

DEVICE AND METHOD FOR SCREEN PROTECTION INSURANCE

FIELD OF THE INVENTION

[0001] The present invention relates to screen protection insurance, and in particular, to a device and a method for assisting a screen protection insurance for a mobile device.

BACKGROUND OF THE INVENTION

[0002] Devices such as smart phones, watches and tablets with screens are spreading in the market. Common damage to these devices is to the screen. Therefore, it is desirable to offer users insurance for the screen damage on their devices. However, it takes some time and effort for the insurers to verify that a device's screen is undamaged before issuing an insurance policy. There are other challenges for insurers. Lack of abilities to solve the above challenges for the verifications may cause the risk of fraud for insurers. As a result, there exist needs for a technique providing an effective insurance of a device.

SUMMARY OF THE INVENTION

[0003] The present invention provides techniques for assisting an effective insurance procedure for a device.

[0004] In one aspect of the present invention, a server computer comprises a control unit and a storage unit, wherein the control unit is configured to receive an image in association with a request for an insurance contract, wherein the image is obtained by taking a photograph of a screen of a mobile device displaying a digital signature generated based on the identification information of the mobile device to be insured. The control unit detects the digital signature and the condition of the screen from the received image. When the screen is detected to be in good condition, the contract information indicating that the insurance is valid for the screen displaying the digital signature and the screen is found to be in good condition is stored and sent to the mobile device.

[0005] The following factors of the present invention make it difficult to for fraud to be committed:

1. Putting a digitally signed fingerprint (herein referred to as a "digital signature") on the screen ensures that the photograph of the screen is that of the mobile device to be insured.
2. The digital signature is timestamped and is required to be submitted within a specified time. The specified time is of short duration (for example 5 minutes or less) from the time of the generation of the digital signature. The timestamp and the short

submission time make it difficult for someone to alter the image (for example, altering the image of a damaged screen to appear to be in the good condition). This assists an insurance company to prevent fraud.

3. Disabling accurate screen capture of the digital signature makes it difficult for a screenshot to be taken and altered and/or used by another party.

[0006] In another aspect of the present invention, a method performed in a computing device comprising a control unit and a storage unit. The above method includes the following steps performed under control of the control unit: receiving an image in association with a request for an insurance contract, wherein the image has been obtained by taking a photograph of a screen of a mobile device displaying a digital signature generated based on identification information of a mobile device; detecting the digital signature and a condition of the screen from the received image; storing on the storage unit insurance contract information indicating that the insurance is valid for the screen displaying the digital signature where the digital signature is detected and the screen is found to be in good condition; sending the insurance contract information to the mobile device.

BRIEF DESCRIPTION OF THE DRAWINGS

[0007] FIG. 1 illustrates an example of an implementation of a system.

[0008] FIG. 2 is a block diagram illustrating an example of the functions of a mobile device.

[0009] FIG. 3 illustrates an example of the appearance of a mobile device.

[0010] FIG. 4 is a block diagram illustrating an example of the functions of a server computer.

[0011] FIG. 5 is a sequence diagram illustrating an example of the process flow of the system where a request for an insurance contract is made.

[0012] FIG. 6 is a sequence diagram illustrating an example of the process flow in the system where a claim is made.

[0013] FIG. 7 is a sequence diagram illustrating an example of the process flow in the system where a completion of a repair is reported.

[0014] FIG. 8 is a block diagram illustrating an example of the hardware elements of a mobile device.

[0015] FIG. 9 is a block diagram illustrating an example of the hardware elements of a server computer.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0016] The present invention will be further described hereinafter with reference to the accompanying drawings. It is to be understood that specific embodiments described herein are

only intended to explain the present invention, and are not taken to limit the present invention. Further, it will be appreciated that the examples provided represent only one of many possible implementations of the present invention.

[0017] Overview

[0018] Referring to FIG. 1, a configuration of a system 1 according to one embodiment will be described. The system 1 assists insurance companies in remotely detecting the good condition of a screen of a mobile device before issuing an insurance contract. The system also assists the insurance company and the consumer in detecting the condition of the screen when the consumer makes a claim against the insurance policy and when the screen is repaired. In this implementation, the system 1 comprises a mobile device 10, a server computer 20, and a client computer 30. The mobile device 10, the server computer 20 and the client computer 30 can mutually communicate via the network N. In FIG. 1, one mobile device 10, one server computer 20, and one client computer 30 are described, but the number of these devices is arbitrary.

