SECURE PORTABLE EMAIL CLIENT SYSTEM

Field of the Invention

[0001] The present invention generally relates to electronic communications, and more particularly to a secure portable email client system enabling an email user to securely manipulate emails both online and offline with a portable device.

Background of the Invention

[0002] Flash memory/non-volatile storage devices such as USB storage devices, SD card, CF, and MMC have become more and more popular in electronics users because they offer convenience for being small in size and being compatible with different hosts such as PCs and PDAs. The flash memory/non-volatile storage devices enable a user to transfer data among different computers that are not otherwise connected. Because these devices utilize a non-volatile solid-state memory as the storage medium, they do not require moving parts or a mechanical drive mechanism for accessing data, resulting in more rapidly reading and writing to the memory.

[0003] Emails have become a part of our lives. Typically, receiving and sending an email requires the use of a personal computer (PC) that is connected to an electronic network such as a local area network or the internet. This creates problems. For example, a user has to use his own PC to view his saved emails if he travels to a location where there is no access to a network. In addition, if a user uses another person's PC to access or view his emails, the emails may be downloaded to the PC's memory, resulting in compromised privacy and security. Furthermore, current email programs such as Microsoft Outlook® are installed in PCs that are so often configured to retrieve email from a preset account. Thus in order to access email from a different account, the email program settings must be reconfigured so that the program retrieves email from the user's email account instead of the PC's owner's email account. Reconfiguring the program settings can be time consuming and difficult.

[0004] US 2003/0174167 discloses a system for accessing and transporting electronic communications using a portable data storage device. More specifically, the disclosed system comprises a portable memory device that is capable of easy connection to

a PC via a USB port or similar port, and an email program, so that the disclosed system allows a user to view, send and save emails via the portable memory device connected to a PC. The disclosed system addresses the issues of convenience, but has its drawbacks. For example, the disclosed system does not prevent another person from accessing the saved emails on the portable memory device if the another person is capable of hackling the password of the user's email account.

[0005] Therefore, there is an imperative need to have a portable email system that can provide maximum security to an user for his emails. This invention satisfies this need by disclosing a secure portable email client system. Other advantages of this invention will be apparent with reference to the detailed description.

Summary of the Invention

[0006] The present invention provides a secure portable email client system for enabling an email user to manipulate emails both online and offline. In one embodiment of the present invention, the secure portable email client system comprises a portable device capable of connecting to and being removed from an external host via an interface, and a secure portable email client program preinstalled in the portable device. The present invention further provides that the program includes a Software Authentication Key (SAK) for program run time verification and anti-piracy protection. In one embodiment of the present invention, the secure portable email client program has at least two copies of the SAK, one is pre-stored in an unused area of the portable device and another is hard-coded in the program; thereby when the program starts, the program will compare the pre-stored SAK in the unused area with the hard-coded SAK from the program so that the secure portable email client program is anti-piracy.

[0007] Accordingly, one objective of the present invention is to enable a user to securely manipulate emails both online (sending or receiving) and offline (checking or editing) in a portable device.

[0008] The objectives and advantages of the invention will become apparent from the following detailed description of preferred embodiments thereof in connection with the accompanying drawings.

Brief Description of the Drawings

[0009] Preferred embodiments according to the present invention will now be described with reference to the Figures, in which like reference numerals denote like elements.

[0010] FIG 1 is an illustrative diagram showing that a secure portable email client system in accordance with present invention enables an authorized email user to securely manipulate email both online and offline with a portable device.

[0011] FIG 2 is an illustrative diagram showing a typical communication interface between a host PC and a portable device.

[0012] FIG 3 depicts utilization of a non-volatile memory that is divided into two storage locations: one is a used area and another an unused area.

[0013] FIG 4 briefly summarizes certain features of the secure portable email client system in accordance with the present invention.

[0014] FIG 5 is a flow chart showing utilization of software authentication key to protect intellectual property of the secure portable email client program.

[0015] FIG 6 is a flow chart showing of how to create/verify user login profile in accordance with one embodiment of the present invention.

[0016] FIG 7a is a flow chart of email database compression by way of click-and-compress in accordance with one embodiment of the present invention.

[0017] FIG 7b is a flow chart of email database compression by way of download-and-compression in accordance with one embodiment of the present invention.

