(12) **BẢN MÔ TẢ SÁNG CHẾ THUỘC BẰNG ĐỘC QUYỀN SÁNG CHẾ**

(19) **Cộng hòa xã hội chủ nghĩa Việt Nam (VN)**
CỤC SỞ HỮU TRÍ TUỆ

(11) **1-0022048**

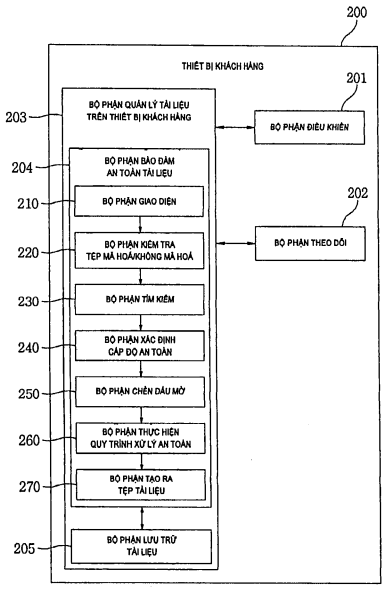
(51)[7] **G06F 21/00**

(13) **B**

(21) 1-2013-03582 (22) 13.11.2013
(30) 10-2013-0106169 04.09.2013 KR
(45) 25.10.2019 379 (43) 25.03.2015 324
(73) MARKANY INC (KR)
10F, Ssanglim bldg, 151-11, Ssanglim-dong, Chung-gu, Seoul, Korea
(72) CHOI, Jong-Uk (KR), CHO, Joo Won (KR), Yusep Rosmansyah (ID)
(74) Công ty TNHH Sở hữu trí tuệ WINCO (WINCO CO., LTD.)

(54) PHƯƠNG PHÁP, THIẾT BỊ KHÁCH HÀNG VÀ HỆ THỐNG TẠO RA TỆP TÀI LIỆU ĐIỆN TỬ ĐỂ NÂNG CAO ĐỘ AN TOÀN CỦA THÔNG TIN KINH DOANH

(57) Sáng chế đề cập đến phương pháp, thiết bị khách hàng và hệ thống tạo ra tệp tài liệu điện tử để nâng cao độ an toàn của thông tin kinh doanh, trong đó phương pháp tạo ra tệp tài liệu điện tử này bao gồm các bước: theo dõi việc tạo ra tệp tài liệu điện tử và các thay đổi của tệp tài liệu điện tử đó, thu nhận tệp quy tắc chứa thông tin thiết lập cấp độ an toàn của tài liệu và quy tắc an toàn, tìm kiếm các từ liên quan đến thông tin kinh doanh từ dữ liệu văn bản tìm được từ tệp tài liệu điện tử, tính điểm số tiếp cận của tệp tài liệu điện tử dựa vào số lần tìm thấy của các từ liên quan đến thông tin kinh doanh và thông tin thiết lập cấp độ an toàn của tài liệu, phân định cấp độ an toàn của tài liệu cho tệp tài liệu điện tử dựa vào điểm số tiếp cận, và chèn dấu mờ vào văn bản của tệp tài liệu điện tử được hiển thị trên thiết bị khách hàng dựa vào thông tin cá nhân của người dùng thu được từ máy chủ. Do đó, có thể ngăn chặn sự rò rỉ tài liệu kinh doanh dưới dạng các tệp tài liệu điện tử chứa thông tin kinh doanh bằng cách sử dụng các biện pháp bảo đảm an toàn sơ bộ và các biện pháp bảo đảm an toàn bổ sung mạnh hơn so với các biện pháp thông thường.



Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập đến phương pháp, thiết bị và hệ thống nâng cao độ an toàn của thông tin kinh doanh. Cụ thể hơn, sáng chế đề cập đến phương pháp tạo ra tệp tài liệu điện tử trên thiết bị khách hàng để nâng cao độ an toàn của thông tin kinh doanh, thiết bị khách hàng tạo ra tệp tài liệu điện tử để nâng cao độ an toàn của thông tin kinh doanh, và hệ thống nâng cao độ an toàn của thông tin kinh doanh, để ngăn chặn sự rò rỉ thông tin kinh doanh.

Tình trạng kỹ thuật của sáng chế

Xã hội hiện đại bước vào thời đại mới là xã hội theo định hướng thông tin nhờ sự đổi mới kỹ thuật và sự phát triển khoa học không ngừng, và do đó, xu hướng làm việc trên các thiết bị thông minh được triển khai trong các cơ quan chính phủ và các doanh nghiệp tư nhân không chỉ ở các quốc gia phát triển mà còn ở các quốc gia đang phát triển, và phần lớn tài liệu được quản lý và truyền ở dạng tài liệu điện tử. Mặc dù hệ thống kinh doanh hoạt động dựa trên các tài liệu điện tử đem đến sự thuận tiện khi sử dụng, nhưng điều không may là, hệ thống này vẫn có những tổn thất do sự rò rỉ thông tin kinh doanh cho bên thứ ba gây ra. Cụ thể là, do kỹ thuật hacking ngày càng tinh vi, nên thông tin kinh doanh của các cơ quan chính phủ và các doanh nghiệp tư nhân có thể bị rò rỉ ra ngoài, điều này có thể quyết định sự sống còn của một tổ chức.

Vì vậy, yêu cầu thiết yếu là phải có phương tiện bảo vệ để ngăn chặn sự rò rỉ thông tin kinh doanh. Nhằm bảo vệ các bí mật kinh doanh và ngăn chặn sự rò rỉ thông tin kinh doanh quan trọng, thông thường, giải pháp quản lý các quyền liên quan đến nội dung dạng số (*DRM: Digital Right Management*) hoặc chống thất thoát dữ liệu (*DLP: Data Loss Prevention*) chủ yếu được áp dụng cho hệ thống bảo đảm an toàn cho thông tin kinh doanh.