[0019] In this embodiment, the mobile device 10 is a mobile device containing a screen to be insured. The mobile device 10 can be a mobile phone, a smartphone, a tablet, a PDA (Personal Digital Assistant), a laptop computer, and/or the like, but is not limited to these.

[0020] The server computer 20 is a computer that can be operated by an insurance company or a party delegated by the insurance company. The server computer 20 may be configured by a general server computer, a personal computer, cloud computing and/or the like, but is not limited thereto.

[0021] The client computer 30 is a computer that is operated by a repair shop, a dealer of mobile device, a sales company of insurance, or a party entrusted by them. The client computer 30 can be configured by a personal computer and/or the like, but is not limited thereto.

[0022] With reference to FIG. 2, an overview of the functions of the mobile device 10 will be described. The mobile device 10 has a database 101, a fingerprint generator 102, a digital signature generator 103, a display controller 104, a camera controller 105, and a communication controller 106 as functional elements, but not limited thereto. These functional elements are implemented, for example, by the CPU in the control unit of the mobile device 10 deploying a computer program stored on the storage unit to memory and executing it to control operations of each element of the mobile device 10. An example of the hardware configuration of the mobile device 10 will be described later.

[0023] The database 101 stores information necessary for processing and information generated by the processing. For example, the information generated by the processing stored in database 101 can be a digital fingerprint or a digital signature to be described later.

[0024] The fingerprint generator 102 generates a digital fingerprint of the mobile device 10 based on the identification information of the mobile device 10. The identification information used for generating the digital fingerprint includes an International Mobile Equipment Identity

(IMEI) number, a Mobile Equipment Identifier (MEID) number, an Electronic Serial Number (ESN), an Identifier For Vendor (IDFV) (for iOS), a custom generated unique ID, a MAC Address, a Serial Number, a Phone Brand, and Phone Model, or a combination of at least some of them. The identification information used to generate the digital fingerprint may be one or a plurality of identification randomly selected from the above identification information of the mobile device 10.

[0025] The digital signature generator 103 generates, based on the digital fingerprint generated by the fingerprint generator 102, a digitally signed and timestamped unique digital signature. That is, the unique digital signature is generated based on the identification information of the mobile device 10 and signed using a private key. The time stamp is a time stamp at the time of generation of the unique digital signature. The unique digital signature may include the location information of the mobile device 10 calculated based on the signal received by the GPS receiver of the mobile device 10. The generated unique digital signature may be represented as an image using a barcode, QR code, or other coded image forms. Herein, the unique digital signature generated with respect to the mobile device 10 by the digital signature generator 103 is referred to as “digital signature”.

[0026] The display controller 104 controls the display of the screen of the mobile device 10. The display controller 104 controls, for example, the display of the image captured by the camera of the mobile device 10 and the display of the digital signature generated by the digital signature generator 103 on the screen.

[0027] The digital signature may be generated by the digital signature generator 103 and displayed on the screen in such a manner so as to facilitate the screen damage detection process to be described later. For example, the digital signature can be displayed in a light colour (e.g., grey). For the same reason, the background of the digital signature displayed on the screen may be a single colour (e.g., white).

[0028] FIG. 3 shows an example of a display on the screen S of the mobile device 10. In this example, the digital signature D is displayed on the screen S of the mobile device 10 under the control of the display controller 104.

[0029] Returning to FIG. 2, the camera controller 105 controls the capture of images by the camera of the mobile device 10. For example, the camera controller 105 stores the image captured by the camera of the mobile device 10 in the database 101 according to the operation of the user.