[0018] FIG 8a is a flow chart of email database encryption by way of download-and-encrypt in accordance with one embodiment of the present invention.

[0019] FIG 8b is a flow chart of email database encryption by way of click-and-encrypt in accordance with one embodiment of the present invention.

[0020] FIG 9 shows the configuration of the aforementioned features in the secure portable email client system illustrating the relations among the features.

Detailed Description of the Invention

[0021] The present invention may be understood more readily by reference to the following detailed description of certain embodiments of the invention.

[0022] Throughout this application, where publications are referenced, the disclosures of these publications are hereby incorporated by reference, in their entireties, into this application in order to more fully describe the state of art to which this invention pertains.

[0023] The present invention provides a secure portable email client system that provides an email user with both convenience and security. The secure portable email client system comprises a portable device **205** and a secure portable email client program residing in the portable device discussed in detail hereinafter. As shown in FIG 1, the secure portable email client system enables an email user to securely manipulate emails both online and offline, as long as the portable device with the email program is connected to any host PC at any location.

[0024] FIG 2 depicts a typical communication interface between a host PC **200** and the portable device **205**. The portable device **205** comprises a memory controller **202**, a host PC interface **201**, a non-volatile/flash memory **204**, and an interface **203** between the memory controller **202** and the non-volatile/flash memory **204**. The host PC interface **201** between the host PC and the portable device might be USB, CF, SD, etc. The host PC is denoted for any external host for the portable device, wherein the external host includes any personal computer or any electrical devices that have functions similar to the PC.

[0025] Now referring to FIG 3, there is provided more details about the non-volatile/flash memory **204**. The non-volatile/flash memory is logically divided into two storage locations: one is called the used area/standard file system area **300** and another the unused area **301**. The used area **300** is used to store the secure portable email client program **302** and data files with standard file format such as FAT, FAT32, NTFS, etc. A user is able to copy, paste, or delete files at the used storage location. The user is also able to format this used memory area. The used storage location has logical address such as CHS and LBA access. In contrast, the unused area **301** is used to store security information **303** such as user profiles and password, SMTP/POP3 login name and password, cryptographic key, etc. A user cannot access to this area without specific command or write/erase/format this area. The unused storage location has specific physical address to access to this area. Note that the secure portable email client program **302** is resided in used area **300** of the portable device **205** so as to enable a user to launch/execute the program in a host system. On the other hand, the program **302** is able

to access/retrieve security information **303** directly from the unused area **301** by using vendor specific commands.

[0026] FIG 4 is a summary of certain features of the secure portable email client program **302** in accordance with embodiment of the present invention.

[0027] 1. Vendor specific command access **401**

[0028] The unused flash memory area **301** is employed to store security information such as manufacturing ID, user profile and password, SMTP/POP3 user name and password, cryptographic key, etc. The secure portable email client program **302** is able to use vendor specific commands with predefined physical memory address at unused area to perform read/write/erase operation. The security information is encrypted before stored into unused area so as to enhance the security level of the secure portable email client system.

[0029] 2. Software Authentication Key (SAK) **402**

[0030] The software authentication key (SAK) is used to protect the intellectual property of the secure portable email client program **302**. The SAK has duo functions. One is to make sure that a user is only able to execute/launch the secure portable email client program **302** from an authenticated portable device that has preinstalled the program **320** by the manufacturer. Another is to make sure that during the program run time process, the portable device is always connected to a computer because the program **302** will continuously check the SAK from the unused area **301**. The program will discontinue/stop if the user fails to plug in the portable device. In one embodiment of the present invention, the secure portable email client program utilizes only one SAK but with two copies: one is preinstalled into the unused memory area of the portable device, while another is hard-coded into the program itself. Now, FIG 5 shows a flow chart of utilization of the SAK to protect intellectual property of the secure portable email client program. When the program **302** starts **500**, it retrieves the SAK **510** from the unused area **301**, and then compares it with the hard-coded copy within the program **515** to check whether the retrieved SAK is valid **520**. If the retrieved SAK is valid, it continues to execute main programs including processes **570**. After the program finishes all the processes, it will come to an end **580**. Back to step **520**, if the retrieved the SAK is invalid, the program will automatically detect the connection of the portable device with the computer **540**. If no connection of the portable device with the computer is detected, the program will stop **560**

to an end **580**. If the connection of the portable device with the computer is detected, the program will retrieve the SAK from the unused area **301** and compare the retrieved SAK with the hard-coded copy to see whether the SAK is valid **550**. If the SAK is valid, then the program will go the step **530** and the subsequent steps. If the SAK is invalid, then the program will go to step **560** and the subsequent steps.