Đơn sáng chế với tên sáng chế là "Methods for Digital Rights Management" (đơn sáng chế Hàn Quốc số 2008-0064164) của Intertrust Technologies Corporation mô tả phương pháp và hệ thống liên quan đến kỹ thuật quản lý các quyền liên quan đến nội

dung dạng số, đánh giá sự cho phép sử dụng liên quan đến nội dung được bảo vệ và xác định xem có hay không cho phép truy nhập nội dung theo yêu cầu hoặc khả năng truy nhập khác. Để quản lý các quyền liên quan đến nội dung dạng số, trước hết, các nội dung được đóng gói, và tài liệu được mã hoá bằng cách gắn thông tin cho phép sử dụng để kiểm soát sự truy nhập của người dùng đối với nội dung tương ứng. Nếu một tài liệu đã mã hoá được phân phối cho người dùng tương ứng, thì người dùng đó có thể truy nhập tài liệu này trong phạm vi khả năng truy nhập đã được phân định cho người dùng bằng cách giải mã tài liệu. Nghĩa là, đây là phương pháp dựa trên phương thức kiểm soát sự truy nhập và mã hoá bằng cách mã hoá và phân phối tài liệu và phương thức kiểm soát sự truy nhập đối với tài liệu đã được giải mã theo khả năng truy nhập của người dùng. Tuy nhiên, phương pháp quản lý các quyền liên quan đến nội dung dạng số (DRM) có nguy cơ là người dùng có khả năng truy nhập tài liệu có thể dễ dàng truy nhập nội dung bất cứ lúc nào, và do đó nội dung có thể bị rò rỉ.

Phương pháp DLP, được áp dụng cho một hệ thống bảo đảm an toàn cho thông tin kinh doanh khác, tìm văn bản bằng cách tìm kiếm tài liệu, xác định cấp độ an toàn, và sau đó tiến hành biện pháp kế tiếp. Symantec, là một công ty tiêu biểu sử dụng phương pháp DLP, tuyên bố rằng "Symantec DLP 11 là giải pháp duy nhất trong lĩnh vực kinh doanh đáp ứng đầy đủ tất cả các khía cạnh liên quan đến việc phát hiện (tìm kiếm các tài liệu bí mật và thông tin cá nhân), giám sát (theo dõi việc sử dụng/khả năng truy nhập), và bảo vệ (tiến hành các biện pháp phòng ngừa sự cố), đó là những chức năng cốt lõi của giải pháp ngăn chặn sự rò rỉ dữ liệu" và rằng "nhờ các chức năng được cải tiến hơn nữa, có thể giảm bớt nguy cơ bị rò rỉ dữ liệu quan trọng do cố ý hoặc do sơ suất có thể ảnh hưởng đến hoạt động kinh doanh của các doanh nghiệp" [IT Daily, 2011]. Tuy nhiên, phương pháp DLP để phát hiện sự rò rỉ nội dung bằng cách tìm kiếm tài liệu được phân phối ở dạng văn bản không mã hoá, và do đó khi tài liệu bị rò rỉ, thì xảy ra vấn đề là văn bản không mã hoá kèm theo cũng có thể bị rò rỉ. Ngoài ra còn xảy ra vấn đề là tài liệu dễ bị hackinh từ bên ngoài do phương pháp này phụ thuộc vào kỹ thuật tìm kiếm dựa trên văn bản không mã hoá.

Các phương pháp DRM và DLP thông thường, là các giải pháp tiêu biểu để bảo đảm an toàn cho thông tin kinh doanh, vẫn còn tồn tại những vấn đề nêu trên. Ngoài ra,

do việc số hoá, nên lượng dữ liệu tăng lên, và cụ thể là, theo các cuộc tấn công sử dụng công nghệ cao như chiến dịch liên tục tấn công có chủ đích vào mạng máy tính của một tổ chức (*APT: Advanced Persistent Threat*), hiện nay xảy ra nhiều trường hợp thông tin được đánh cắp bằng các kỹ thuật mã hoá hoặc giả mạo, và do đó khó có thể ngăn chặn sự rò rỉ thông tin bằng hệ thống bảo đảm an toàn cho thông tin kinh doanh thông thường.

Ngoài ra, liên quan đến một hiện tượng khác xuất hiện trong ngành công nghệ thông tin (*IT: Information Technology*) hiện nay, nhờ vào những thay đổi của nhiều loại thiết bị, hệ thống máy tính thông thường hiện nay tung ra thị trường nhiều loại thiết bị cỡ nhỏ nối tiếp sau các thiết bị di động như máy điện thoại thông minh và máy tính cá nhân (*PC: Personal Computer*) dạng bảng, v.v.. Ngoài các thiết bị tiêu biểu như đồng hồ iWatch của Apple, và kính Google Glasses của Google, nhiều loại thiết bị cỡ nhỏ đang được tung ra thị trường như camera, thiết bị ghi cỡ nhỏ, v.v.. Do đó, vì dễ bị rò rỉ thông tin cho bên thứ ba, nên yêu cầu thiết yếu là phải ngăn chặn sự rò rỉ thông tin thông qua bản quyền của chủ sở hữu và ngăn chặn sự sao chép bất hợp pháp bằng cách chèn dấu mờ vào nội dung. Ngoài ra, do những thay đổi về thiết bị và những thay đổi về môi trường kinh doanh, mục tiêu hacking không chỉ giới hạn ở máy chủ, mà mục tiêu hacking có thể mở rộng đến các thiết bị cá nhân. Vì vậy, cần phải bảo đảm an toàn cho thiết bị cá nhân.

Tài liệu tham khảo về giải pháp kỹ thuật đã biết

Tài liệu sáng chế

(Tài liệu sáng chế 1) Đơn sáng chế Hàn Quốc số 2008-0064164 (ngày công bố đơn: 08.07.2008)

Bản chất kỹ thuật của sáng chế

Để giải quyết vấn đề nêu trên, mục đích của sáng chế là nhằm đề xuất phương pháp, thiết bị và hệ thống nâng cao độ an toàn của thông tin kinh doanh, khắc phục các điểm yếu trong hệ thống an toàn bằng cách kết hợp phương pháp DRM dựa trên phương thức kiểm soát khả năng truy nhập bằng cách mã hoá tài liệu dạng số và phân quyền sử dụng tài liệu dạng số cho từng người dùng, và kiểm tra dữ liệu bằng cách tìm kiếm theo phương pháp DLP.

Ngoài ra, khi kết hợp phương pháp DRM và phương pháp DLP, các hệ thống hiện

có không kết hợp một cách đơn thuần, mà cấp độ an toàn của tài liệu được thiết lập dựa trên điểm số tiếp cận tính mức độ tiếp cận của thông tin kinh doanh bằng chức năng tìm kiếm theo phương pháp DLP, và tài liệu được mã hoá và được xử lý an toàn bằng phương pháp DRM, và do đó có thể kiểm soát khả năng truy nhập đối với từng người dùng. Ngoài ra, chức năng chèn dấu mờ để phân định sự phân biệt không nhìn thấy được được tạo ra trên màn hình được hiển thị cho người dùng xem dựa vào dữ liệu tìm kiếm. Với phương pháp và thiết bị chèn dấu mờ, người làm rò rỉ thông tin có thể được xác định dễ dàng khi tài liệu dạng số bị rò rỉ cho bên thứ ba. Vì vậy, một mục đích khác của sáng chế là nhằm đề xuất phương pháp, thiết bị và hệ thống chèn/phát hiện dấu mờ dưới dạng môđun cơ bản để tăng cường các biện pháp bảo đảm an toàn bổ sung của công ty, điều này được đánh giá cao khi các thiết bị cỡ nhỏ được triển khai.