[0030] In addition, the camera controller 105 can store the image captured by the camera of the mobile device 10 in the database 101 when predetermined conditions have been satisfied. Specifically, when the user of the mobile device 10 first points a face of the screen of the mobile device 10 to a mirrored surface, the camera controller 105 determines, on the basis of the image captured by the camera, whether or not the following matters are satisfied;

- 1) the screen displaying the digital signature appears on the mirrored surface;

- 2) the entire screen appearing on the mirrored surface is within the field of view of the camera;
- 3) the proportion of the entire screen to the entire image to be captured is within a predetermined range (for example, 80% to 100%);
- 4) the screen appearing on the mirrored surface is flat; and
- 5) the face of the screen is parallel to the face of the mirrored surface.

[0031] When all or a part of the above is satisfied, the image is captured by the camera of the mobile device 10 and the camera controller 105 stores the captured image (automatically, without user operation) in the database 101.

[0032] Further, while the digital signature generated by the digital signature generator 103 is displayed on the screen, the camera controller 105 can prohibit the unauthorised saving of the digital signature displayed on the screen of the mobile device 10, for example by screen capture. By doing this, it may be possible to prevent the tampering of the digital signature.

[0033] Communication controller 106 controls the transmission and reception of data between mobile device 10 and external devices. For example, the communication controller 106 controls the transmission to the server computer 20 of the digital signature generated by the digital signature generator 103 and the image of the screen captured by the camera of the mobile device 10 on which the digital signature is displayed.

[0034] With reference to FIG. 4, the overview of the functions of server computer 20 will be described below. The server computer 20 has database 201, communication controller 202, detection component 203, insurance manager 204, verification component 205 as functional components, but not limited thereto. These functional elements are implemented, for example, by the CPU in the control unit of the server computer 20 by deploying a computer program stored on the storage unit to memory and executing it to control operations of each element of the server computer 20. An example of a hardware configuration of the server computer 20 will be described later.

[0035] The database 201 stores information necessary for processing and information generated by the processing. For example, the database 201 stores a digital signature to be described later which is received from the mobile device 10.

[0036] Communication controller 202 controls transmission and reception of data between server computer 20 and external devices. For example, the communication controller 202 receives an image obtained by capturing an image of a screen on which a digital signature is displayed, in association with a request for a screen protection insurance contract. As described above, the digital signature is generated by the digital signature generator 103, for example, based on the identification information of the mobile device 10. The image of the screen on which the digital signature is displayed may be an image captured by the camera of the mobile device 10 or an image captured by the camera of the device other than the mobile device 10.

[0037] The detection component 203 can detect the digital signature and the condition of the screen of the mobile device 10 from the received image. Detection of the condition of the screen can confirm the presence or absence of damage to the screen, for example, by scanning the image. The detection component 203 can detect both the digital signature generated by the digital signature generator 103 and the condition of the screen of the mobile device 10 from the single image captured.

[0038] Insurance manager 204 manages screen insurance contracts, insurance claims, and screen repair status. For example, the insurance manager 204 receives an image in association with a request for insurance contracts on a screen, and once the digital signature is detected by the detection component 203 and it is determined that the screen is intact, the insurance contract information indicating that the insurance of the screen displaying the digital signature is valid can be stored in the database 201. Then, at least a part of the stored insurance contract information is transmitted to the mobile device 10 via the communication controller 202.

[0039] The verification component 205 determines the validity of the insurance claim being made (namely, whether or not the screen that the insurance claim is made is covered with valid insurance). This determination is made, for example, after an insurance claim is filed by a person who wants his screen of mobile to be repaired. The verification component 205 compares the digital signature detected from a pre-repair image (an image of the damaged screen before the damaged screen is repaired) received in relation to the filing of an insurance claim, with the information stored in the database 201. In the case where the information stored in the database 201 indicates that the screen is insured, the verification component 205 determines that insurance of the screen relating to the insurance claim is valid and that costs of the repair of damage of the screen detected by the detection component 203 can be claimed.

[0040] Process flow

[0041] With reference to FIG. 5, a flow of processing performed in the mobile device 10 and the server computer 20 when insuring the screen of the mobile device 10 will be described. This processing is performed under the control of the control units of the mobile device 10 and the server computer 20. The same applies to the processing flow described later.