[0031] 3. User Access Control **403**

[0032] To prevent illegal access to email database, a special login message box will pop up before user is able to access to email database. FIG 6 is an exemplary flow chart showing the user access control methodology.

[0033] As shown in FIG 6, when the secure portable email client program **302** starts **600**, the user will be asked whether there is an existing user profile **610**. If the answer is no, the user will be asked to create a new user profile **620** by keying in a new user name **621**, following with a new password **622** and repeat of the password for confirmation **623**. The program will check whether the passwords are matched. If the passwords are matched, the user will be asked whether he wishes to confirm to create a new user profile **624**. If the passwords are not matched, the user will be requested to key in a password again **622**. Back to step **624**, if the user does not wish to create a new user profile the program will come to an end **630**. If the user wishes to create a new user profile, the program will encrypt the user name and password **625**. The encrypted user name and password will be stored **626** at the unused memory area **301**. Then the program will go to the main screen **617** of the secure portable email client program. Back to step **610,** if there is an existing user profile at unused memory area, the program will retrieve the stored encrypted user name and password **611** from the unused memory area **301**. Then the user will be requested to key in his user name **612** and password **613** that will be encrypted **614**. The program will compare **615** the encrypted user name and password with the stored ones to check whether there is a match **616**. If there is no match between the encrypted user name and password with the stored ones, the user will be requested to key in his user name and password again following the steps **612, 613, 614, 615**. If there is a match between the encrypted user name and password with the stored ones, the program will go to the main screen **617** of the secure portable email client program. After the user finishes his/her task, the program will come to an end **630**.

[0034] 4. Proprietary database with compression and encryption enhancement **404**

[0035] The secure portable email client program **302** of the present invention provides a proprietary database system to define how email body, email attachment, and email records are stored. It is noted that one of the disadvantages of using portable device is the limited capacity. Hence, compression methodology is deployed to reduce the size of email database system. Exemplary applications of the compression to the email database system are shown in FIG 7a and FIG 7b described in details hereinafter. The compression algorithm may be Huffman algorithm, Lempel-Ziv algorithm, arithmetic algorithm, etc. Moreover, the security of the email database system is enhanced by using encryption methodology. Exemplary applications of the encryption to the email database system are shown in FIG 8a and FIG 8b described in details hereinafter. The encryption algorithm may be Data Encryption Standard, Advanced Encryption Standard, etc. It will become apparent later that the proprietary email database system of the present invention provides superior security to all common email systems because the common email systems apply compression and encryption only at the time when an email is being sent or received so as to avoid the email from being intercepted by unauthorized person during email transmit over the Internet.

[0036] The program will automatically/selectively compress and encrypt an email and any accompanying attachment based on certain criteria/condition such as sender's email address, file size, file type, and etc. The program provides two options for user to utilize email database compression as shown in FIG 7a and FIG7b.

[0037] FIG 7a is a flow chart showing the email database compression by way of click-and-compression in accordance with one embodiment of the present invention. After the secure portable email client program **301** starts **700**, if a user chooses to compress an email **710**, the program will compress the email fields based on the user's preferences **711**. Then the program will check whether the compression ratio is acceptable **712**. If the compression ratio is not acceptable, the program will undo the compression **713** so that the email fields remain uncompressed. If the compression ratio is acceptable, the program will continue to compress the attachment fields based on the user's preferences **714**. Then the program will check whether the compression ratio is acceptable **715**. If the compression ratio is not acceptable, the program will undo the compression **716** so that the attachment

fields remain uncompressed. If the compression ratio is acceptable, then the program will replace the compressed email and its attachment into the database **717** before the compression process comes to an end **720**.

