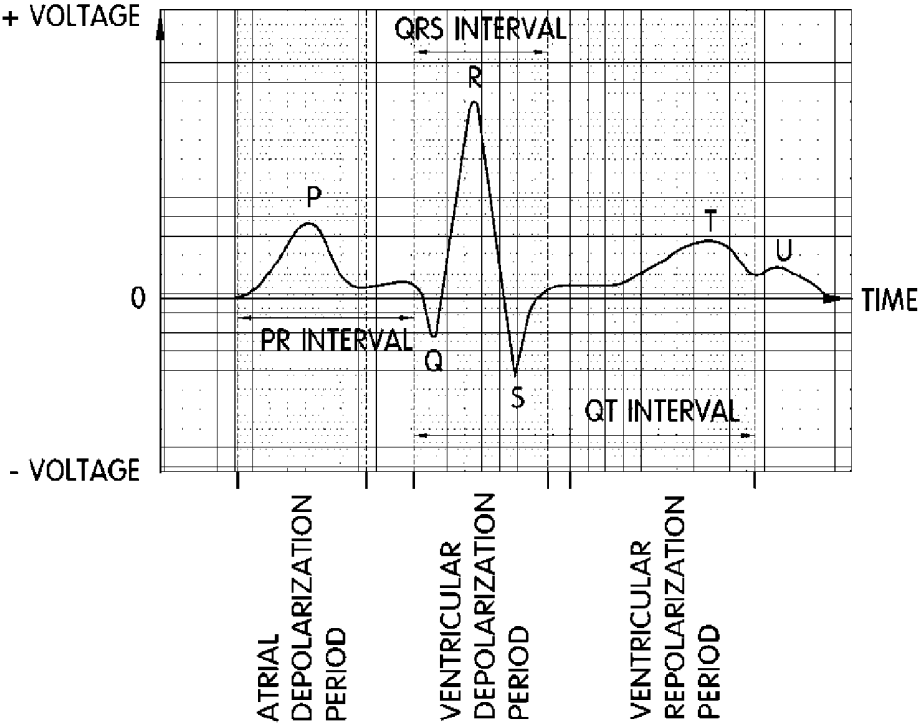


FIG.3

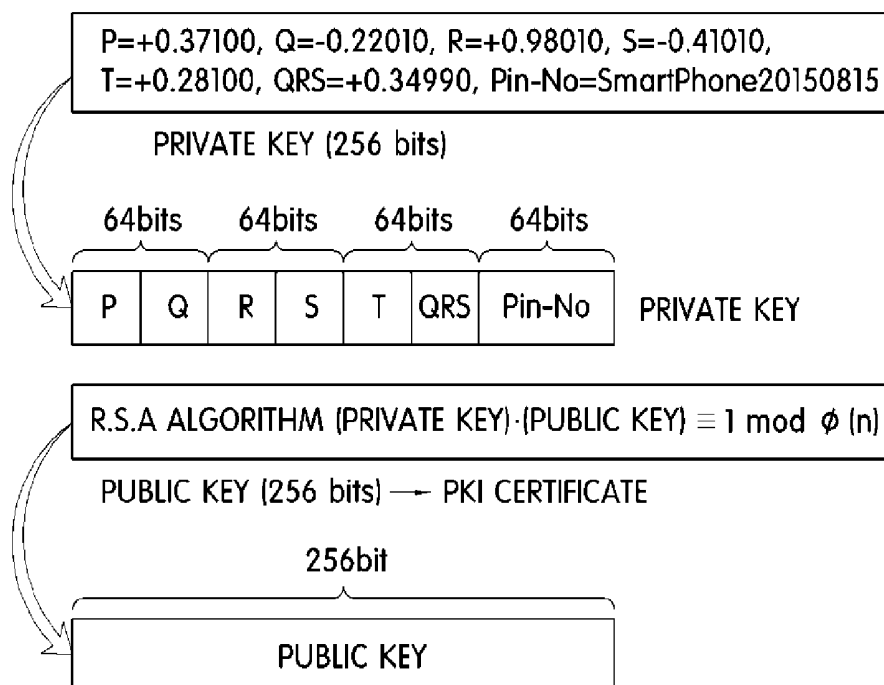


FIG.4

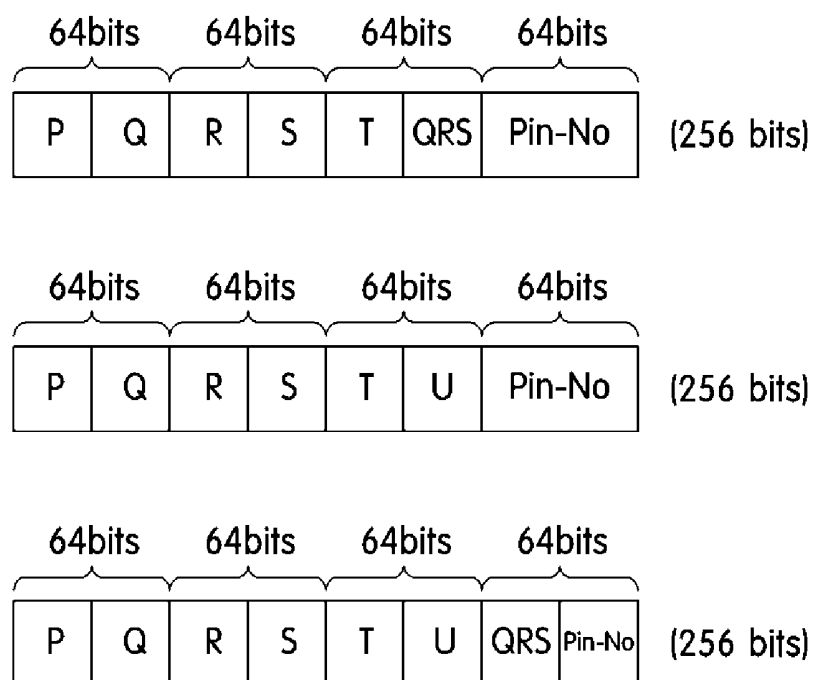


FIG.5

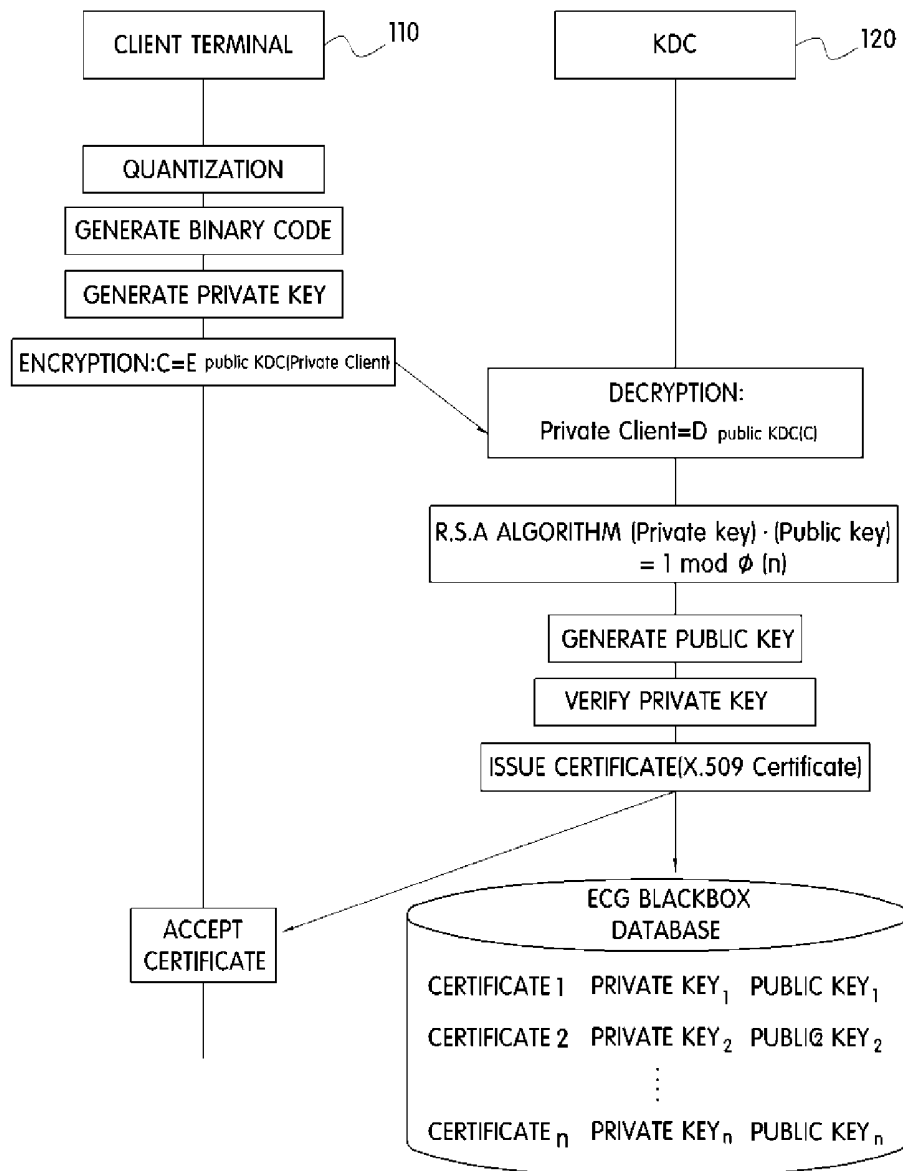


FIG.6

SYSTEM, TERMINAL, AND METHOD FOR DIGITAL ELECTROCARDIOGRAM AUTHENTICATION

CROSS-REFERENCE TO RELATED APPLICATION

[0001] This application claims priority to and the benefit of Korean Patent Application No. 10-2015-0082898, filed on Jun. 11, 2015, the disclosure of which is incorporated herein by reference in its entirety.

BACKGROUND

[0002] 1. Field of the Invention

[0003] The present invention relates to a terminal, system, and method for electrocardiogram (ECG) biometric authentication, and more particularly, to an ECG biometric authentication terminal, a biometric authentication system using the same, and a method thereof in which currents flowing in a body are generated when depolarization and repolarization occurs in an atrium/ventricle of the heart, and changes of the currents are measured and quantized to be converted into a digital binary code to facilitate determining similarities between the currents and improve reliability because similarities can only be determined through an image and a processing method is complex and unreliable when the measured changes of the currents are shown as waveforms on an analog graph such that the present invention provides a client terminal in the form of a smart watch used by coming into contact with a client's skin, changes QRS complex information unique to each individual into a digital code while extracting ECG information, and uses a Rivest-Shamir-Adleman (RSA)/Elliptic Curve Cryptosystem (ECC) algorithm to execute an authentication process by utilizing QRS complex digital ECG information as a private key of an asymmetric cryptographic system in which a public key and the private key form a pair.