Một mục đích khác nữa của sáng chế là nhằm nâng cao độ an toàn trong môi trường kinh doanh dựa trên các thiết bị di động cho các loại thiết bị khác nhau và các thiết bị thông minh bằng cách thiết lập hệ thống bảo đảm an toàn dựa trên các thiết bị người dùng. Sáng chế đề xuất biện pháp bảo đảm an toàn sơ bộ bằng cách tìm kiếm các tài liệu và thiết lập các cấp độ an toàn ở ngay trên thiết bị đầu cuối người dùng, chứ không phải hệ thống bảo đảm an toàn trên máy chủ hiện có, và biện pháp bảo đảm an toàn bổ sung bằng cách chèn dấu mờ dạng văn bản. Vì vậy, một mục đích khác nữa của sáng chế là nhằm đề xuất hệ thống bảo đảm an toàn có hiệu quả theo xu hướng chuyển sang môi trường kinh doanh dựa trên các thiết bị di động.

Tuy nhiên, đối tượng của sáng chế không chỉ giới hạn ở các đối tượng nhằm giải quyết các vấn đề nêu trên, và có thể được mở rộng theo nhiều cách khác nhau trong phạm vi không vượt ra ngoài phạm vi của sáng chế.

Để đạt được mục đích của sáng chế, phương pháp tạo ra tệp tài liệu điện tử trên thiết bị khách hàng để nâng cao độ an toàn của thông tin kinh doanh theo các phương án thực hiện sáng chế có thể bao gồm các bước: theo dõi việc tạo ra tệp tài liệu điện tử trên thiết bị khách hàng và các thay đổi của tệp tài liệu điện tử đó, thu nhận tệp quy tắc từ máy chủ, tìm kiếm dữ liệu văn bản từ tệp tài liệu điện tử, tìm kiếm các từ liên quan đến thông tin kinh doanh từ dữ liệu văn bản tìm được, tính điểm số tiếp cận của tệp tài liệu điện tử dựa vào số lần tìm thấy của các từ liên quan đến thông tin kinh doanh và thông tin thiết

lập cấp độ an toàn của tài liệu, phân định cấp độ an toàn của tài liệu cho tệp tài liệu điện tử dựa vào điểm số tiếp cận, thu nhận thông tin cá nhân của người dùng sử dụng thiết bị khách hàng từ máy chủ và chèn dấu mờ vào văn bản của tệp tài liệu điện tử được hiển thị trên thiết bị khách hàng dựa vào thông tin cá nhân của người dùng thu được, dựa vào cấp độ an toàn của tài liệu đã được phân định cho tệp tài liệu điện tử, thực hiện quy trình xử lý an toàn theo quy tắc an toàn, quy trình xử lý an toàn này có một trong số các cách xoá, cách ly, mã hoá và thông báo, và tạo ra tệp tài liệu điện tử được bảo vệ bằng cách chèn thông tin về khả năng truy nhập vào phần đầu của tệp tài liệu điện tử.

Theo phương án thực hiện sáng chế, tệp quy tắc có thể chứa các biểu thức chính quy, các từ khoá, quy tắc an toàn và thông tin thiết lập cấp độ an toàn của tài liệu. Thông tin thiết lập cấp độ an toàn của tài liệu có thể chứa hệ số quan trọng của các từ liên quan đến thông tin kinh doanh, quy tắc về cấp độ an toàn của tài liệu và quy tắc về khả năng truy nhập của người dùng xác định khả năng truy nhập của người dùng đối với tài liệu theo cấp độ an toàn của tài liệu.

Theo phương án thực hiện sáng chế, điểm số tiếp cận có thể được tính là tổng của tích số giữa số lần tìm thấy của các từ liên quan đến thông tin kinh doanh và hệ số quan trọng của các từ liên quan đến thông tin kinh doanh.

Theo phương án thực hiện sáng chế, bước chèn dấu mờ bao gồm bước thay đổi ít nhất một thông số trong số cỡ phông chữ và độ rộng phông chữ của văn bản theo thông tin cá nhân của người dùng.

Theo phương án thực hiện sáng chế, phương pháp này còn bao gồm bước tải tệp tài liệu điện tử từ máy chủ xuống thiết bị khách hàng, bước tải tệp tài liệu điện tử xuống thiết bị khách hàng bao gồm các bước: ở máy chủ, xác minh thông tin đăng nhập của người dùng trên thiết bị khách hàng, xem xét sơ đồ tổ chức và thông tin cá nhân của người dùng từ cơ sở dữ liệu nhân sự trên máy chủ, xem xét tệp quy tắc chứa thông tin thiết lập cấp độ an toàn của tài liệu và quy tắc an toàn từ cơ sở dữ liệu quy tắc trên máy chủ, phân định cấp độ an toàn của tài liệu liên quan đến khả năng truy nhập của người dùng cho tệp tài liệu điện tử dựa vào thông tin thiết lập cấp độ an toàn của tài liệu và chèn dấu mờ vào tệp tài liệu điện tử dựa vào thông tin cá nhân của người dùng, mã hoá tệp tài liệu điện tử sau khi phân định cấp độ an toàn của tài liệu và chèn dấu mờ, và truyền tệp tài liệu điện tử đã

mã hoá từ máy chủ đến thiết bị khách hàng.