[0038] FIG 7b is a flow chart showing the email database compression by way of download-and-compression in accordance with another embodiment of the present invention. After the portable secure email client program starts **750**, if a new email is received **751**, the program will load the user settings **752**. Then the program will check whether the auto-compression function is on **753**. If the auto-compression function is not on, the program will directly store the email into the database **758**. If the auto-compression function is on, the program will further check whether the email matches the criteria for auto compression **754**. If the email does not match the criteria, the program directly stores it into the database **758**. If the email matches the criteria, the program will compress the email fields based on the user's preferences **755**. Then the program will check whether the compression ratio is acceptable **756**. If the compression ratio is not acceptable, the program will undo the compression **757**, and then save it as uncompressed into the database **758**. If the ratio is acceptable, the program will store the compressed email into the database **758**.

[0039] Still referring to FIG 7b, after the program finishes the email fields, then it continues to check whether this email contains any attachment **759**. If the email does not contain any attachment, the program will end **770**. If the email contains any attachment, the program will first create an attachment folder **760**. Then the program will check whether the auto compression function is on **761**. If the auto-compression function is not on, the program will directly store the attachment into the database **766**. If the auto-compression is on, the program will then check whether the attachment matches the criteria **762**. If the attachment does not match the criteria, the program directly stores it into the database **766**. If the attachment matches the criteria, the program will compress the attachment fields based on user preferences **763**. Then the program will check whether the ratio is acceptable **764**. If the ratio is not acceptable, the program will undo the compression **765**, and then save it into the database **766**. If the ratio is acceptable, the program will store the compressed attachment into the database **766**. The program will check whether there are more attachments **766**. If there are more attachments, the program

will route back to step **759**, and then go through all the subsequent steps of the program as discussed above. If there is no more attachment, the program will end **770**.

[0040] FIG 8a is a flow chart showing the email database encryption by way of click-and-encrypt in accordance with one embodiment of the present invention. As shown in FIG 8a, the secure portable email client program may use a passkey and/or a cryptographic key for the email database encryption. The passkey has the features including: being mainly used for login to the system by an user; being stored inside the Vendor Specification area; having only one copy that can exist at one time and be modified from time to time by the user; and being secondarily used as default key for the encryption process. The cryptographic key has the features including: being used in encryption process to protect the contents of an email confidential; requiring the user to key in on the spot when the program starts; and being stored together with the encrypted contents. One of advantages of using two keys is the provision of flexibility to the users who are able to choose whether to key in different cryptographic keys for every piece of data to be encrypted or to automatically use the passkey as the cryptographic key. Now there is provided a brief description of the flowchart as shown in FIG 8a. After the program starts **800**, the user is required to select an email to be encrypted **810**. Then the program checks whether the user wants to use the passkey to encrypt the email **811**. If the user wants to use the passkey, the program will retrieve the passkey from the unused area **815**. Then the program encrypts the email fields based on the user's preferences **816**. After that, the program will encrypt the attachment fields based on the user's preferences **817**. After all the encryption, the program will place the encrypted email and its attachment in the database **818**,and then come to an end **820**. Now returning to step 811, if the user does not want to use the passkey, the user need to enter a new cryptographic key **812**. Then the user will be instructed to reenter the new cryptographic key for a second time **813**. The program will check whether these two cryptographic keys are match **814**. If the keys do not match, the program will instruct the user to repeat steps **812, 813, 814**. If the keys match, the program will continue to step **816** until the end **820**.

[0041] FIG 8b is a flow chart showing the email database encryption by way of download-and-encrypt in accordance with another embodiment of the present invention. After the portable secure email client program starts **850**, if a new email is received **851**, the program will load the user settings **852**. Then the program will check whether the

auto-encryption function is on **853**. If the auto-encryption function is not on, the program will directly store the email into the database **857**. If the auto-encryption function is on, the program will check whether the email matches the criteria **854**. If the email does not match the criteria, the program directly stores it into the database **857**. If the email matches the criteria, the program will retrieve the Passkey **855**. Then the program will encrypt the email fields based on the user's preferences **856**, and store the encrypted email into the database **857**.

