

## METHOD AND SYSTEM FOR DISABLING CAMERA FEATURE OF A MOBILE DEVICE

### Field of the Invention

[0001] The present invention relates to a mobile device. In particular, the invention relates to a method and system for temporary disabling a camera feature of a mobile device.

### Background

[0002] With rising concerns over security and privacy, many facilities restrict or prohibit still or video photography. However, it is a challenge to enforce such restriction ever since the camera is integrated with or can be added to mobile devices, such as mobile phones, PDA.

[0003] The most straightforward solution to such restriction is to prohibit all such mobile devices to be carried into the restricted area. All individuals are required to hand over their mobile devices before entering the restricted area. Security officers are often appointed at the entrance checkpoint of the restricted areas to perform checking to ensure that only owners of non-camera mobile devices are allowed to access the restricted areas. However, such method may not always be practical and it often causes a crowd at the entrance checkpoint. Besides, it requires additional storage space to keep the handed over devices temporary and safely. Moreover, as the mobile devices are getting smaller in size, it makes the restriction more difficult to be exercised when the user does not declare prior to entering the restricted areas.

[0004] As the camera feature is becoming popular, it would be difficult to find in the market a mobile device not integrated with a camera. As these mobile devices are multifunctional, where the individual uses the mobile devices often for non-photography purpose, such as making phone call or scheduling with e-calendar, and many more. It becomes inconvenient for users who rely heavily on most of the non-

camera related features, when they are prohibited to carry the mobile device in to the restricted areas merely because of the camera feature.

### Summary

**[0005]** The present invention seeks to provide a method and system for disabling a camera feature of a mobile device. The system provides a software module that engages the camera feature of the mobile device to deny other applications from utilizing the same, thereby disabling the camera feature. The camera feature disablement occurred when a first control signal is received. The camera feature is enabled/restored when a second control signal is received to trigger the software module to disengage the camera feature.

**[0006]** According to one aspect of the present invention, there is provided a method for disabling/enabling a camera feature of a mobile device, the method comprises executing a software module on the mobile device; receiving a first control signal, wherein the software module extracts commands from the control signal; engaging the camera feature based on the commands to deny other applications on the mobile device from utilizing the camera feature, thereby disabling the camera feature, receiving a second control signal, wherein the software module extracts commands from the second control signal; and disengaging the camera feature thereby allowing the camera feature to be utilized by the other applications on the mobile phone.

**[0007]** In accordance with another aspect, there is provided a system for disabling/enabling a camera feature of a mobile device. The system comprises a software module executable on the mobile device, which is operable to engage the camera feature upon receiving a first control signal to deny other applications on the mobile device from utilize the camera feature, thereby disabling the camera feature. The software module is further operable to disengaging the camera denial feature when a second control signal is received, thereby allowing the camera to be utilized by the other applications on the mobile phone.

[0008] In one embodiment, the method and system verifies an authenticity contained in the commands of the second control signal against the first control signal. The authenticity may include a password or the like. The software module may be configured to execute at startup of the mobile device. Operationally, the method and system shuts down other applications utilizing the camera feature, before engaging the camera feature. The system and method may also reboot the mobile device for shutting down the other applications.

[0009] In another embodiment, the commands of the first control signal may include a prescribed time period, and the camera feature is enabled (restored) to other application after expiration of the prescribed time period.

[0010] In yet another embodiment, the first and second control signal may be in a form of short messaging service message received wirelessly. Alternatively, the first control signal and/or the second control signal may be created via entering commands through the software module manually.

#### Brief Description of the Drawings

[0011] This invention will be described by way of non-limiting embodiments of the present invention, with reference to the accompanying drawings, in which:

[0012] **FIG. 1** illustrates a schematic block diagram of a mobile communication device in accordance with one embodiment of the present invention;

[0013] **FIG. 2** illustrates a process for disabling camera feature of a mobile communication device when the owner of device is entering a restricted area in accordance with one embodiment of the preset invention; and

[0014] **FIG. 3** illustrates a process for disabling camera feature of a mobile device in accordance with one embodiment of the present invention.

## Detailed Description

[0015] In line with the above summary, the following description of a number of specific and alternative embodiments are provided to understand the inventive features of the present invention. It shall be apparent to one skilled in the art, however that this invention may be practiced without such specific details. Some of the details may not be described at length so as not to obscure the invention. For ease of reference, common reference numerals will be used throughout the figures when referring to the same or similar features common to the figures.