[0004] 2. Discussion of Related Art

[0005] Generally, a technology of utilizing various signals or data that can be extracted from a living body to use the signals or data in various types of systems is being advanced. For example, a biometric authentication technology which uses biometric signals or data to construct a security system has recently been coming into the spotlight.

[0006] A biometric authentication technology refers to a technology of authenticating a user by extracting signals or data related to a living body from the user, comparing the signals or data with pre-stored data, and confirming that the user is the user. Since the biometric authentication technology uses unique biometric signals or data of an individual unlike an identification (ID) card or a password, the biometric authentication technology is coming into the spotlight in the security field due to not having concerns of theft or loss and being difficult to forge or falsify.

[0007] In addition, the biometric authentication technology is also applicable in fields such as financial services, communication services, information security, the medical field, public safety management, and electronic commerce. In addition, although inputting a password or drawing a pattern exists as a method for authenticating a user in a portable terminal, a user authentication method using the biometric authentication technology is recently being developed to improve accuracy in authenticating a user.

[0008] Fingerprints, veins, irises, voices, faces, or lines on palms are commonly being utilized in the biometric authentication technology. Particularly, the most common method among biometric authentication methods being applied to security systems is a fingerprint recognition technology. Although fingerprints have been used for a long time as a biometric authentication method due to their characteristics of not changing for a lifetime, there is a problem in which accuracy is degraded when fingerprints are faded or dry or when fingers are stained with foreign substances.

[0009] In addition, a voice recognition technology using information on pitches of sounds according to intonations and speaking habits exist as a biometric authentication technology. Although the voice recognition technology has advantages of being able to authenticate a user even from a remote place and not requiring separate training related to a method of use, there is a disadvantage of having difficulty in authentication in a case of a hoarse throat due to cold and the like, and there is also a problem in which accuracy of authentication is degraded when others imitate a user's voice or background noise is high.

[0010] Consequently, a technology of recognizing a living body using electrocardiograms (ECGs) among biometric signals is recently being developed to solve the above problems of the biometric authentication technology.

[0011] In FIG. 1, ECG analog signals that represent normal heartbeats and electrical signals generated as a result of the heartbeats are displayed using P, QRS, T, and U waveforms.

[0012] An ECG refers to a record of electrical signals generated in the heart. A part referred to as "sinoauricular node" is present in the heart. The sinoauricular node is a particular part of the heart that controls heartbeats by cyclically generating electricity and inducing contraction of the heart.