[0042] Still referring to FIG 8b, after the program finishes the email fields, then it continues to check whether this email contains any attachment **858**. If the email does not contain any attachment, the program will end **870**. If the email contains any attachment, the program will first create an attachment folder **859**. Then the program will check whether the auto-encryption function is on **860**. If the auto-encryption function is not on, the program will directly store the attachment into the database **864**. If the auto-compression is on, the program will then check whether the attachment matches the criteria **861**. If the attachment does not match the criteria, the program directly stores it into the database **864**. If the attachment matches the criteria, the program will retrieve the Passkey **862**. Then the program will encrypt the attachment field based on the user's preferences **863**, and store the encrypted attachment into the database **864**. The program will check whether there are more attachments **865**. If there are more attachments, the program will route back to step **860**, and then go through all the subsequent steps of the program as discussed above. If there is no more attachment, the program will end **870**.

[0043] 5. Send/Receive Email **405**

[0044] The secure portable email client program **302** comprises algorithms for sending and receiving emails by different types of email protocols such as SMTP/POP3, IMAP, etc. The program is able to get authentication from an email server so as to send/receive email to/from the email server. The present invention further provides that the email account authentication information (such as SMTP/POP3 user name and password) is stored in the unused area **301** of the portable device, rather than in the used area **300**. Storing of the email account authentication information in the unused area **301** enhances the security of the emails.

[0045] 6. Disk Space Indicator **406**

[0046] The secure portable email client program **302** comprises a disk space indicator to display the available space of the portable device in one embodiment of the present invention. Thus the user is able to efficiently utilize the available space. The main benefit to show memory space in "real time" is to let the user know their available memory disk space so that the user is able to backup his files/emails before the memory is full. In addition, the program is able to alert the user based on certain criteria before the memory is full.

[0047] 7. Backup System **407**

[0048] The secure portable email client program **302** further contains a backup feature to manage the backup email folder (PC based backup) and to alert a user to backup prior to user definition. A backup system is also provided for compression and encryption in order to enhance email database backup security.

[0049] 8. Auto Detect Email Setting **408**

[0050] The secure portable email client program **302** provides a feature of auto-detect email setting in one embodiment of the present invention. The auto-detect email setting feature allows the program to automatically check available email server settings (specified by user) and switch to the correct setting. Thus, the user does not need to change email server setting so long as the setting is correct, and the program will switch to the correct setting such as dial-up or under different LAN setting.

[0051] 9. Multiple email accounts and folders **409**

[0052] The secure portable email client program **302** further comprises a feature of allowing a user to create multiple email accounts and folders in one embodiment of the present invention. The user is able to create more than one email account (such as company email, yahoo, hotmail accounts) under a single email client program. Thus, the user is able to send/receive/download/store email under a single email client system. In addition, the user is also able to organize email folders based on his preferences.

[0053] 10. Address Book/Contact **410**

[0054] The secure portable email client program **302** provides a user to create/edit contact person information such as name, hand phone number, address, etc. In addition, the encryption processes as discussed in feature **404** may be applied to the address book/contact to enhance security level.

[0055] Now there is provided one configuration of the aforementioned features in accordance with one embodiment of the present invention. It is to be appreciated that the provided configuration is for the purpose of illustration only. FIG 9 shows the configuration of the aforementioned features in the secure portable email client system illustrating the relations among the features. The features are numbered from 1 –10 corresponding to the items discussed above. The functions underlying each arrow are summarized herein. The process **901** refers to retrieve the SAK from the unused memory area. This process is called by other processes from time to time to verify that the system is being executed from the authentic portable device. The process **902** takes place when user log in the system. Both the stored username and passkey are retrieved from the unused memory area. The process **903** decrypts the username and passkey retrieved from the unused memory area before verification. The process **904** refers to that the data retrieved from the database is either being compressed or decompressed automatically. The process **905** refers to that the data retrieved from the database is either being encrypted or decrypted automatically. The process **906** refers to the software authentication process of all features during program run time. The process **907** keeps trying on difference server setting. The process **908** retrieves different server setting from the database. The process **909** is sending the email to server while the process **910** is receiving email from the server. The process **911** is to save or updated emails to the database. The process **912** is that when a record is saved or deleted to or from database, the system will first check the disk space usage, and updated it when necessary. The process **913** happens when the disk space usage had gone over limit. The process **914** refers to that records are retrieved from the database for backup to other disk drive. The process **915** will read/write Account information from/to database when user request. Finally, the process **916** will read/write Contact information from/to database when user request.