[0016] **FIG. 1** illustrates a schematic block diagram of a mobile communication device **100** in accordance with one embodiment of the present invention. The mobile communication device **100** can be any portable device having a camera feature and wireless communication features, such as GSM, Bluetooth, Wi-Fi and etc. The features can be any hardware or software based features accessible by the user of the mobile communication device **100**. The mobile communication device comprises a camera server **102**, a plurality of applications **104** and a software agent **110**. The camera server **102** is a controller for controlling the camera feature of the mobile communication device **100**. The applications **104** are provided to utilize the camera feature of the mobile communication device **100**. The applications **104** may include any one or more of a barcode scanner application, a name card scanner application, a video recording application and any third party applications adapted to utilize the camera feature. The software agent **110** is configured to communicate with the camera server **102**, and when its owner/user enters a restricted area, it is operable to disable the camera feature of the mobile communication device **100**.

[0017] Still referring to **FIG. 1**, when the mobile communication device **100** enters a restricted area, a command signal is sent to the software agent **110** via the wireless communication feature to disable the camera feature. Depending on the route of communication used, the command signal can be transmitted to the mobile communication device **100** in various forms. For example, the command signal can be sent through the GSM communication link as a short messaging service (SMS). The

command signal contains restriction policies and/or a prescribed time period for camera disablement. To prevent the user of the mobile communication device 100 from reversing the executions by the software agent 110, the control signal may further contain a password for enforcing the policies. Such control signal generally cannot be viewed by the user or it is encrypted when received by the mobile communication device 100, and once the control signal is parsed by the software agent 110, the control signal will be removed/deleted from the mobile communication device 100. When the software agent 110 detects that the control signal is to disable the camera within the prescribed time period or until another control signal is received to restore (to enable) the functionality of the camera feature, the software agent 110 monopolies the logical connection with the camera server 102 to engage the camera feature. Before the camera feature is restored, all other applications 104 attempting to utilize the camera feature of the mobile communication device 100 are denied as the camera feature is already engaged by the software agent 100. The camera feature disablement is no longer required, generally upon owner/user of the mobile communication device 100 exits the restricted area or the prescribed time period expires. In the case another control signal is required to restore the functionality of the camera feature, the software agent 110 needs to validate the control signal and when the control signal is verified to be a desired control signal to restore the functionality of the camera feature, the software agent 110 disengages the logical connection with the camera server 102 which allows other applications 104 to use the camera feature of the mobile communication device 100 as desired.

[0018] The software agent 110 records a camera status data and when the software agent 110 is turned on or rebooted, the software agent 110 reads the camera status data and put the camera feature into the recorded status accordingly. For example, when the current camera status data recorded that the camera feature is disabled, when the software agent 110 is rebooted, the software agent 110 automatically disables the camera feature after the software agent 110 is booted up. Further, the software agent 110 can be configured to automatically start up when the mobile communication device 100 is rebooted, accordingly, the software agent 110 can always

maintain a status of the camera feature even when the mobile communication device 100 is rebooted by the user. Thus, when the camera feature is disabled by the software agent 110, even if the user reboots the mobile communication device 100, when the mobile communication device 100 is restarted, the camera feature can still be disabled by the software agent 110. The functionality of the camera feature can only be restored once another control signal to enable to the camera feature is received, or the prescribed time period expires.

[0019] The control signal generally contains commands that are readable by the software agent 110. The control signal may comprise any of the restriction policy information, a prescribed time period, password, enabling/disabling instruction, and etc. The control signal can be sent via any of the communication channels available to the mobile communication device 100 and the control signal can be in a form appropriate to the communication channels used. When required, the control signal can be an encrypted signal for transmission.

[0020] Instead of a control signal that are sent wirelessly, the software agent 110 can be triggered to enable/disable the camera feature of the mobile communication device manually in accordance with another embodiment of the present invention. When in used, the software agent 110 prompts to enter a password or the like to disable the camera feature of the mobile communication device 100. After the password is entered, the software agent 110 engages the camera feature to prevent other applications 104 from using it, thereby disabling the camera feature. To restore the functionality of the camera feature, the password is required to be entered again to disengage the camera feature.

