

Description

Title of Invention: AUTHENTICATION SYSTEM AND METHOD USING FLASH OF SMART MOBILE

Technical Field

- [1] The present invention relates to an authentication system and method using a flash of a smart mobile, and more specifically relates to an authentication system and method using a flash of a smart mobile capable of authentication by transmitting data through light emitted from a flash of a smart mobile, thereby enhancing security and safety in comparison with other authentication systems such as ID, password, official certification, OTP and so on.

Background Art

- [2] In general, a conventional charge settlement method of a commercial transaction which is implemented for purchasing or selling a merchandise has been mostly performed by cash or a credit card possessed by an user. In case of using a credit card, the user presents a credit card after purchasing a merchandise or receiving a service, and then a store requests and receiving an approval to/from a transaction server using an inquiry terminal installed thereof.
- [3] However, the credit card which should be possessed for using this transaction is easy to be frequently lost, the fact of losing is not aware easily because it is used in large amount transaction more than dozens of thousands won rather than small amount transaction the such that the frequency of use is low when it was lost, thereby it is frequent that the lost credit card is used in a malicious transaction such as an unlawful transaction in real state during without recognition of losing.
- [4] And, since the credit card accompanies a commercial transaction according to information stored by a magnetic strip method, it is weak to forgery and alteration, thereby damages more than dozens of million won are occurred by forged and altered credit card.
- [5] Even if not the above losing or forgery and alteration, the credit card number and the term of validity is sufficient for transaction for purchasing a merchandise at present when shopping through Internet is a daily work, and these information is easily exposed from an online shopping mall or a store during transaction by the credit card, thereby cases of taking unlawful profit in an Internet shopping mall are frequently occurred by using these information maliciously and damages are increasing in the real state.
- [6] In this reasons, a purchaser possessing a credit card does not trust the Internet shopping mall to dislike providing their credit card. Thus there is inconvenience that

needlessly large amount of money should be possessed, or large amount of time should be spent for purchasing necessary merchandise because purchase through communication network is not considered. It is a real state that these problems are obstacles to progress toward a credit society.

- [7] Relative prior art is Korean registered patent No. 10-1260698 (Method and system for call authentication using terminal information, Registered date: April 29, 2013) and Korean Patent Publication No. 10-2001-0068073 (System and method for transaction by using communication terminals, Publication date: July 13, 2001)

Disclosure of Invention

Technical Problem

- [8] The present invention relates to an authentication system and method using a flash of a smart mobile, and more specifically relates to an authentication system and method using a flash of a smart mobile capable of authentication by transmitting data through light emitted from a flash of a smart mobile thereby enhancing security and safety in comparison with other authentication systems such as ID, password, official certification, OTP and so on.
- [9] Other objects of the present invention are understood through features of the present invention, known from embodiments of the present invention, and embodied by means described in claims and combination thereof.

Solution to Problem

- [10] To solve the above problems, the present invention includes technical features as follows.
- [11] An authentication system using a flash of a smart mobile according to the present invention includes a smart mobile having a flash which emits light; a light receiver receiving light emitted from the smart mobile to convert into data; and an authentication server generating authentication information from the data and transmitting to the smart mobile.
- [12] An authentication system using a flash of a smart mobile according to the present invention may further include a recognition module recognizing which light among a plurality of lights emitted from the smart mobile is to be received.
- [13] An authentication system using a flash of a smart mobile according to the present invention may further include a selection module selecting a light from the smart mobile among a plurality of lights emitted in the same space with the light of from the smart mobile.
- [14] In an authentication system using a flash of a smart mobile according to the present invention, the light emitted from the smart mobile is formed in one-time.
- [15] In an authentication system using a flash of a smart mobile according to the present

invention, emission speed and frequency of the light emitted from the smart mobile may be controllable.

[16] In an authentication system using a flash of a smart mobile according to the present invention, emission range of the light emitted from the smart mobile may be controllable.

[17] In an authentication system using a flash of a smart mobile according to the present invention, emission distance of the light emitted from the smart mobile may be controllable.

[18] In an authentication system using a flash of a smart mobile according to the present invention, the light receiver may be formed into one of a credit card, a bank or a member store.

[19] In an authentication system using a flash of a smart mobile according to the present invention, the authentication server may be applicable to an authentication for a transaction or an authentication for a person.