[0056] While the present invention has been described with reference to particular embodiments, it will be understood that the embodiments are illustrative and that the invention scope is not so limited. Alternative embodiments of the present invention will become apparent to those having ordinary skill in the art to which the present invention pertains. Such alternate embodiments are considered to be encompassed within the spirit and scope of the present invention. Accordingly, the scope of the present invention is described by the appended claims and is supported by the foregoing description.

CLAIMS

What is claimed is:

1. A secure portable email client system for enabling an email user to manipulate emails both online and offline, comprising:

a portable device capable of connecting to and being removed from an external host via an interface; and

a secure portable email client program preinstalled in the portable device; thereby the secure portable email client program enables the email user to securely receiving, reviewing, and storing emails.

2. The secure portable email client system of claim 1, wherein the portable device may be any removable disk which contains flash memory / non-volatile storage such as USB storage device, SD card, CF, and MMC.

3. The secure portable email client system of claim 1, wherein the portable device has one used memory location area and one unused memory location area; wherein the one used memory location area is accessible and can be formatted by the email user; wherein the one unused memory location area is not accessible and cannot be formatted by the email user; and wherein the unused memory area is only accessible with vendor specific command.

4. The secure portable email client system of claim 1, wherein the secure portable email client program includes a Software Authentication Key (SAK) for program run time verification and anti-piracy protection; and wherein the secure portable email client program has at least two copies of the SAK, one is pre-stored in an unused area of the portable device and another is hard-coded in the program; thereby when the program starts, the program will compare the pre-stored SAK in the unused area with the hard-coded SAK from the program so that the secure portable email client program is anti-piracy.

5. The secure portable email client system of claim 1, wherein the secure portable email client program includes an algorithm for encrypting Login name and password so as to prevent email database from illegal access.

6. The secure portable email client system of claim 1, wherein the secure portable email client program includes a proprietary database system with encryption and compression methodology to define how email body, email attachment and email record are stored in the portable memory device, so as to enhance email database security.

7. The secure portable email client system of claim 6, wherein the compression methodology includes click-and-compression and download-and-compression.

8. The secure portable email client system of claim 6, wherein the encryption methodology includes click-and-encrypt and download-and-encrypt.

9. The secure portable email client system of claim 1, wherein the secure portable email client program includes an algorithm for auto detection of preset email server setting.

10. The secure portable email client system of claim 1, wherein the secure portable email client program includes disk space indicator so as to allow the email user to properly backup his files/emails.

11. The secure portable email client system of claim 1, wherein the secure portable email client program includes an algorithm for enabling the email user to compress and encrypt emails before emails are stored in the memory.

12. A secure portable email client program for enabling an email user to manipulate emails both online and offline, said program including a Software Authentication Key (SAK) for program run time verification and anti-piracy protection; and wherein the secure portable email client program has at least two copies of the SAK, one is pre-stored in an unused area of the portable device and another is hard-coded in the program; thereby when

the program starts, the program will compare the pre-stored SAK in the unused area with the hard-coded SAK from the program so that the secure portable email client program is anti-piracy.

13. The secure portable email client program of claim 12, further comprising an algorithm for encrypting Login name and password so as to prevent email database from illegal access.

14. The secure portable email client program of claim 12, further comprising a proprietary database system with encryption and compression methodology to define how email body, email attachment and email record are stored in the portable memory device, so as to enhance email database security.

15. The secure portable email client system of claim 14, wherein the compression methodology includes click-and-compression and download-and-compression.

16. The secure portable email client system of claim 14, wherein the encryption methodology includes click-and-encrypt and download-and-encrypt.

17. The secure portable email client program of claim 12, further comprising an algorithm for auto detection of email server setting.

18. The secure portable email client program of claim 12, further comprising a disk space indicator so as to allow the email user to properly backup his files/emails.

19. The secure portable email client program of claim 12, further comprising an algorithm for enabling the email user to compress and encrypt emails before emails are stored in the memory.

20. A method for securely manipulating an email by an email user through the secure portable email client system of claim 1, said method comprising the steps of:

storing security information by utilizing an unused memory area of the portable device;

accessing to unused memory area such as read/write/erase at physical memory address by vendor specific commands; and

deploying of encryption methodology to enhance email database security.