[0021] FIG. 2 illustrates a process for disabling camera feature of a mobile communication device 100 when the owner or user of the device 100 is entering a restricted area in accordance with one embodiment of the preset invention. The process comprises providing a software agent in step 202; executing the software agent 110 in step 204; receiving a controller signal in step 206; reading and parsing policy in step

208; and activating/deactivating a camera feature in steps 210. In the step 202, it is required that the mobile communication device 100 is provided with the software agent 110. The software agent 110 can be pre-installed or be installed as required. Once installed, the software agent 110 is executed and running at the background of the mobile device in the step 204. In step 206, the software agent 110 awaits a control signal to be received. The control signal can be any transmission signal that contains an appropriate command for disabling the camera feature, such as a configuration SMS, or the like. The control signal can be sent through any of the communication channels of the mobile communication device 100, such as GSM, GPRS, Bluetooth etc. When the software agent 110 verified that the control signal is the appropriate command, the software agent 110 reads and parses the control signal to extract the control policy in step 208. Based on the commands and parameters parsed from the control signal, the operation to enable/disable the camera feature is carried out accordingly in the step 210.

[0022] In step 206, the signal can be sent in various ways. In one embodiment, the control signal is transmitted to the mobile communication device 100 automatically when owner/user of the mobile communication device 100 enters the restricted area. Location based services and global positioning system, for example can be used to detect if owner/user of the mobile communication device 100 enters the restricted area. In another embodiment, the message is sent from a control station manually where the mobile communication device 100 is required to register with the entrance checkpoint upon entering the restricted area.

[0023] To prevent unauthorized activation of the camera feature, the control signal may include authentication data for disabling and enabling the camera feature. The authentication data can be a password. Accordingly, once the camera feature is disabled, it can only be enabled with an appropriate authentication data.

[0024] FIG. 3 illustrates a process for disabling camera feature of a mobile device in accordance with one embodiment of the present invention. The process comprises shutting down application running the camera feature in step 302; engaging

the camera feature in step 304; prompting message when other application is accessing the camera feature in step 306; checking if time period for disablement expires in step 308; receiving another control signal for restoring in step 310; checking presence of authentication in step 312; and disengaging the camera feature in step 314. In the step 302, the software agent 110 performs a check to see if any other application 104 is utilizing the camera feature. If any active application is utilizing the camera feature, the software agent 100 shuts down the active application. A non-limiting example of shutting down the action application is by rebooting the operating system of the mobile communication device. In the step 304, the camera feature starts to monopoly the camera server 102, thereby engaging the camera feature. When another application is attempted to utilize the camera feature thereafter, a message will be prompted to show that the camera feature is currently disabled, or the camera feature cannot be activated in the step 306. In the step 308, the software agent 110 checks if the prescribed time-period to disable the camera feature expires. If so, the software agent 110 restores the functionality of the camera feature. If the prescribed time-period has not expired, the software agent 110 awaits for the next control signal to restore the functionality of the camera feature, and if no other control signal is received to enable the camera feature, the camera feature remains engaged by the software agent 110 thereby disabling other applications 104. When the software agent 110 receives a control signal to restore the functionality of the camera feature in step 310, the software agent checks for matching authenticity in step 312. If the control signal contains a matching authenticity, the software agent 110 disengages the camera feature thereby allowing other applications to utilize the camera feature. If the control signal does not contain a matching authenticity, the software agent 110 ignores the control signal and keeps the camera feature disabled.

[0025] Whenever possible, the software agent 110 is generally configured to have a high priority level to prevent interruption by other applications during its operations.

[0026] In an alternative embodiment, the software agent 110 shuts down the active application in step 302 by way of automatically rebooting the mobile communication device 100. After the mobile communication device 100 is rebooted, the software agent 110 is executed at startup and engages the camera server 102 to disable the camera feature.

[0027] The following non-limiting examples illustrate various methods of transmitting the control signal to enable/disable the camera feature.

[0028] Example 1: Via Bluetooth

[0029] The Bluetooth of the mobile communication device is required to be turned on to receive a control signal to enable/disable the camera feature. The Bluetooth transceiver at the restricted area is adapted to search for any active Bluetooth device and once detected, the Bluetooth transceiver sends a control signal to enable and disable the camera feature of the mobile communication device.

[0030] Example 2: Via Global Positioning System (GPS)

[0031] A mobile communication device with GPS receiver is able to detect a location of the mobile communication device. The software agent further provides a database of camera-restricted area and when the software agent detects that the mobile communication device is within the restricted area, the software agent automatically engages the camera feature to disable the camera feature.

[0032] In an alternative embodiment of the present example, the database of camera-restricted areas is stored at a remote location accessible by the mobile communication device.