[20] An authentication method using a flash of a smart mobile according to the present invention includes a step of emitting light using a flash equipped to a smart mobile; a step of receiving a light emitted from the smart mobile to convert into data; and a step of receiving a data converted by the receiver to generate the data into authentication information and transmit to the smart mobile, in an authentication server.

[21] An authentication method using a flash of a smart mobile according to the present invention may further include a recognition module recognizing which light among a plurality of lights emitted from the smart mobile is to be received.

[22] An authentication method using a flash of a smart mobile according to the present invention may further include a selection module selecting a light from the smart mobile among a plurality of lights emitted in the same space with the light of from the smart mobile.

[23] In an authentication method using a flash of a smart mobile according to the present invention, the light emitted from the smart mobile may be formed in one-time.

[24] In an authentication method using a flash of a smart mobile according to the present invention, emission speed and frequency of the light emitted from the smart mobile may be controllable.

Advantageous Effects of Invention

[25] Since the present invention is capable of authentication by transmitting through light emitted from a flash of a smart mobile according to foregoing solution of the problem, security and stability can be improved in comparison with other authentication systems such as an ID, a password, a public authentication which are necessary to a bank task, a personal authentication, an identity authentication and a transaction remittance.

- [26] And, even if the smart mobile is lost or a stranger acquiring this are misappropriating, cryptography such as patterns cannot be solved thereby it is not available.
- [27] Further, carrying is easy to use anywhere regardless of the place because the transaction is available using a flash equipped to the smart mobile.
- [28] Other effects of the present invention are understood through features of the present invention, are known from examples of the present invention, and are demonstrated by means shown in claims and combination thereof.

Brief Description of Drawings

- [29] FIG. 1 is a perspective view of an embodiment of the authentication system using a flash of a smart mobile according to the present invention.
- [30] FIG. 2 is a block diagram illustrating a state of adding a recognition module and a selection module.
- [31] FIG. 3 is a flow chart of an embodiment of the authentication method using a flash of a smart mobile according to the present invention.
- [32] 100: Authentication system using flash of smart mobile
- [33] 110: Smart mobile
- [34] 120: Light receiver
- [35] 130: Authentication server
- [36] 140: Recognition module
- [37] 150: selection module
- [38] S100: Method of authentication using flash of smart mobile
- [39] S110: Step of emitting
- [40] S120: Step of light receiving
- [41] S130: Step of authenticating
- [42] S140: Step of recognizing
- [43] S150: Step of selecting

Mode for the Invention

- [44] The following specifications of the present invention are referring to accompanying drawings which illustrate a specific example implementing the present invention. These embodiments are described in more detail enough to let those skilled in the art implement the present invention. The various embodiments of the present invention are different to each other, however, it is understood that those are not exclusive each other. For example, specific forms, structures and features described herein may be achieved in other embodiments without departing from the spirits and the scopes of the technology concept of the present invention. Further, the location and arrangement of each element in each embodiment described herein may be modified without departing from the concepts and the scopes of the present invention. Therefore, the following

specifications are not adopted with restricted meaning, and the scopes of the inventive concept are only limited by whole scopes equivalent to insistence of claims and accompanying claims. The similar reference numbers in drawings refer the same or similar functions in various aspects.

- [45] FIG. 1 is a perspective view of an embodiment of the authentication system using a flash of a smart mobile according to the present invention. And FIG. 2 is a block diagram illustrating a state of adding a recognition module and a selection module.
- [46] An authentication system 100 using a flash of a smart mobile according to the present invention, as shown in FIG. 1 and FIG. 2, includes a smart mobile 110, a light receiver 120, and an authentication server 130.
- [47] The smart mobile 110 is generally equipped with a flash emitting light on a rear side of the smart mobile 110.
- [48] The smart mobile 110 is a device which is capable of wireless connection with the other party in anytime and anywhere to exchange information while moving, and is a mobile phone capable of at least third generation communication, a tablet PC, a PDA, a PMP and so on.
- [49] The smart mobile 110 is referring to a mobile phone conventionally, the mobile phone has various function such as transmitting/receiving text messages, a voice communication, a data communication by accessing the Web.
- [50] The present invention is a next generation wireless communication technology using light emitted from a flash of a smart mobile 110, being improved in security and stability in comparison with other authentication systems such as an ID, a password, a public authentication which are necessary to a bank task, a personal authentication, an identity authentication and a transaction remittance.
- [51] As light emitted from the flash of the smart mobile 110 is transmitted by data communication to be authenticated, the flash of the smart mobile 110 can be used as an optical communication device such as a Li-Fi which is highlighted as next generation wireless communication technology using light.
- [52] The Li-Fi (Light-Fidelity) is a technology in which unlimited Internet shared Wi-Fi technology is merged with the flash of the smart mobile 110, i.e., high efficient illumination LED technology.
- [53] The smart mobile 110 can data communication under LED illuminance in which the light emitted from the flash is not visible to the naked eye, and can be used at an area sensitive to radio interference such as an airplane or a nuclear power plant.
- [54] As the smart mobile 100 capable of data communication uses a flash equipped to the smart mobile 110, an additional device is not necessary and this is not harmful to a human body in comparison to other wire/wireless optical communication technologies.
- [55] The light emitted from the smart mobile 110 is formed in one-time. Studying more