[0042] In step S11, after receiving an instruction to start processing for the issuance of the insurance contract from the user, the mobile device 10 generates the digital fingerprint of the mobile device 10 based on the identification information of the mobile device 10. Details of the identification information of the mobile device 10 are as described above. The generated digital fingerprint is stored on the storage unit of the mobile device 10.

[0043] In step S12, the mobile device 10 generates a digital signature that has been time-stamped based on the digital fingerprint generated in step S11 (namely, based on the identification information of the mobile device 10).

[0044] In step S13, the mobile device 10 displays the digital signature generated in step S12 on the screen. As described above, the digital signature can be displayed in a light colour (e.g., grey). The background of the digital signature displayed on the screen may be a single colour

(e.g., white). An image of the screen on which the digital signature is displayed is captured by the camera. The image capture can be performed in various ways.

[0045] For example, if the mobile device 10 includes a camera, the image captured by the camera of the mobile device 10 may be stored in the database 101 according to the operation of the user. Alternatively, as described above, the image captured by the camera can be stored in the database 101 when predetermined conditions are satisfied. As another example, an image may be obtained by capturing the image of the screen of the mobile device 10 with a camera of a device other than the mobile device 10.

[0046] In step S14, the mobile device 10 transmits the image of the screen captured as described above to the server computer 20 in association with a request for insurance contract for the screen. If an image has been captured by a camera of a device other than the mobile device 10, the obtained image may be transmitted to the server computer 20 by an apparatus other than the mobile device 10 (for example, client computer 30).

[0047] In step S15, the server computer 20 receives a single image received from the mobile device 10 (or another device) in association with the request for insurance contract of the screen, and detects the digital signature (the digital signature generated with respect to the mobile device 10) and the condition of the screen of the mobile device 10 (for example, whether there is damage) from the received image.

[0048] In step S16, if the digital signature is detected and it is determined that the condition of the detected screen is in good condition (for example, in intact condition) in step S15, the server computer 20 stores on the storage unit the digital signature, insurance contract information indicating that insurance is valid for the screen displaying the digital signature, and insurance policy information. Namely, in this step, insurance for protection of the screen of the mobile device 10 is issued. In addition, the server computer 20 extracts the digital fingerprint from the received image and stores the digital fingerprint on the storage unit. Furthermore, the insurance contract information (and information on the issue of the insurance) is transmitted to the mobile device 10.

[0049] According to the above processing, where the server computer 20 detects the digital signature and determines that the condition of the detected screen is in good condition (for example, in intact condition) the insurance for the screen of the mobile device 10 is issued. Therefore, it is possible to judge whether or not it is an appropriate screen (undamaged screen) for insurance issuance without depending on a physical inspection of the screen.

[0050] In addition, the server computer 20 detects the digital signature and the condition of the screen of the mobile device 10 from a single image received from the mobile device 10. As a result, it is possible to determine the identification information of the mobile device 10, the timing of insurance contract request (which can be obtained from the time stamp of the digital signature), and the condition of the screen by a single communication between the mobile device 10 and the server computer 20. In other words, the procedures for issuance of insurance contracts can be simplified.

[0051] In one implementation of this invention, the flow of processing performed at mobile device 10 and server computer 20 when submitting an insurance claim for damage to the screen of mobile device 10 (for example, cracking of the screen) is described in FIG. 6.

[0052] In step S21, in response to the operation by the user who files the screen insurance claim, the mobile device 10 reads the digital signature stored on the storage unit and displays it on the screen. The damaged screen on which the digital signature is displayed is photographed by the camera. The image capture can be performed by various methods as already described above. The image captured here can be referred to as a pre-repair image.

[0053] In step S22, the mobile device 10 transmits the pre-repair image obtained above to the server computer 20 in association with the screen insurance claim. If the image is captured by a camera of a device other than the mobile device 10, the obtained image may be transmitted to the server computer 20 by an apparatus other than the mobile device 10 (for example, client computer 30).