Hệ thống nâng cao độ an toàn của thông tin kinh doanh theo các phương án khác để thực hiện sáng chế có thể bao gồm máy chủ có bộ phận xác định quy tắc trên máy chủ được kết nối với cơ sở dữ liệu quy tắc và bộ phận quản lý an toàn được kết nối với cơ sở dữ liệu nhân sự, và thiết bị khách hàng được kết nối với máy chủ qua mạng, thiết bị khách hàng này có bộ phận theo dõi được tạo cấu hình để theo dõi việc tạo ra tệp tài liệu điện tử và các thay đổi của tệp tài liệu điện tử đó, bộ phận điều khiển được tạo cấu hình để thu nhận tệp quy tắc từ cơ sở dữ liệu quy tắc trên máy chủ, và bộ phận bảo đảm an toàn tài liệu, bộ phận bảo đảm an toàn tài liệu này có bộ phận tìm kiếm được tạo cấu hình để tìm kiếm dữ liệu văn bản từ tệp tài liệu điện tử và tìm kiếm các từ liên quan đến thông tin kinh doanh từ dữ liệu văn bản tìm được, bộ phận xác định cấp độ an toàn được tạo cấu hình để tính điểm số tiếp cận của tệp tài liệu điện tử dựa vào số lần tìm thấy của các từ liên quan đến thông tin kinh doanh và thông tin thiết lập cấp độ an toàn của tài liệu và phân định cấp độ an toàn của tài liệu liên quan đến khả năng truy nhập của người dùng cho tệp tài liệu điện tử dựa vào điểm số tiếp cận, bộ phận chèn dấu mờ được tạo cấu hình để chèn dấu mờ vào văn bản của tệp tài liệu điện tử được hiển thị trên thiết bị khách hàng dựa vào thông tin cá nhân của người dùng thu được từ máy chủ, bộ phận thực hiện quy trình xử lý an toàn được tạo cấu hình để thực hiện quy trình xử lý an toàn trên tài liệu điện tử theo quy tắc an toàn dựa vào cấp độ an toàn của tài liệu đã được phân định, quy trình xử lý an toàn này có một trong số các cách xoá, cách ly, mã hoá và thông báo, và bộ phận tạo ra tệp tài liệu được tạo cấu hình để tạo ra tệp tài liệu điện tử được bảo vệ bằng cách chèn thông tin về khả năng truy nhập vào phần đầu của tệp tài liệu điện tử.

Theo phương án thực hiện sáng chế, tệp quy tắc có thể chứa các biểu thức chính quy, các từ khoá, quy tắc an toàn và thông tin thiết lập cấp độ an toàn của tài liệu. Thông tin thiết lập cấp độ an toàn của tài liệu có thể chứa hệ số quan trọng của các từ liên quan đến thông tin kinh doanh, quy tắc về cấp độ an toàn của tài liệu và quy tắc về khả năng truy nhập của người dùng xác định khả năng truy nhập của người dùng đối với tài liệu theo cấp độ an toàn của tài liệu.

Theo phương án thực hiện sáng chế, điểm số tiếp cận có thể được tính là tổng của tích số giữa số lần tìm thấy của các từ liên quan đến thông tin kinh doanh và hệ số quan

trọng của các từ liên quan đến thông tin kinh doanh.

Theo phương án thực hiện sáng chế, bộ phận chèn dấu mờ có thể được tạo cấu hình để thay đổi ít nhất một thông số trong số cỡ phông chữ và độ rộng phông chữ của văn bản theo thông tin cá nhân của người dùng.

Theo phương án thực hiện sáng chế, máy chủ được tạo cấu hình để xác minh thông tin đăng nhập của người dùng trên thiết bị khách hàng, xem xét sơ đồ tổ chức và thông tin cá nhân của người dùng từ cơ sở dữ liệu nhân sự, xem xét tệp quy tắc chứa quy tắc an toàn và thông tin thiết lập cấp độ an toàn của tài liệu từ cơ sở dữ liệu quy tắc, phân định cấp độ an toàn của tài liệu liên quan đến khả năng truy nhập của người dùng cho tệp tài liệu điện tử dựa vào thông tin thiết lập cấp độ an toàn của tài liệu và chèn dấu mờ vào tệp tài liệu điện tử dựa vào thông tin cá nhân của người dùng, và mã hoá tệp tài liệu điện tử sau khi phân định cấp độ an toàn của tài liệu và chèn dấu mờ, và thiết bị khách hàng còn có bộ phận lưu trữ tài liệu được tạo cấu hình để tải tệp tài liệu điện tử đã mã hoá từ máy chủ xuống thiết bị khách hàng.

Thiết bị khách hàng tạo ra tệp tài liệu điện tử để nâng cao độ an toàn của thông tin kinh doanh theo các phương án khác để thực hiện sáng chế có thể bao gồm phương tiện theo dõi việc tạo ra tệp tài liệu điện tử và các thay đổi của tệp tài liệu điện tử đó, phương tiện thu nhận tệp quy tắc từ máy chủ, phương tiện tìm kiếm dữ liệu văn bản từ tệp tài liệu điện tử, phương tiện tìm kiếm các từ liên quan đến thông tin kinh doanh từ dữ liệu văn bản tìm được, phương tiện tính điểm số tiếp cận của tệp tài liệu điện tử dựa vào số lần tìm thấy của các từ liên quan đến thông tin kinh doanh và thông tin thiết lập cấp độ an toàn của tài liệu, phương tiện phân định cấp độ an toàn của tài liệu cho tệp tài liệu điện tử dựa vào điểm số tiếp cận, phương tiện thu nhận thông tin cá nhân của người dùng sử dụng thiết bị khách hàng từ máy chủ và chèn dấu mờ vào văn bản của tệp tài liệu điện tử được hiển thị trên thiết bị khách hàng dựa vào thông tin cá nhân của người dùng thu được, phương tiện thực hiện quy trình xử lý an toàn theo quy tắc an toàn dựa vào cấp độ an toàn của tài liệu đã được phân định, quy trình xử lý an toàn này có một trong số các cách xoá, cách ly, mã hoá và thông báo, và tạo ra tệp tài liệu điện tử được bảo vệ bằng cách chèn thông tin về khả năng truy nhập vào phần đầu của tệp tài liệu điện tử.

Theo phương án thực hiện sáng chế, tệp quy tắc có thể chứa các biểu thức chính

quy, các từ khoá, quy tắc an toàn và thông tin thiết lập cấp độ an toàn của tài liệu. Thông tin thiết lập cấp độ an toàn của tài liệu có thể chứa hệ số quan trọng của các từ liên quan đến thông tin kinh doanh, quy tắc về cấp độ an toàn của tài liệu và quy tắc về khả năng truy nhập của người dùng xác định khả năng truy nhập của người dùng đối với tài liệu theo cấp độ an toàn của tài liệu.

Theo phương án thực hiện sáng chế, điểm số tiếp cận có thể được tính là tổng của tích số giữa số lần tìm thấy của các từ liên quan đến thông tin kinh doanh và hệ số quan trọng của các từ liên quan đến thông tin kinh doanh.

Nhờ phương pháp, thiết bị và hệ thống nâng cao độ an toàn của thông tin kinh doanh theo các phương án thực hiện sáng chế, có thể kiểm soát khả năng truy nhập tài liệu đối với từng người dùng, và tạo ra các biện pháp bảo đảm an toàn sơ bộ mạnh hơn để ngăn chặn sự rò rỉ thông tin kinh doanh trước khi áp dụng biện pháp bảo đảm an toàn phù hợp cho mỗi tài liệu, bằng cách tìm xem tài liệu điện tử có trong công ty có chứa thông tin bí mật của công ty hay không sử dụng kỹ thuật tìm kiếm tài liệu điện tử, tính điểm số tiếp cận dựa vào mức độ tiếp cận và xác định cấp độ an toàn của tài liệu tương ứng, và kiểm soát khả năng truy nhập của người dùng theo từng cấp độ an toàn của tài liệu.