[0033] Example 3: Via SMS

[0034] The mobile communication devices can receive the control signal in a form of SMS message, typically via GSM network. The SMS message contains simple messages/commands and parameters recognized by the camera control agent to perform the camera disablement/enablement operation. The transmission can be done manually or automatically. For manual SMS transmission, the SMS can be sent by the security officer before owner/user of the mobile communication device enters the restricted area. And when owner/user of the mobile communication device leaves the restricted area, another SMS is required to restore the functionality of the camera feature. For automatic SMS transmission, the SMS message is sent automatically to engage the controller agent to disable the camera feature when owner or user of the mobile communication device enters the restricted area. A location-based service may be used to automatically detect if the owner/user of the mobile communication device enters the restricted area.

[0035] It is understood that the camera feature includes an imaging device that can be in-built or connected to the mobile devices as a peripheral device/accessory in accordance with the present invention. Also, the camera feature can be used to capture still image or video. It is also understood that a mobile communication device 100 can include more than one camera feature, for example a secondary camera for video calls.

[0036] It is also understood that it needs not necessary be a mobile communication device 100 as illustrated above. It can be any portable device capable of taking picture or video, such as personal data assistant (PDA) and the like.

[0037] While specific embodiments have been described and illustrated, it is understood that many changes, modifications, variations and combinations thereof could be made to the present invention without departing from the scope of the invention.

## Claims

1. A method for disabling/enabling a camera feature of a mobile device, the method comprising:
  - executing a software agent on the mobile device;
  - receiving a first control signal, wherein the software agent extracts commands from the control signal;
  - engaging the camera feature based on the commands to deny other applications on the mobile device from utilizing the camera feature, thereby disabling the camera feature,
  - receiving a second control signal, wherein the software agent extracts commands from the second control signal; and
  - disengaging the application denying feature thereby allowing the camera feature to be utilized by the other applications on the mobile phone.
2. The method according to claim 1, further comprising verifying an authenticity contained in the commands of the second control signal against the first control signal.
3. The method according to claim 2, wherein the authenticity includes a password.
4. The method according claim 3, wherein the software agent is executed at startup of the mobile device.
5. The method according to any one of the preceding claims, further comprising shutting down other application utilizing the camera feature, prior to engaging the camera feature.
6. The method according to claim 5, wherein the step of shutting down other application utilizing the camera feature includes rebooting the mobile device.

7. The method according to any one of the preceding claims, further comprising prompting message that the camera feature is not available, when other application is executed to utilize the camera feature while the software agent is engaging the same.
8. The method according to any one of the preceding claims, wherein the commands of the first control signal include a prescribed time period, and the camera feature is enabled to other application after expiration of the prescribed time period.
9. The method according any one of the preceding claims, wherein the first signal and/or second signal is received via a wireless link.
10. The method according to claim 9, wherein the first and second control signal are in a form of short messaging service message.
11. The method according to any one of the preceding claims, wherein the first control signal and/or the second control signal is created via entering commands through the software agent manually.
12. A system for disabling/enabling a camera feature of a mobile device, the system comprising:
  - a software module executable on the mobile device, said software module is operable to engage the camera feature upon receiving a first control signal to deny other applications on the mobile device from utilizing the camera feature, thereby disabling the camera feature,
  - wherein the software module is operable to disengage the camera feature when a second control signal is received, thereby allowing the camera to be utilized by the other applications on the mobile phone.
13. The system according to claim 12, wherein the software module operable to verify an authenticity of the second control signal against the first control signal.

14. The system according to claim 13, wherein the authenticity includes a password.
15. The system according to any one of the claims 12 to 14, wherein the software module is executed at startup of the mobile device.
16. The system according to any one of the claims 12 to 15, wherein the software module is operable to shut down other application utilizing the camera feature, prior to engaging the camera feature.
17. The system according to claim 16, wherein shutting down other application utilizing the camera feature includes rebooting the mobile device.
18. The system according to any one of the claims 12 to 17, wherein the software module is operable to prompt message that the camera feature is not available, when other application is executed to utilize the camera feature while the software agent is engaging the same.
19. The system according to any one of the claims 12 to 18, wherein the first control signal include a prescribed time period, and the camera feature is enable to other application after expiration of the prescribed time period.
20. The system according any one of the claims 12 to 19, wherein the first signal and/or second signal is received via a wireless link.
21. The system according to claim 20, wherein the first and second control signals are in a form of short messaging service message.
22. The system according to any one of the claims 12 to 21, wherein the first control signal and/or the second control signal is created via entering commands through the software module manually.