[0054] In step S23, the server computer 20 receives the pre-repair image in association with the screen insurance claim. The server computer 20 detects the digital signature and the damage of the screen from the pre-repair image as received and verifies the validity of the insurance claim for repair of the damage to the screen. In order to verify the validity of the insurance claim, the server computer 20 compares the digital signature of the mobile device 10 stored on the storage unit with the digital signature detected from the received image, and determines whether or not the both correspond to each other. In the above comparison, for example, the identification information, time stamp, and location of the mobile device 10 included in the digital signature are compared. If it is determined to correspond, the server computer 20 judges whether or not the insurance claim for repair of the detected damage is valid based on the valid insurance policy information of the mobile device 10 stored on the storage unit.

[0055] In step S24, the server computer 20 stores the result of determination of the validity of insurance claim (for example, information indicating that insurance claim for the repair of the damaged device is valid), and transmits the result to the mobile device 10.

[0056] According to the above processing, in order to verify the validity of the insurance claim, the server computer 20 compares the digital signature of the mobile device 10 stored on the storage unit with the digital signature detected from the image received in association with the insurance claim from the mobile device 10. By doing this, it can be determined whether the damaged screen is the same as the insured screen. When it is determined to be the same, the server computer 20 judges whether or not the insurance claim for the repair of the detected damage is valid based on the valid insurance policy information of the mobile device 10 stored on the storage unit.

[0057] With reference to FIG. 7, the flow of processing executed in the mobile device 10 and the server computer 20 when reporting the completion of repair after repairing the screen will be described.

[0058] In step S31, in response to an operation by the user who reports the completion of repair of the screen, the mobile device 10 reads the digital signature stored on the storage unit and displays it on the repaired screen. The screen on which this digital signature is displayed is photographed by the camera of the mobile device 10 or the camera of another device. The image photographed here is referred to as a post-repair image.

[0059] In step S32, the mobile device 10 transmits to the server computer 20 the post-repair image of the screen obtained above, in association with a screen repair completion report. If the post-repair image is captured by the camera of a device other than the mobile device 10, the captured image may be transmitted to the server computer 20 by a device other than the mobile device 10 such as the client computer 30.

[0060] In step S33, the server computer 20 receives the post-repair image in association with a screen repair completion report. The server computer 20 detects the digital signature and the condition of the screen from the received post-repair image and confirms whether the repair of the damage has been completed. Specifically, in order to confirm the completion of repair of the damage, the server computer 20 compares the digital signature of the mobile device 10 stored on the storage unit with the digital signature detected from the received image, and confirms that the screen repair completion report is related to the completion of repair of the screen on which the insurance claim was made. Then, the server computer 20 scans the received image and confirms that the screen is repaired and in good condition.

[0061] In step S34, the server computer 20, if completion of repair is confirmed in step S33, stores information indicating that repair has been completed on the storage unit. When the above information is stored on the storage unit, this prevents a second or multiple claims for the same damage. In addition, the server computer 20 notifies the mobile device 10 that the repair completion report has been accepted.

[0062] According to the above processing, when the server computer 20 accepts the repair completion report, this allows for the prevention of second or multiple claims for the same damage. As a result, even if multiple insurance claims are illegally submitted against the same damage, the insurance claim may only be approved once.

[0063] Hardware structure

[0064] With reference to FIG. 8, an example of a hardware configuration of the mobile device 10 will be described. The mobile device 10 includes, but not limited, a control unit 1001, a communication device 1004, a storage unit 1005, a microphone 1006, a camera 1007, a physical keyboard 1008, a screen (display) 1009, a speaker 1010, a wireless modem 1011, and a GPS receiver 1012. The control unit 1001 has a processor 1002 and a memory 1003. Though not shown, these elements are connected by various interfaces to communicate with each other. In the control unit 1001, the processor 1002 reads the computer program stored on the storage unit 1005, develops it in the memory 1003, and executes it, thereby controlling the operation of the hardware elements of the mobile device 10 to implement various functions.

[0065] With reference to FIG. 9, an example of a hardware configuration of the server computer 20 will be described below. Though not limited, the server computer 20 includes a control unit 2001, a communication device 2004, a storage unit 2005, an input device 2006, and an output device 2007. The control unit 2001 has processor 2002 and memory 2003. Though not shown, these elements are connected by various interfaces and communicate with each other. In the control unit 2001, the processor 2002 reads the computer program stored on the storage unit 2005, develops it in the memory 2003, and executes it, thereby controlling the operation of the hardware elements of the server computer 20 to implement various functions.