[0013] Electrical signals generated from the sinoauricular node are transmitted throughout the heart along an electrical conduction system in the heart. Cells that form heart muscles contract due to the electrical signals transmitted to each part of the heart and cause the heart to beat. Here, a record of the electrical signals transmitted to the heart measured using electrodes attached to skin is referred to as the ECG. Electrodes are attached to various parts of the body, and an electrical phenomenon in each part of the heart can be understood well through the electrodes.

[0014] The biometric authentication technology using an ECG can be utilized in a security technology. That is, the biometric authentication technology using an ECG can be utilized as a technology for authenticating a user by extracting ECG signals from the user and comparing the extracted ECG signals with pre-stored ECG signals of a registered user. However, in this case, high accuracy of authentication is required to utilize ECG signals in user authentication and security technologies. A method of determining similarities between the extracted ECG signals of the user and the pre-stored ECG signals of the registered user is important for improving the accuracy of authentication. That is, accuracy of a method for determining similarities between the signals needs to be improved to use an ECG in a user authentication technology.

[0015] Conventionally, although image patterns have been extracted from analog ECG waveforms and the patterns have been compared to use an ECG in an authentication

technology, this is unreliable since there are frequent errors in determining the similarities by comparing the image patterns.

[0016] Particularly, biometric authentication using image patterns is very insecure due to being replicable.

SUMMARY OF THE INVENTION

[0017] Consequently, the present invention has been devised to solve the above problems of the related art. A heart sends out a small amount of action currents every time it contracts, and an electrocardiogram (ECG) is a recording of electrical changes generated due to heartbeats on a body surface as waveform curves using an electrocardiograph as illustrated in FIG. 1. Since ECG measurement can be conveniently performed through the body surface, and the result provides a large amount of information on heart activity as well as being unique to each individual, it is an aspect of the present invention to provide an ECG biometric authentication terminal utilized in biometric authentication for confirming a client, a biometric authentication system using the same, and a method thereof.

[0018] It is another aspect of the present invention to provide an ECG biometric authentication terminal capable of confirming a client in real-time by grafting ECG measurement and processing technologies onto a smart device used by coming into contact with a client's body surface at all times or as needed, a biometric authentication system using the same, and a method thereof.

[0019] It is yet another aspect of the present invention to provide an ECG biometric authentication terminal that uses a Rivest-Shamir-Adleman (RSA)/Elliptic Curve Cryptosystem (ECC) algorithm to enhance security by utilizing a client's ECG information as a private key of an asymmetric cryptographic system in which a public key and the private key form a pair, a biometric authentication system using the same, and a method thereof.

[0020] To achieve objectives mentioned above, according to an aspect of the present invention, an ECG biometric authentication system of the present invention which is a biometric authentication system that performs biometric authentication using cyclical biometric voltage information having unique values for each client includes one or more client terminals and a key distribution center (KDC) that uses ECG information of the one or more client terminals to issue a digital certificate.

[0021] According to another aspect of the present invention, an ECG biometric authentication terminal of the present invention includes a smart band that surrounds a client's wrist, has one or more biometric electrodes coming into contact with skin of the wrist embedded therein, and detects analog ECG electrical signals through the one or more biometric electrodes, and a smart watch electrically connected to the one or more biometric electrodes to collect the analog ECG electrical signals and encode the analog ECG electrical signals into digital signals.

[0022] According to yet another aspect of the present invention, an ECG biometric authentication method of the present invention which is a method for a client terminal to be issued with a certificate from a KDC using an ECG includes collecting, by the client terminal, analog ECG waveform information in which upward pulses and downward pulses are displayed as a continuous curve, quantizing the analog ECG waveform information so that the analog ECG waveform information has discontinuous and unique

ECG information values, and binarizing the ECG information values which has become unique by the quantization to generate a binary code.

BRIEF DESCRIPTION OF THE DRAWINGS

[0023] The above and other objects, features and advantages of the present invention will become more apparent to those of ordinary skill in the art by describing exemplary embodiments thereof in detail with reference to the accompanying drawings, in which:

[0024] FIG. 1 is a view illustrating a graph showing P, QRS, T, and U waveforms that form electrocardiogram (ECG) analog signals and a heart which is the cause of the waveforms according to the related art;

[0025] FIG. 2 is a block diagram illustrating a configuration of an ECG biometric authentication system according to the present invention;

[0026] FIG. 3 is a graph illustrating analog ECG electrical signals having particular voltage waveforms obtained from biometric electrodes according to the present invention;

[0027] FIG. 4 is a conceptual view illustrating a digital code that quantizes the analog ECG electrical signals having particular voltage waveforms to generate a private key and a public key according to the present invention;

[0028] FIG. 5 is a conceptual view illustrating types of digital codes according to various embodiments of the present invention; and

[0029] FIG. 6 is a flowchart illustrating a process of ECG biometric authentication according to the present invention.