carefully, the one-time is represented in a different way into a one-time password generator which is for consolidating security against financial hacking, smishing or pharming.

[56] The one-time password generator is a security system which is used just at a session of each login time, has purpose for preventing password stolen which may be occurring by reusing repeatedly same password.

[57] It is impossible to reuse because a password called by hash based on unidirectional cryptography in difference with conventional password is used and it is disused after the session, and then it can prevent a surreptitious use even if it was lost.

[58] The light emitted from the smart mobile (110) can be controllable in speed and frequency. This is same as the concept of the one-time or one-time password as describe above, it is impossible to use surreptitiously by the other person even if the smart mobile 110 is lost, and a financial task, a transaction task and personal authentication task can be processed in safe.

[59] The present invention is used as a powerful device by supplementing a financial task or personal authentication task through foregoing one-time or one-time password and through adjusting emitting light speed and frequency.

[60] The light emitted from the smart mobile 110 is blink at least 60ps per a second. This is a frequency for a human being to recognize naturally.

[61] The smart mobile 100 can control emission range of the emitting light. These can be recognized even if the light to a transaction transmitted from the authentication server 130 or personal authentication information that will be described below is not emitted in an accurate range but emitted around there.

[62] The smart mobile 110 can control emission distance of the emitting light. These can be recognized even if the light emitted to the authentication information transmitted from the authentication server 130 is just arrived in a predetermined distance.

[63] The light receiver 120 receives light emitted from the smart mobile 110 to convert into data. Specifically, the light emitted from the smart mobile 110 can be converted into data for programing by using wavelength of the light in the light receiver 120.

[64] The light receiver 120 may be formed inito at least one of a credit card, a bank or a member store. The member store is generally a department store, a cafeteria, a restaurant, a hotel, a golf link, a travel bureau or a gas station.

[65] The authentication server 130 receives data converted at the light receiver 120 to generate authentication information from the data and transmit to the smart mobile 110

[66] The authentication server 130 is a system generated for ascertaining transmitted data which is converted at the light receiver 120 to certify and approve a transaction or not, or an person or not.

[67] The authentication server 130 is applied to authentication for a transaction or a

person.

[68] The authentication server 130 transmits the generated authentication information to the smart mobile 110 in a form of message to activate on a display; thereby the authentication information is outputted on the display of the smart mobile 110.

[69] The authentication server 130 transmits the authentication information to the smart mobile 110 and stores the authentication in temporary, simultaneously. This is preparation for the situation that the authentication information is not transmitted normally when the authentication information is transmitted from the authentication server to the smart mobile 110.

[70] After confirming the authentication information transmitted to the smart mobile 110, the flash of the smart mobile 110 is emitted to complete a transaction or personal authentication.

[71] If the transaction or personal authentication is confirmed by emitting the flash of the smart mobile 110, the authentication server 130 transmit information of transaction completion or person identification to the smart mobile 110 and the light receiver 120.

[72] The recognition module 140 recognizes receiving data from which light among a plurality of lights emitted through the smart mobile 110. Specifically, the recognition module 140 recognizes a light for transmitting data among lights emitted from the smart mobile 110 that is emitted for taking a picture or a movie, or for lightening a dark place such that the error caused by a plurality of lights can be minimized.

[73] The selection module 150 selects a light from the smart mobile 110 among a plurality of lights emitted in the same place with the light emitted from the smart mobile 110. The selection module 150 selects a light (it means data) emitted from the smart mobile 110 among a plurality of lights that is emitted in the same place with the light emitted from the smart mobile 110, and that is a fluorescent lamp or a bedroom lamp in case of indoor, or a street lamp or luminescent lamp in case of outdoor.