CLAIMS:

1. A computing device comprising a control unit and a storage unit, wherein the control unit is configured to perform the functions of:

receiving an image in association with a request for an insurance contract, wherein the image has been obtained by taking a photograph of a screen of a mobile device displaying a digital signature generated based on identification information of the mobile device to be insured, and

wherein the photograph is taken by a camera of the mobile device, using a mirror directed to the screen;

detecting the digital signature and a condition of the screen from the received image; and

storing on the storage unit insurance contract information indicating that the insurance is valid for the screen displaying the digital signature where the digital signature is detected and the screen is found to be in good condition.

2. The computing device according to claim 1, wherein the generation of the digital signature is further based on a timestamp indicating the time of the digital signature to be generated.

3. The computing device according to claim 1, wherein the generation of the digital signature is further based on a location of the mobile device.

4. The computing device according to claim 1, wherein the control unit is further configured to perform:

receiving a pre-repair image in association with the filing of an insurance claim;

detecting the digital signature and a damage on the screen from the received pre-repair image;

determining validity of the insurance claim for the damage to the screen based on the stored insurance contract information and the digital signature detected from the received pre-repair image; and

sending the result of the determination of the validity of the insurance claim to the mobile device and storing the result on the storage unit.

5. The computing device according to claim 4, wherein the control unit is further configured to perform:

receiving an post-repair image in association with a report for completion of repair;

detecting the digital signature and a condition of the screen from the received post-repair image;

determining whether or not the screen has been repaired based on the stored insurance contract information and the digital signature and the condition detected from the received post-repaired image; and

storing on the storage unit information indicating that the screen has been repaired where it has been determined that the screen has been repaired.

6. The computing device according to any of claims 1 to 5, wherein the digital signature is displayed in light colour on the screen.

7. A mobile device comprising a control unit, a storage unit, a screen and a camera, wherein the control unit is configured to perform the functions of:

generating a digital signature that is digitally signed based on identification information of the mobile device and is time-stamped;

displaying the digital signature on the screen; and

in association with a request for an insurance contract, sending, to a server computer, an image obtained by the camera when it is determined that a face of the screen displaying the digital signature appears on a mirrored surface directed to the screen, that the screen appears entirely on the mirrored surface and is within the field of view of the camera, and that the face of the screen is parallel to the face of the mirror.

8. The mobile device according to claim 7, wherein the digital signature is displayed in light colour on the screen.

9. A method performed in a computing device comprising a control unit and a storage unit, wherein the method includes the following steps performed under control of the control unit:

receiving an image in association with a request for an insurance contract, wherein the image has been obtained by taking a photograph of a screen of a mobile device displaying a digital signature generated based on identification information of the mobile device to be insured, and

wherein the photograph is taken by a camera of the mobile device, using a mirror directed to the screen;

detecting the digital signature and a condition of the screen from the received image;
and

storing on the storage unit insurance contract information indicating that the insurance is valid for the screen displaying the digital signature where the digital signature is detected and the screen is found to be in good condition.

10. A system including a mobile device and a server computer,

wherein the mobile device comprising a first control unit, a screen and a camera, the first control unit being configured to perform the functions of:

generating a digital signature that is digitally signed based on identification information of the mobile device and is time-stamped;

displaying the digital signature on the screen; and

in association with a request for an insurance contract, sending, to the server computer, an image obtained by the camera when it is determined that a face of the screen displaying the digital signature appears on a mirrored surface directed to the screen, that the screen appears entirely on the mirrored surface and is within the field of view of the camera, and that the face of the screen is parallel to the face of the mirror, and

wherein the server computer comprising a second control unit and a storage unit, the second control unit being configured to perform the functions of:

receiving the image in association with the request for the insurance contract;

detecting the digital signature and a condition of the screen from the received image;
and

storing, on the storage unit, insurance contract information indicating that the insurance is valid for the screen of the mobile device displaying the digital signature where the digital signature is detected and the screen is found to be in good condition.