DETAILED DESCRIPTION OF EXEMPLARY EMBODIMENTS

[0030] Advantages and features of the present invention and a method for achieving the same will become apparent with reference to embodiments described in detail below and the accompanying drawings. However, the present invention is not limited to the embodiments disclosed hereinafter and may be implemented in various other forms. The embodiments are merely for completing the disclosure of the present invention, are provided to fully inform those of ordinary skill in the art to which the present invention pertains of the scope of the present invention, and are merely defined by the scope of the claims. Sizes and relative sizes of layers and regions in the drawings may be exaggerated for clarity of description. Like reference numerals refer to like elements throughout the specification.

[0031] Hereinafter, a preferred embodiment of an electrocardiogram (ECG) biometric authentication system according to the present invention having the configuration mentioned above will be described in detail with reference to the accompanying drawings.

[0032] In FIG. 2, a configuration of a system in which ECG biometric authentication is performed by an ECG biometric authentication terminal being connected over a network to a key distribution center (KDC) is illustrated in a block diagram.

[0033] Referring to FIG. 2, an ECG biometric authentication system 100 of the present invention includes one or more client terminals 110 and a KDC 120 that uses ECG biometric information to execute biometric authentication of a client. Although there are various types of biometric authentication (electroencephalogram, ECG, electromyogram, electrooculogram, etc.), the present invention uses

ECG authentication among the above through which electrical changes according to a number of heartbeats are displayed and are easily acquirable in everyday lives and are particularly difficult to replicate.

[0034] The client terminal **110** includes an ECG measurement sensor **112**, an ECG signal acquisition unit **114**, an ECG signal processing unit **116**, and an ECG signal communication unit **118**.

[0035] The ECG measurement sensor **112** is formed of one or more biometric electrodes. The one or more biometric electrodes may be formed of snap electrodes that can be used for a long time without irritating a client's skin.

[0036] The ECG signal acquisition unit **114** is connected via a wire to the ECG measurement sensor **112** to collect and process ECG signals from the one or more biometric electrodes. The ECG signals collected by the ECG signal acquisition unit **114** are analog electrical signals. As illustrated in FIG. 2, analog electrical signals having particular voltage waveforms are provided from the one or more biometric electrodes.

[0037] The ECG signal acquisition unit **114** may include a switch **114a** that determines a measurement time in real time when it is determined that measuring an ECG signal and converting the ECG signal to a digital code required for biometric authentication is needed. Alternatively, the ECG signal acquisition unit **114** may include a timer **114b** capable of determining a measurement cycle when cyclical measurement is required.

[0038] For example, slight differences may be generated when ECG measurement is performed while resting and after exercising, while lying down and sitting down, or before eating or drinking and after eating or drinking. Thus, the switch **114a** or the timer **114b** may be used to select a proper measurement time, or an average value of information acquired through measurement for a predetermined amount of time or repeated measurement may be used when executing biometric authentication to prevent an authentication error.

[0039] The ECG signal processing unit **116** performs a function of converting analog electrical signals having continuously changing amplitudes (voltage levels) on a continuous time axis into discontinuous digital signals (codes) that change by integers in predetermined units.

[0040] For this, the ECG signal processing unit **116** firstly amplifies sizes of the analog electrical signals through an analog signal amplification module **116a**. The ECG signal processing unit **116** quantizes the analog electrical signals having particular waveforms through a quantization module **116b** as illustrated in FIG. 4. In this way, the continuous analog electrical signals may be quantized based on a predetermined voltage level and be marked as P(+0.37100), Q(-0.22010), R(+0.98010), S(-0.41010), T(+0.28100), QRS(+0.34990), etc. Here, QRS is marked as (Q+R+S). The quantization result may be output as quantum codes which are decimals with five digits formed only of "1(or high)," "0 (or middle)," and "-1(or low)" through a digital encoding module **116c**.

[0041] The heart (refer to FIG. 1) is formed of two atriums and two ventricles. The heart generates micro-electricity every predetermined cycle by energy obtained from food and beats in the order of P, QRS, and T. In this way, the heart has a cardiac cycle from a predetermined heartbeat until a following heartbeat, and the cardiac cycle is divided into an atrial systolic period, a ventricular systolic period, and an

atrial/ventricular diastolic period. A left atrium and a right atrium are contracted and a left ventricle and a right ventricle are relaxed in the atrial systolic period, the left atrium and the right atrium are relaxed and the left ventricle and the right ventricle are contracted in the ventricular systolic period, and the left and right atriums and the left and right ventricles are all relaxed in the atrial/ventricular diastolic period.