Ngoài ra, có thể theo dõi đường rò rỉ thông tin khi tài liệu bị rò rỉ ra ngoài do thao tác chụp ảnh, v.v. cho bên thứ ba, bằng cách chèn dấu mờ vào tài liệu dựa vào một giá trị cụ thể có thể phân biệt từng người dùng và tạo ra sự phân quyền đối với tài liệu được hiển thị trên màn hình cho từng người dùng xem, và do đó tạo ra các biện pháp bảo đảm an toàn bổ sung cho công ty để triển khai nhiều loại thiết bị cỡ nhỏ.

Tuy nhiên, hiệu quả đạt được của sáng chế không chỉ giới hạn ở các hiệu quả nêu trên, và có thể được mở rộng theo nhiều cách khác nhau trong phạm vi không vượt ra ngoài phạm vi của sáng chế.

Mô tả vắn tắt các hình vẽ

Fig.1 là sơ đồ thể hiện hệ thống nâng cao độ an toàn của thông tin kinh doanh bao gồm máy chủ và thiết bị khách hàng.

Fig.2 là hình vẽ thể hiện thiết bị khách hàng theo phương án thực hiện sáng chế.

Fig.3 là hình vẽ thể hiện bộ phận theo dõi theo phương án thực hiện sáng chế.

Fig.4 là hình vẽ thể hiện bộ phận điều khiển theo phương án thực hiện sáng chế.

Fig.5 là hình vẽ thể hiện tệp quy tắc theo phương án thực hiện sáng chế.

Fig.6 là hình vẽ thể hiện ví dụ về thông tin thiết lập cấp độ an toàn được sử dụng trong sáng chế.

Fig.7 là hình vẽ thể hiện bộ phận tìm kiếm theo phương án thực hiện sáng chế.

Fig.8 là hình vẽ thể hiện bộ phận xác định cấp độ an toàn theo phương án thực hiện sáng chế.

Fig.9 là hình vẽ thể hiện cách chèn dấu mờ bằng cách thay đổi cỡ phông chữ và thay đổi độ rộng phông chữ theo phương án thực hiện sáng chế.

Fig.10 là hình vẽ thể hiện chức năng của bộ phận thực hiện quy trình xử lý an toàn theo phương án thực hiện sáng chế.

Fig.11 là hình vẽ thể hiện cách tạo ra tệp tài liệu có phần đầu theo phương án thực hiện sáng chế.

Fig.12 là hình vẽ thể hiện bộ phận lưu trữ tài liệu theo phương án thực hiện sáng chế.

Fig.13a là lưu đồ thể hiện phương pháp tạo ra tệp tài liệu điện tử trên thiết bị khách hàng để nâng cao độ an toàn của thông tin kinh doanh theo phương án thực hiện sáng chế.

Fig.13b là lưu đồ thể hiện phương pháp tải tài liệu từ máy chủ xuống thiết bị khách hàng để nâng cao độ an toàn của thông tin kinh doanh theo phương án thực hiện sáng chế.

Mô tả chi tiết sáng chế

Nhằm mục đích giải thích rõ về các phương án thực hiện sáng chế, cấu trúc hoặc chức năng cụ thể được trình bày chỉ để làm ví dụ minh hoạ dựa vào các phương án thực hiện sáng chế được mô tả trong phần mô tả chi tiết sáng chế dưới đây. Ngoài ra, các phương án thực hiện sáng chế có thể được thực hiện theo nhiều dạng khác nhau, và không được phép hiểu rằng sáng chế chỉ giới hạn ở các phương án được mô tả trong phần mô tả chi tiết sáng chế.

Sáng chế có thể được thực hiện theo nhiều phương án cải biến khác nhau, và sáng chế có thể có nhiều dạng khác nhau. Vì vậy, các phương án cụ thể để làm ví dụ sẽ được thể hiện trên các hình vẽ và được mô tả chi tiết trong phần mô tả chi tiết sáng chế. Tuy nhiên, sáng chế không chỉ giới hạn ở các phương án cụ thể được mô tả, và cần phải hiểu rằng sáng chế bao gồm tất cả các phương án cải biến, các phương án tương đương hoặc các phương án thay thế nằm trong phạm vi của sáng chế.

Các thuật ngữ dùng trong sáng chế được sử dụng chỉ để mô tả các phương án cụ thể của sáng chế, và các thuật ngữ đó không được sử dụng để giới hạn phạm vi của sáng chế. Danh từ chung dùng trong sáng chế có thể được hiểu theo nghĩa là danh từ đó dùng ở dạng số ít cũng như danh từ đó dùng ở dạng số nhiều, trừ trường hợp trong sáng chế có định nghĩa khác một cách rõ ràng theo ngữ cảnh. Chữ "bao gồm" hoặc "có", v.v. trong sáng chế được sử dụng để biểu thị sự có mặt của các dấu hiệu, trị số, bước, thao tác, bộ phận cấu thành, thành phần được mô tả trong sáng chế hoặc dạng kết hợp của các loại nêu trên, và không được phép hiểu là loại trừ khả năng có mặt hoặc xuất hiện thêm của một hoặc nhiều dấu hiệu, trị số, bước, thao tác, bộ phận cấu thành, thành phần khác hoặc dạng kết hợp của các loại nêu trên.

Tất cả các thuật ngữ dùng trong sáng chế bao gồm cả các thuật ngữ kỹ thuật hoặc khoa học đều có nghĩa giống với nghĩa thường được hiểu đối với người có hiểu biết trung bình về lĩnh vực kỹ thuật mà sáng chế liên quan đến, trừ trường hợp trong sáng chế có định nghĩa khác. Các thuật ngữ như các thuật ngữ được định nghĩa trong từ điển thông dụng phải được hiểu theo nghĩa giống với nghĩa phù hợp với ngữ cảnh dùng trong lĩnh vực kỹ thuật liên quan, và không được phép hiểu theo nghĩa lý tưởng hoặc quá câu nệ, trừ trường hợp trong sáng chế có định nghĩa khác một cách rõ ràng.

Các phương án ưu tiên để thực hiện sáng chế sẽ được mô tả chi tiết dưới đây có dựa vào các hình vẽ kèm theo. Các số chỉ dẫn giống nhau được sử dụng để thể hiện các bộ phận cấu thành giống nhau trên các hình vẽ, và trong sáng chế sẽ không mô tả lại bộ phận cấu thành giống nhau.