[74] The selection module 150 prevent the light of the smart module 110 with data from interfering with other light emitted in the same place with the light emitted from the smart mobile 110 such as a fluorescent lamp or a bedroom lamp in case of indoor, or a street lamp or luminescent lamp in case of outdoor.

[75] Although the authentication system of the present invention illustrates the transaction or personal authentication by using the light of the flash equipped to the smart mobile 110, anything capable of authenticating the transaction and person, even if sound such as high frequency wave can be used in the authentication.

[76] Exemplary embodiment of the authentication method using a flash of the smart mobile according to the present invention will now be described more specifically with reference to drawings appended herein

[77] FIG. 3 is a flow chart of an embodiment of the authentication method using a flash of

a smart mobile according to the present invention.

[78] An authentication method S100 using a flash of a smart mobile according to the present invention, as shown in FIG. 3, includes a step S110 of emitting light using a flash equipped to a smart mobile; a step S120 of receiving a light emitted from the smart mobile to convert into data; and a step S130 of receiving a data converted by the receiver to transmit a authentication information which is generated by affirmation and identifying the data to the smart mobile, in an authentication server.

[79] The step of emitting S110 emits light using a flash equipped to the smart mobile 110.

[80] The present invention is a next generation wireless communication technology using light emitted from a flash of a smart mobile 110, is improved in security and stability in comparison with other authentication systems such as an ID, a password, a public authentication which are necessary to a bank task, a personal authentication, an identity authentication and a transaction remittance.

[81] As light emitted from the flash of the smart mobile 110 is transmitted by data communication to be authenticated, the flash of the smart mobile 110 can be used as an optical communication device such as a Li-Fi which is highlighted as next generation wireless communication technology using light.

[82] The smart mobile 110 can data communication under LED illuminance in which the light emitted from the flash is not visible to the naked eye, and can be used at an area sensitive to radio interference such as an airplane or a nuclear power plant.

[83] The light emitted from the smart mobile 110 is formed in one-time. Studying more carefully, describing in other expression, it is temporary password generator by which security is reinforced against a financial hacking, a smishing or a pharming, using a one-time password.

[84] The one-time password generator is a security system which is used just at a session of each login time, and prevents password stolen which may be occurring by reusing repeatedly same password.

[85] It is impossible to reuse because a password called by hash based on unidirectional cryptography in difference with conventional password is used and it is disused after the session, and then it can prevent a surreptitious use who has known the password illegally even if it was lost.

[86] The light emitted from the smart mobile (110) can be controllable in speed and frequency. This is same as the concept of the one-time or one-time password as describe above, it is impossible to use surreptitiously by the other person even if the smart mobile 110 is lost, and a financial task or personal authentication task can be processed in safe.

[87] The smart mobile 110 can control an emitting range and distance of the emitting light. These can be recognized even if the light to a transaction transmitted from the

authentication server 130 or personal authentication information is just emitted in a predetermined range.

[88] The step of receiving light receives the light emitted from the smart mobile 110 at the light receiver 120 receives to convert into data. Specifically, the light emitted from the smart mobile 110 can be converted into data for programing using wavelength of the light in the light receiver 120.

[89] The step of authenticating S130 receives data converted at the light receiver 120 to generate authentication information from the data and transmit to the smart mobile 110

[90] The authentication server 130 is a system generated for ascertains transmitted data which is converted at the light receiver 120 to certify and approve a transaction or not, or an person or not.

[91] The authentication server 130 is applied to authentication for a transaction or a person.

[92] The authentication server 130 transmits the generated authentication information to the smart mobile 110 in a message to activate on a display; thereby the authentication information is outputted on the display of the smart mobile 110.

[93] The authentication server 130 transmits the authentication information to the smart mobile 110 and temporary stores the authentication, simultaneously. This is preparation for the situation that the authentication information is not transmitted normally when the authentication information is transmitted from the authentication server to the smart mobile 110.

[94] The step of recognizing S140 recognizes receiving data from which light among a plurality of lights emitted through the smart mobile 110. Specifically, the recognition module 140 recognizes a light for transmitting data among lights emitted from the smart mobile 110 that is emitted for taking a picture or a movie, or for lightening a dark place such that the error caused by a plurality of lights can be minimized.