[0042] Referring again to FIG. 3, an ECG is represented as wave frequencies that have recorded action currents and action potential differences due to a contraction of the heart being recorded as a waveform curve. Upward pulses and downward pulses are alternatively repeated in the ECG waveform, and the pulses are referred to as a P-wave, a Q-wave, an R-wave, an S-wave, and a T-wave, in that order.

[0043] Here, the P-wave in FIG. 3 is a waveform that has recorded a systolic process of the left and right atriums, the QRS complex is a waveform that has recorded a systolic process of the left and right ventricles, and the T-wave is a waveform that has recorded a diastolic process of the left and right ventricles. The P-wave is generated in a depolarization period of the atriums, the QRS complex is generated in a depolarization period of the ventricles, and the T-wave is generated in a repolarization period of the ventricles.

[0044] The depolarization of the atriums and ventricles and repolarization of the ventricles of the heart may be measured on a surface of the client's skin. Consequently, the present invention aims to measure influences of the depolarization and repolarization using the client terminal **110** using the ECG measurement sensor **112**.

[0045] Referring again to FIG. 4, the analog ECG waveforms are converted into binary digital codes through a quantization process. ECG digital information may represent 256-bit information by being formed of quantum codes of P-wave information (32-bit), Q-wave information (32-bit), R-wave information (32-bit), S-wave information (32-bit),

[0046] T-wave information (32-bit), QRS complex information (32-bit), and PIN information (64-bit).

[0047] For example, as a result of detecting a P-wave, a Q-wave, an R-wave, an S-wave, a T-wave, and a QRS complex at an inflection point at which an upward pulse is changed to downward pulse (or a downward pulse is changed to an upward pulse) from an ECG waveform curve and extracting and quantizing the inflection point (a feature point), it can be seen that a P-wave information value, a Q-wave information value, an R-wave information value, an S-wave information value, a T-wave information value, and a QRS complex information value are displayed as "+0.37100," "-0.22010," "+0.98010," "-0.41010," "+0.28100," and "+0.34990," respectively. For example, as illustrated in FIG. 2, each pulse value may be quantized using a grid box.

[0048] In yet another case, as illustrated in FIG. 5, a U-wave may be further included in addition to the P-wave, the Q-wave, the R-wave, the S-wave, the T-wave, and the QRS complex. However, the U-wave has a disadvantage compared to the QRS complex waveform in that upward pulses and downward pulses are clear and irregular. Consequently, still referring to FIG. 5, both of the U-wave and the QRS complex may be used.

[0049] Quantum code information values extracted from the ECG analog waveforms have values unique to each client, and the unique values may be used as information for biometric authentication of the present invention.

[0050] The ECG signal communication unit 118 has various communication functions such as communication via a mobile communications network, short-range wireless communication, etc. and may communicate in real-time with the KDC 120 that includes wireless communication modules such as a Bluetooth module capable of wireless data communication, an infrared communication module, a Zigbee module, etc.

[0051] Referring again to FIG. 2, a smart watch may be used as the client terminal 110 of the present invention. That is, the client terminal 110 includes a smart watch W and a smart band B that fixes the smart watch W to a wrist. The ECG measurement sensor 112, i.e., the biometric electrodes, may be installed in the smart band B that comes into contact with skin of the wrist. The smart band B may be a closed ring type that is flexible and contractible. Alternatively, the smart band B may be a fastening type that can be selectively opened or closed.

[0052] A smartphone, a personal digital assistant (PDA), a handheld personal computer (PC), a mobile phone, a home server PC, etc. may be used as the smart watch W.

[0053] The smart band B may be provided in the form of a patch to easily come into contact with skin to most effectively detect influences of depolarization and repolarization of the heart. The smart band B surrounds the client's wrist and allows the biometric electrodes to correspond to the skin of the wrist.

[0054] Consequently, among elements of the client terminal 110, the ECG measurement sensor 112 is embedded in the smart band B, the ECG signal acquisition unit 114, the ECG signal processing unit 116, and the ECG signal communication unit 118 that collect, process, and communicate ECG signals are embedded in the smart watch W, and the ECG measurement sensor 112 and the ECG signal acquisition unit 114 may perform wired or wireless communication with each other via the smart band B.