Fig.1 là sơ đồ thể hiện hệ thống nâng cao độ an toàn của thông tin kinh doanh. Như được thể hiện trên Fig.1, để ngăn chặn sự rò rỉ thông tin kinh doanh theo phương án thực hiện sáng chế, hệ thống 100 tạo ra tệp tài liệu điện tử để nâng cao độ an toàn của thông

tin kinh doanh bao gồm máy chủ 110 và thiết bị khách hàng 200. Máy chủ 110 có thể có bộ phận xác định quy tắc trên máy chủ 120 và bộ phận quản lý an toàn 130. Thiết bị khách hàng 200 có thể có bộ phận điều khiển 201, bộ phận theo dõi 202, và bộ phận quản lý tài liệu trên thiết bị khách hàng 203.

Máy chủ 110 trong hệ thống 100 tạo ra tệp tài liệu điện tử để nâng cao độ an toàn của thông tin kinh doanh có thể có bộ phận xác định quy tắc trên máy chủ 120 và bộ phận quản lý an toàn 130. Bộ phận xác định quy tắc trên máy chủ 120 thực hiện chức năng quản lý các quy tắc để bảo vệ thông tin kinh doanh và cung cấp các quy tắc đó cho thiết bị khách hàng. Bộ phận xác định quy tắc trên máy chủ 120 có thể có bộ phận quản lý quy tắc 122 và bộ phận truyền quy tắc 124. Bộ phận quản lý quy tắc 122 lưu trữ và quản lý các quy tắc, v.v. để thiết lập cấp độ an toàn của tài liệu và cấp bậc của người dùng liên quan đến khả năng truy nhập theo điểm số tiếp cận liên quan đến thông tin kinh doanh trong tài liệu tương ứng. Bộ phận truyền quy tắc 124 thực hiện chức năng truyền tệp quy tắc tương ứng đến thiết bị khách hàng. Bộ phận quản lý an toàn 130 thực hiện chức năng xác minh thông tin đăng nhập của người dùng, phát hiện thông tin nhật ký, và trợ giúp mã hoá tài liệu. Cụ thể hơn, bộ phận quản lý an toàn này có thể có bộ phận xác minh thông tin đăng nhập 134 để xác minh khả năng truy nhập sau khi từng người dùng đăng nhập dựa vào thông tin người dùng và sơ đồ tổ chức từ cơ sở dữ liệu nhân sự khi người dùng đăng nhập vào máy chủ, bộ phận phát hiện thông tin nhật ký 136 thu nhận và quản lý thông tin liên quan đến việc phát hiện thấy thông tin kinh doanh ở phía khách hàng và thực hiện quy trình xử lý an toàn theo kết quả phát hiện được, và bộ phận mã hoá 132 mã hoá tài liệu và cung cấp tài liệu cho thiết bị khách hàng.

Thiết bị khách hàng 200 trong hệ thống 100 tạo ra tệp tài liệu điện tử để nâng cao độ an toàn của thông tin kinh doanh có thể có bộ phận điều khiển 201 thu nhận tệp quy tắc từ máy chủ và ra lệnh tìm kiếm tệp tài liệu điện tử, bộ phận theo dõi 202 thông báo về sự thay đổi của quy trình xử lý hoặc sự thay đổi của tệp thông qua sự theo dõi PC của người dùng, và bộ phận quản lý tài liệu trên thiết bị khách hàng 203 quản lý tài liệu ở phía thiết bị khách hàng. Ngoài ra, bộ phận quản lý tài liệu trên thiết bị khách hàng 203 có thể có bộ phận bảo đảm an toàn tài liệu 204 thực hiện chức năng bảo đảm sự an toàn của tài liệu và bộ phận lưu trữ tài liệu 205 thực hiện chức năng tải tài liệu lên máy chủ và

sao lưu tài liệu.

Fig.2 là hình vẽ thể hiện chi tiết thiết bị khách hàng 200 theo phương án thực hiện sáng chế. Thiết bị khách hàng 200 có thể có bộ phận điều khiển 201, bộ phận theo dõi 202, và bộ phận quản lý tài liệu trên thiết bị khách hàng 203. Bộ phận quản lý tài liệu trên thiết bị khách hàng 203 có thể có bộ phận bảo đảm an toàn tài liệu 204 và bộ phận lưu trữ tài liệu 205. Các dấu hiệu cụ thể của bộ phận lưu trữ tài liệu 205 được thể hiện trên Fig.12. Cụ thể hơn, liên quan đến bộ phận bảo đảm an toàn tài liệu 204 trong bộ phận quản lý tài liệu trên thiết bị khách hàng 203, bộ phận bảo đảm an toàn tài liệu này có thể có bộ phận giao diện 210, bộ phận kiểm tra tệp mã hoá/không mã hoá 220, bộ phận tìm kiếm 230, bộ phận xác định cấp độ an toàn 240, bộ phận chèn dấu mờ 250, bộ phận thực hiện quy trình xử lý an toàn 260 và bộ phận tạo ra tệp tài liệu 270.

Bộ phận giao diện 210 thu nhận thông tin cảnh báo về việc tạo ra hoặc thay đổi tài liệu từ bộ phận theo dõi 202, thu nhận lệnh tìm kiếm từ bộ phận điều khiển 201, và thu nhận tài liệu đã được tải xuống từ máy chủ từ bộ phận lưu trữ tài liệu 205. Tệp tài liệu điện tử được thu nhận ở bộ phận giao diện 210 và được tải xuống từ máy chủ sẽ được cung cấp cho bộ phận kiểm tra tệp mã hoá/không mã hoá 220 để xác định xem tệp tài liệu điện tử ở dạng được mã hoá hay không được mã hoá. Nếu xác định rằng tệp tài liệu điện tử được mã hoá, thì tệp tài liệu điện tử này có thể được giải mã và lưu trữ vào bộ nhớ tạm thời. Tệp tài liệu điện tử không được mã hoá hoặc tệp tài liệu điện tử đã được giải mã sẽ được cung cấp cho bộ phận tìm kiếm 230 trong bộ phận bảo đảm an toàn tài liệu, để thực hiện việc tìm xem tệp tài liệu đó có chứa thông tin kinh doanh hay không. Các dấu hiệu cụ thể của bộ phận tìm kiếm 230 được thể hiện trên Fig.7. Bộ phận xác định cấp độ an toàn 240 xác định cấp độ an toàn của tài liệu và cấp bậc của người dùng liên quan đến khả năng truy nhập dựa vào văn bản tài liệu tìm được bằng bộ phận tìm kiếm 230 và tệp quy tắc thu được từ máy chủ. Các dấu hiệu cụ thể của bộ phận xác định cấp độ an toàn 240 được thể hiện trên Fig.8. Tài liệu có cấp độ an toàn đã được xác định sẽ được bổ sung thông tin cá nhân của người dùng từ máy chủ ở bộ phận chèn dấu mờ 250, và các dấu mờ dạng văn bản để phân định sự phân quyền khác nhau đối với tài liệu được hiển thị trên màn hình cho từng người dùng xem được chèn vào tài liệu dựa trên thông tin cá nhân của người dùng. Sau đó, quy trình xử lý an toàn như xoá, cách ly, v.v., được thực

hiện đối với tệp tài liệu điện tử có dấu mờ bằng bộ phận thực hiện quy trình xử lý an toàn 260, và tệp tài liệu cuối cùng đã chèn thông tin về khả năng truy nhập đối với tệp tài liệu được tạo ra bằng bộ phận tạo ra tệp tài liệu 270.

