

CLAIMS

1. A method for accessing an application program, comprising:

receiving a program lock accessing request of a user, wherein a program lock is running in a user device and is used for managing application programs installed in the user device;

receiving an encryption configuration request of the user, wherein the encryption configuration request includes an identifier of an application program and an encryption level;

determining a relationship between the application program and the encryption level, wherein the encryption level is used for indicating whether the application program is encrypted, the encryption level comprises unencrypted, encrypted, hidden, or hidden and encrypted; if the encryption level of the application program is hidden or is encrypted and hidden, hiding a user interface (UI) interface of the application program;

monitoring an the application program installed in a the user device;

if it is monitored that a the user requests to access the application program, determining whether the application program is encrypted;

if the application program that the user requests to access is encrypted, requesting the user to input verification information, determining whether the verification information is correct;

if the verification information is correct, running the application program that the user requests to access and presenting a running result; and

if the verification is not correct, executing a protection operation to the application program that the user requests to access;

the method further comprising: receiving an application program hidden cancellation request transmitted by the user via the program lock, requesting the user to input a password, and verifying the password;

if the password is correct, displaying the hidden UI interface of the application program again.

~~2. The method of claim 1, further comprising:~~

~~before monitoring the application program installed in the user device,~~

~~determining a relationship between the application program and an encryption level, wherein the encryption level is used for indicating whether the application program is encrypted, the encryption level comprises unencrypted, encrypted, hidden, or hidden and encrypted;~~

~~if the encryption level of the application program is hidden or is encrypted and hidden, hiding a user interface (UI) interface of the application program.~~

~~3. The method of claim 2, further comprising:~~

~~after hiding the UI interface of the application program,~~

~~receiving an application program hidden cancellation request transmitted by the user, requesting the user to input a password, and verifying the password;~~

~~if the password is correct, displaying the hidden UI interface of the application program again.~~

42. The method of claim 1, wherein the determining whether the application program that the user requests to access is encrypted comprises:

querying a relationship between the application program that the user requests to access and the encryption level to obtain the encryption level of the application program that the user requests to access, and determining whether the application program is encrypted according to the encryption level of the application program.

53. The method of claim 1, wherein the executing the protection operation to the application program if the verification is not correct comprises:

prompting the user to input the verification information again and returning to the process of determining whether the verification information is correct;

if the user has inputted error verification information for a predefined number of times, forbidding the running of the application program, or, outputting prompt information prompting the user that the application program cannot be accessed.

64. The method of claim 53, wherein the outputting the prompt information comprises:

informing the user that the application program has a fault via voice or a window.

75. An apparatus for accessing an application program, comprising: a monitoring module, a first determining module, a verification module, a first executing module and a second executing module; wherein

the monitoring module is adapted to monitor an application program installed in a user device;

the first determining module is adapted to determine, when it is monitored that a user requests to access the application program, whether the application program that the user requests to access is encrypted;

the verification module is adapted to request, if the application program that the user requests to access is encrypted, the user to input verification information and determine whether the verification information is correct;

the first executing module is adapted to run, if the verification information is correct, the application program that the user requests to access and present a running result; and

the second executing module is adapted to execute a protection operation to the application program that the user requests to access if the verification information is not correct;

a second determining module, adapted to receive a program lock accessing request of the user, wherein the program lock is running in the user device and is used for managing application programs installed in the user device; receive an encryption configuration request of the user, wherein the encryption configuration request includes an identifier of the application program and an encryption level; determine a relationship between the application program and the encryption level, wherein the encryption level indicates whether the application program is encrypted, and the encryption level comprises unencrypted, encrypted, hidden, or encrypted and hidden; and

a third executing module, adapted to hide a user interface (UI) interface of the application program if the encryption level of the application program is hidden or is encrypted and hidden;

a fourth executing module, adapted to receive an application program hidden cancellation request transmitted by the user via the program lock,

request the user to input a password, verify the password, and display the hidden application program again if the password is correct.

~~8. The apparatus of claim 7, further comprising:~~

~~a second determining module, adapted to determine a relationship between the application program and an encryption level, wherein the encryption level indicates whether the application program is encrypted, and the encryption level comprises unencrypted, encrypted, hidden, or encrypted and hidden; and~~

~~a third executing module, adapted to hide a user interface (UI) interface of the application program if the encryption level of the application program is hidden or is encrypted and hidden.~~

~~9. The apparatus of claim 8, further comprising:~~

~~a fourth executing module, adapted to receive an application program hidden cancellation request transmitted by the user, request the user to input a password, verify the password, and display the hidden application program again if the password is correct.~~

406. The apparatus of claim 75, wherein the second determining module is adapted to query a relationship between the application program that the user requests to access and the encryption level to obtain the encryption level of the application program, and determine whether the application program is encrypted according to the encryption level of the application program.

447. The apparatus of claim 75, wherein the second executing module comprises:

a first executing unit, adapted to prompt the user to input the verification information again and trigger the verification module to determine whether the verification information is correct; and

a second executing unit, adapted to forbid the running of the application program if the user has inputted error verification information for a predefined number of times, or output prompt information prompting the user that the application program cannot be accessed.

428. The apparatus of claim 447, wherein the second executing unit is adapted to inform the user that the application program has a fault via voice or a window.

~~13. A terminal, comprising an apparatus for accessing an application program as claimed in any one of claims 7 to 12.~~

~~14. The terminal of claim 13, wherein the terminal is a cell phone, a palmtop computer or a personal digital assistant (PDA).~~

9. A non-transitory computer-readable storage medium comprising a set of instructions for accessing an application program, the set of instructions to direct at least one processor to perform acts of:

receiving a program lock accessing request of a user, wherein a program lock is running in a user device and is used for managing application programs installed in the user device;

receiving an encryption configuration request of the user, wherein the encryption configuration request includes an identifier of an application program and an encryption level;

determining a relationship between the application program and the encryption level, wherein the encryption level is used for indicating whether the application program is encrypted, the encryption level comprises unencrypted, encrypted, hidden, or hidden and encrypted; if the encryption level of the application program is hidden or is encrypted and hidden, hiding a user interface (UI) interface of the application program;

monitoring the application program installed in the user device;

if it is monitored that the user requests to access the application program, determining whether the application program is encrypted;

if the application program that the user requests to access is encrypted, requesting the user to input verification information, determining whether the verification information is correct;

if the verification information is correct, running the application program that the user requests to access and presenting a running result; and

if the verification is not correct, executing a protection operation to the

application program that the user requests to access;

the method further comprising: receiving an application program hidden cancellation request transmitted by the user via the program lock, requesting the user to input a password, and verifying the password;

if the password is correct, displaying the hidden UI interface of the application program again.