[0055] Next, referring to FIG. 4, the present invention may utilize the quantum codes determined by the method above to encrypt a private key.

[0056] The present invention uses a particular algorithm to encrypt data. Here, data encryption refers to a type of a lock in which data is transformed using a particular algorithm to prevent an unauthorized person from accessing the data. In this case, the particular algorithm being used serves as a key for locking the lock.

[0057] Conversely, to reproduce the encrypted data mentioned above, a means capable of decrypting the particular algorithm used in the encryption should be provided. The means for decrypting the particular algorithm serves as a key for unlocking the lock. That is, when the key is provided, the key may be used to decrypt the algorithm used in encrypting the data, and the data may be decrypted into an original form. Consequently, the algorithms used in encryption and decryption of the data are referred to as keys.

[0058] The present invention uses an asymmetric cryptographic system in which a key used for encryption and a key used for decryption are different. The asymmetric cryptographic system is an encryption technique in which a key used for encryption and a key used for decryption are different and is also referred to as a cryptosystem.

[0059] For example, the asymmetric cryptographic system is generally characterized as a public key infrastructure (PKI). A public key and a private key are configured by a product of two large decimals (normally a number with 140

digits or more) and additional computations, and a user is authenticated through a digital certificate.

[0060] Hereinafter, a process of issuing a client terminal with a certificate from the KDC using an ECG will be described with reference to the drawings.

[0061] Referring to FIG. 6, analog ECG waveform information in which upward/downward pulses are displayed as a continuous curve is quantized. The quantized discontinuous ECG information values have unique values.

[0062] A 256-bit private key is generated using each ECG waveform information value that has become unique by quantization. The private key of this degree is a sufficient number that enables all animals to be used as unique keys.

[0063] Encryption is performed by generating a pair of keys formed of the private key and a public key. The encryption result is transmitted to the KDC 120.

[0064] The KDC 120 decrypts the encryption result to generate the public key. Here, the KDC 120 issues a certificate using the RSA/ECC algorithm. In this case, PKI authentication is executed by providing the public key using the RSA/ECC algorithm.

[0065] The client terminal 110 receives the certificate and uses the certificate in the authentication process. The certificate is a digital document that proves that the particular client terminal 110 owns the corresponding public key.

[0066] Meanwhile, after the client terminal 110 has finished the authentication through the above-mentioned process of being issued with the digital certificate from the KDC 120, the client terminal 110 may restart the authentication process when the digital certificate needs to be renewed. Here, one hour may be set by the timer 114b, and when a private key is not received by the KDC 120 based on ECG information from the client terminal 110 during the set amount of time, the authentication process may be completely cancelled and be newly executed from a starting point to further enhance security.

[0067] The ECG biometric authentication terminal of the present invention is provided in the form of a smart watch and may be applied to an electronic bracelet that is worn by a particular criminal for surveillance of the criminal. A state in which the electronic bracelet is worn can be checked from a remote place by ECG information of the individual criminal being sent to the KDC in real-time or periodically.

[0068] As described above, the following effects can be expected by the configuration of the present invention.

[0069] First, an ECG biometric authentication terminal is in contact with a client's skin all the time such that it is convenient to perform real-time authentication and security is considerably enhanced due to authentication being completely impossible when the ECG biometric authentication terminal is detached from the client.

[0070] Second, a private key generated by processing QRS complex information unique to each individual to be quantized into digital codes through a quantization process is applied to a public key algorithm that uses a public key-private key combination such that security is further enhanced.

[0071] As described above, it can be recognized that the technical spirit of the present invention is a configuration in which an ECG biometric authentication terminal is provided in the form of a smart watch such that biometric electrodes that measure heartbeats can be installed in a band that is in contact with a client's wrist all the time, a function of quantizing analog ECG waveforms to process the analog

ECG waveforms to be converted into digital codes is embedded in a main body of a smart device such that the smart device may be used for its original function as well as for authentication during mobile banking and other payments processed using the smart device, and the digital codes acquired by processing the ECG waveforms are utilized in an RSA/ECC algorithm to enhance security. Those of ordinary skill in the art will be able to modify the present invention in various other ways within the scope of the basic technical spirit of the present invention.

What is claimed is:

1. A system for electrocardiogram (ECG) biometric authentication which is a biometric authentication system that performs biometric authentication using cyclical biometric voltage information having unique values for each client, the system comprising:

one or more client terminals; and

a key distribution center (KDC) configured to use ECG information of the one or more client terminals to issue a digital certificate.