Fig.3 là hình vẽ thể hiện chi tiết bộ phận theo dõi 202 trong thiết bị khách hàng 200 trên Fig.2. Bộ phận theo dõi 202 có thể có bộ phận lọc quy trình xử lý 310, bộ phận lọc tệp 320, và bộ phận ánh xạ danh sách tệp 330. Bộ phận lọc quy trình xử lý 310 thực hiện chức năng thông báo thông tin về quy trình xử lý trong trường hợp tệp tài liệu điện tử được tạo ra hoặc có thay đổi trong quy trình xử lý tệp tài liệu của thiết bị khách hàng thông qua sự quan sát theo thời gian thực đối với quy trình xử lý tệp điện tử. Bộ phận lọc tệp 320 thực hiện chức năng quan sát theo thời gian thực đối với tệp tài liệu dựa vào tên tệp và phần mở rộng, v.v., và trong trường hợp phát hiện thấy có sự thay đổi của tệp tài liệu, thì bộ phận lọc tệp thực hiện chức năng thông báo về sự thay đổi đó. Bộ phận ánh xạ danh sách tệp 330 quản lý danh sách tệp đã được kiểm tra một lần để loại bỏ ra khỏi lần kiểm tra tiếp theo, do đó nâng cao hiệu quả của việc kiểm tra.

Fig.4 là hình vẽ thể hiện chi tiết bộ phận điều khiển 201 trong thiết bị khách hàng 200 trên Fig.2. Bộ phận điều khiển 201 có thể có bộ phận thiết lập trạng thái ban đầu 410, bộ phận giao diện 420, bộ phận thu nhận tệp quy tắc 430 và bộ phận ra lệnh kiểm tra 440. Bộ phận thiết lập trạng thái ban đầu 410 thực hiện chức năng thiết lập trạng thái ban đầu để đưa bộ phận bảo đảm an toàn tài liệu 204 trong bộ phận quản lý tài liệu trên thiết bị khách hàng 203 trở về trạng thái ban đầu của nó. Bộ phận bảo đảm an toàn tài liệu cần phải được đưa về trạng thái ban đầu bằng bộ phận thiết lập trạng thái ban đầu vì trạng thái thiết lập của nó có thể thay đổi liên tục do sự cập nhật định kỳ hoặc sự thay đổi thông số thiết lập của người dùng, v.v.. Bộ phận giao diện 420 thu nhận thông tin được cung cấp từ bộ phận thiết lập trạng thái ban đầu. Bộ phận thu nhận tệp quy tắc 430 thu nhận tệp quy tắc từ máy chủ, và có thể thực hiện các chức năng như mở, đóng tệp quy tắc thu được, đọc, ghi, xoá, v.v., các mục cụ thể trong tệp quy tắc. Bộ phận ra lệnh kiểm tra 440 có vai trò giống như bộ phận bảo đảm an toàn tài liệu thực hiện việc kiểm tra đối với tệp tài liệu được tải xuống thiết bị khách hàng.

Fig.5 là hình vẽ thể hiện tệp quy tắc được quản lý ở máy chủ, và được thu nhận từ máy chủ để nạp vào thiết bị khách hàng theo phương án thực hiện sáng chế. Tệp quy tắc

500 chứa các biểu thức chính quy 510, các từ khoá 520, quy tắc an toàn 530 và thông tin thiết lập cấp độ an toàn 540. Theo phương án thực hiện sáng chế, tệp quy tắc 500 có thể được cập nhật định kỳ bằng máy chủ.

Các biểu thức chính quy 510 biểu diễn tất cả thông tin có thể hiểu được bằng cách nhận biết hoặc suy ra thông tin kinh doanh trong các biểu thức chính quy. Các biểu thức chính quy được hỗ trợ để tìm kiếm và thay thế các hàng chữ trong nhiều chương trình soạn thảo văn bản và ngôn ngữ lập trình. Các từ khoá 520 cung cấp các từ liên quan đến thông tin kinh doanh. Ví dụ, các từ khoá có thể là các từ như bí mật, bảo vệ, công bố hạn chế, bí mật cấp độ thứ nhất, bí mật cấp độ thứ hai, bí mật nước ngoài, v.v..

Quy tắc an toàn 530 là bản tóm tắt nội bộ từ trước về biện pháp bảo đảm an toàn sẽ được áp dụng tuỳ thuộc vào cấp độ an toàn của tài liệu. Thông tin thiết lập cấp độ an toàn 540 có thể chứa quy tắc về cấp độ an toàn của tệp tài liệu 541 và quy tắc về khả năng truy nhập của người dùng 542. Thông tin thiết lập cấp độ an toàn 540 có thể chứa thông tin về hệ số quan trọng của mỗi từ liên quan đến thông tin kinh doanh để thiết lập cấp độ an toàn của các tài liệu kinh doanh, và thông tin liên quan đến việc thiết lập cấp độ an toàn của thông tin kinh doanh như thông tin về chu kỳ đọc, v.v., đối với từng cấp độ an toàn của tài liệu.

Fig.6 là hình vẽ thể hiện ví dụ về tệp quy tắc có thể được sử dụng trong sáng chế. Fig.6(a) thể hiện thông tin về hệ số quan trọng của mỗi từ liên quan đến thông tin kinh doanh. Ví dụ, từ "năm vào công ty" có hệ số quan trọng bằng 1 điểm, và từ "số nhận dạng của ban lãnh đạo và nhân viên" có hệ số quan trọng bằng 5 điểm.