[95] The step of selecting selects a light from the smart mobile 110 among a plurality of lights emitted in the same place with the light emitted from the smart mobile 110.

[96] The selection module 150 selects a light (it means data) emitted from the smart mobile 110 among a plurality of lights that is emitted in the same place with the light emitted from the smart mobile 110, and that is a fluorescent lamp or a bedroom lamp in case of indoor, or a street lamp or luminescent lamp in case of outdoor.

[97] The selection module 150 prevent the light of the smart module 110 with data from interfering with other light emitted in the same place with the light emitted from the smart mobile 110 such as a fluorescent lamp or a bedroom lamp in case of indoor, or a street lamp or luminescent lamp in case of outdoor.

[98] The above describes the present invention in accordance with an exemplary embodiment, however, it will be clarified to those skilled in the art that various changes

and modifications can be implemented in scope of claims, and those changes and modifications belongs the scope of accompanying claims.

Claims

- [Claim 1] An authentication system comprising:
a smart mobile terminal having a flash which emits light;
a light receiver receiving the light emitted from the smart mobile terminal and converting the received light to data, the light receiver is associated with one of a credit card, a bank or a member store; and
an authentication server generating authentication information from the data received from the light receiver and transmitting the authentication information to the smart mobile terminal,
wherein the light emitted from the smart mobile terminal is for one-time use such that the light is used as a one-time password that is discarded after the light is used to generate the authentication information, and
wherein a speed and a number of light emission from the flash of the smart mobile terminal are controlled such that light is emitted differently each time when the light is emitted from the flash of the smart mobile terminal for authentication.
- [Claim 2] The authentication system of claim 1, further comprising:
a recognition module recognizing the light convertible to the data among a plurality of lights emitted from the smart mobile terminal such that the recognized light is received by the light receiver,
wherein the plurality of lights comprise light used for capturing a picture or a moving picture or light used for lighting up a dark place.
- [Claim 3] The authentication system of claim 1, further comprising:
a selection module selecting the light emitted from the smart mobile terminal among a plurality of lights comprising lights emitted from sources other than the smart mobile terminal.
- [Claim 4] The authentication system of claim 1, wherein an emission range of the light emitted from the smart mobile terminal is controllable.
- [Claim 5] The authentication system of claim 1, wherein an emission distance of the light emitted from the smart mobile terminal is controllable.
- [Claim 6] The authentication system of claim 1, wherein the authentication server is applicable to an authentication for a transaction or an authentication for a person.
- [Claim 7] A method of authentication using a flash of a smart mobile terminal, the method comprising:
emitting light, by the flash;

receiving, by a light receiver, the light emitted from the smart mobile terminal and converting the received light to data; and
 receiving, by an authentication server the data from the light receiver;
 and
 generating, by the authentication server, authentication information from the received data and transmitting the authentication information to the smart mobile terminal,
 wherein the light emitted from the smart mobile terminal is for one-time use such that the light is used as a one-time password that is discarded after the light is used to generate the authentication information,
 wherein a speed and a number of light emission from the flash of the smart mobile terminal are controlled such that light is emitted differently each time when the light is emitted from the flash of the smart mobile terminal for authentication; and
 wherein the light receiver is associated with one of a credit card, a bank or a member store.

[Claim 8]

The method of claim 7, further comprising:
 recognizing the light convertible to the data among a plurality of lights emitted from the smart mobile terminal such that the recognized light is received by the light receiver,
 wherein the plurality of lights comprise light used for capturing a picture or moving picture or light used for lighting up a dark place.

[Claim 9]

The method of claim 7, further comprising:
 selecting the light emitted from the smart mobile terminal among a plurality of lights comprising lights emitted from sources other than the smart mobile terminal.

[Claim 10]

An authentication system comprising:
 a smart mobile terminal having a flash which emits light;
 a light receiver receiving the light emitted from the smart mobile terminal and converting the received light to data;
 an authentication server generating authentication information from the data received from the light receiver and transmitting the authentication information to the smart mobile terminal;
 a recognition module recognizing the light convertible to the data among a plurality of lights emitted from the smart mobile terminal such that the recognized light is received by the light receiver; and

a selection module selecting the light emitted from the smart mobile terminal among a plurality of lights comprising lights emitted from sources other than the smart mobile terminal,
wherein the light receiver is associated with one of a credit card, a bank or a member store