2. The system of claim 1, wherein the client terminal includes:

an ECG measurement sensor formed of one or more biometric electrodes;

an ECG signal acquisition unit configured to collect analog ECG signals from the one or more biometric electrodes;

an ECG signal processing unit configured to encode the analog ECG signals into digital signals; and

an ECG signal communication unit configured to encrypt digital codes and transmit and receive digital codes from the KDC.

3. The system of claim 2, wherein, in encoding the analog ECG signals into digital signals in the ECG signal processing unit, the result is output as quantum codes which are decimals with five digits formed only of "1(or high)," "0(or middle)," and "-1(or low)".

4. The system of claim 3, wherein the analog ECG signals form a continuous ECG waveform curve in which upward pulses and downward pulses alternate, and the ECG waveform curve is formed by including a P-wave, a Q-wave, an R-wave, an S-wave, a T-wave, and a U-wave, in that order.

5. The system of claim 4, wherein, as a result of extracting and quantizing a feature point of each wave, the digital codes are formed of 32-bit P-wave information, 32-bit Q-wave information, 32-bit R-wave information, 32-bit S-wave information, 32-bit T-wave information, 32-bit QRS complex information and 32-bit PIN information.

6. The system of claim 5, wherein the digital codes are utilized to encrypt a private key in an asymmetric cryptographic system of a public key infrastructure (PKI).

7. A terminal for electrocardiogram (ECG) biometric authentication, the terminal comprising:

a smart band configured to surround a client's wrist, have one or more biometric electrodes coming into contact with skin of the wrist embedded therein, and detect analog ECG electrical signals through the one or more biometric electrodes; and

a smart watch electrically connected to the one or more biometric electrodes to collect the analog ECG electrical signals and encode the analog ECG electrical signals into digital signals.

8. The terminal of claim 7, wherein:

the analog ECG electrical signals form an ECG waveform curve including a P-wave, a Q-wave, an R-wave, an S-wave, and a T-wave; and

the digital codes are binary codes including P-wave information, Q-wave information, R-wave information, S-wave information, and T-wave information by quantizing the P-wave, the Q-wave, the R-wave, the S-wave, and the T-wave using a grid box.

9. The terminal of claim 8, wherein the digital codes further include QRS complex information.

10. A method for a client terminal to be issued with a certificate from a key distribution center (KDC) using an electrocardiogram (ECG), the method comprising:

collecting, by the client terminal, analog ECG waveform information in which upward pulses and downward pulses are displayed as a continuous curve;

quantizing the analog ECG waveform information so that the analog ECG waveform information has discontinuous and unique ECG information values; and

binarizing the ECG information values which has become unique by the quantization to generate a binary code.

11. The method of claim 10, further comprising:

changing the binary code into a private key and encrypting the private key;

transmitting, by the client terminal, the encryption result to a key distribution center (KDC);

decrypting a public key, in the KDC, by applying the encryption result to a Rivest-Shamir-Adleman (RSA)/Elliptic Curve Cryptosystem (ECC) algorithm;

transmitting the public key to the client terminal from the KDC; and

executing authentication, by the client terminal, using the public key.

12. The method of claim 11, wherein, in decrypting the encryption result to generate the public key, the KDC uses the RSA/ECC algorithm to issue ECG biometric private key verification and an X.509 certificate.

* * * * *

专利名称(译)	用于数字心电图认证的系统，终端和方法		
公开(公告)号	US20160360998A1	公开(公告)日	2016-12-15
申请号	US15/178415	申请日	2016-06-09
[标]申请(专利权)人(译)	JUN MOON SEOG		
申请(专利权)人(译)	君之于		
当前申请(专利权)人(译)	君之于		
[标]发明人	JUN MOON SEOG		
发明人	JUN, MOON-SEOG		
IPC分类号	A61B5/117 A61B5/00 A61B5/0456 A61B5/0408 A61B5/04		
CPC分类号	A61B5/117 A61B5/04085 A61B5/681 A61B5/0456 A61B5/04012 A61B5/0402 A61B5/04525		
优先权	1020150082898 2015-06-11 KR		
其他公开文献	US9750435		
外部链接	Espacenet USPTO		

摘要(译)

提供了一种心电图 (ECG) 生物认证系统，其使用具有针对每个客户端的唯一值的生物特征信息来执行生物特征认证，所述生物特征信息包括一个或多个客户端终端和使用一个或多个客户端终端的ECG信息来发布的密钥分发中心 (KDC)。数字证书。根据心电图生物认证系统的配置，增强了安全性。