Fig.6(b) là hình vẽ thể hiện cấp bậc của người dùng liên quan đến khả năng truy nhập đối với tài liệu kinh doanh theo vị trí ở trong công ty. Ví dụ, người dùng sử dụng thiết bị khách hàng ở vị trí là nhân viên bình thường có cấp bậc của người dùng bằng '5', phó bộ phận có cấp bậc của người dùng bằng '4', trưởng bộ phận có cấp bậc của người dùng bằng '3', trưởng nhóm hoặc phó phòng có cấp bậc của người dùng bằng '2', và ban lãnh đạo có cấp bậc của người dùng bằng '1'. Thông thường, cấp bậc của người dùng càng cao, thì khả năng truy nhập đối với tài liệu càng lớn.

Fig.7 là hình vẽ thể hiện chi tiết bộ phận tìm kiếm 230, bộ phận tìm kiếm này có thể nằm ở trong bộ phận bảo đảm an toàn tài liệu của thiết bị khách hàng theo phương án

thực hiện sáng chế. Bộ phận tìm kiếm 230 có thể có bộ phận giao diện 710, bộ phận lọc 730 và bộ phận phát hiện 750. Bộ phận giao diện 710 thu nhận lệnh kiểm tra tài liệu từ bộ phận ra lệnh kiểm tra 440 trong bộ phận điều khiển 201, và thu nhận tệp tài liệu điện tử không mã hoá hoặc tệp tài liệu điện tử đã được giải mã cần phải kiểm tra từ bộ phận kiểm tra tệp mã hoá/không mã hoá 220 trong bộ phận bảo đảm an toàn tài liệu 204.

Bộ phận lọc 730 có cấu tạo gồm nhiều bộ lọc thực hiện chức năng tìm kiếm chỉ duy nhất văn bản liên quan đến một tài liệu điện tử cụ thể để tìm kiếm thông tin văn bản ở trong các tài liệu điện tử. Bộ phận lọc 730 thực hiện chức năng phát hiện định dạng tài liệu, kiểm tra lỗi trong tài liệu, tìm kiếm thông tin trong tài liệu, tìm kiếm văn bản. Cụ thể hơn, bộ phận lọc 730 có thể có bộ lọc văn bản trong tệp 732, bộ lọc văn bản trong bộ nhớ 734, bộ lọc định dạng tệp 736, bộ lọc tệp nén 738, và bộ lọc một trang cụ thể 740.

Bộ lọc văn bản trong tệp 732 thực hiện chức năng đưa ra thông tin mật của một tệp cụ thể và tìm kiếm văn bản trong tệp tương ứng. Bộ lọc văn bản trong bộ nhớ 734 thực hiện chức năng đưa ra thông tin địa chỉ của một bộ nhớ cụ thể lưu trữ dữ liệu và tìm kiếm văn bản trong bộ nhớ tương ứng. Bộ lọc định dạng tệp 736 thực hiện chức năng kiểm tra xem phần mở rộng của tệp tương ứng sẽ được tìm kiếm có bị giả mạo hay không. Bộ lọc tệp nén 738 có thể tìm kiếm chỉ duy nhất thông tin tệp (tên tệp, thông tin định dạng, v.v.) trong tệp nén tương ứng hoặc cho phép chỉ duy nhất một tệp cụ thể được lọc trong trường hợp tệp được kiểm tra là tệp nén. Bộ lọc một trang cụ thể 740 thực hiện chức năng lọc thông tin văn bản chỉ trong một trang cụ thể trong số toàn bộ các tệp.

Thông tin văn bản tìm được bằng bộ phận lọc 730 được cung cấp cho bộ phận phát hiện 750. Sau khi so sánh thông tin văn bản tìm được với các biểu thức chính quy và các từ khoá để tìm thông tin kinh doanh ở trong tệp quy tắc thu được từ máy chủ, bộ phận phát hiện 750 phát hiện ra tệp tài liệu tương ứng có chứa các từ liên quan đến thông tin kinh doanh hay không. Bộ phận phát hiện 750 có thể nạp tệp quy tắc chứa các biểu thức chính quy và các từ khoá từ bộ phận thu nhận tệp quy tắc 430 trong bộ phận điều khiển 201 và lưu trữ tệp quy tắc đã nạp vào bộ nhớ riêng biệt.

Fig.8 là hình vẽ thể hiện chi tiết bộ phận xác định cấp độ an toàn 240, bộ phận xác định cấp độ an toàn này có thể nằm ở trong bộ phận bảo đảm an toàn tài liệu của thiết bị khách hàng theo phương án thực hiện sáng chế. Bộ phận xác định cấp độ an toàn 240 có

thể có bộ phận giao diện 810, bộ phận đếm 820, bộ phận tính điểm số 830 và bộ phận phân định cấp độ an toàn 840.

Bộ phận giao diện 810 thu nhận kết quả phát hiện thông tin văn bản từ bộ phận phát hiện 750 trong bộ phận tìm kiếm 230 cùng với lệnh để thiết lập trạng thái ban đầu khi xác định cấp độ an toàn. Bộ phận đếm 820 thực hiện chức năng đếm số lần tìm thấy của các từ liên quan đến thông tin kinh doanh bằng bộ phận phát hiện. Ngoài ra, bộ phận tính điểm số 830 tính điểm số tiếp cận của thông tin kinh doanh bằng cách sử dụng biểu thức "tổng của (số lần tìm thấy của từ × hệ số quan trọng của mỗi từ liên quan đến thông tin kinh doanh) = điểm số tiếp cận". Ví dụ, giả sử rằng từ "số nhận dạng" được tìm thấy hai lần trong văn bản, và từ "năm vào công ty" được tìm thấy một lần, dựa vào hệ số quan trọng của mỗi từ được thể hiện trên Fig.6(a), có thể thấy rằng "số nhận dạng" có hệ số quan trọng bằng 5, và "năm vào công ty" có hệ số quan trọng bằng 1. Vì vậy, trong trường hợp này, dựa vào biểu thức nêu trên, điểm số tiếp cận của tài liệu tương ứng được tính dưới dạng 5×2 (hệ số quan trọng của từ "số nhận dạng" × số lần tìm thấy) + 1×1 (hệ số quan trọng của từ "năm vào công ty" × số lần tìm thấy) = 11, tức là, 11 điểm.

Bộ phận phân định cấp độ an toàn 840 thực hiện chức năng phân định cấp độ an toàn của tài liệu để kiểm soát khả năng truy nhập vào mỗi tài liệu đối với từng người dùng theo thông tin thiết lập cấp độ an toàn có trong tệp quy tắc dựa vào điểm số tiếp cận được tính bằng bộ phận tính điểm số. Trong trường hợp này, Fig.6(c) là hình vẽ thể hiện quy tắc thiết lập cấp độ an toàn của tài liệu để phân định các cấp độ an toàn dựa vào điểm số tiếp cận theo một phương án thực hiện sáng chế. Theo phương án này, ví dụ, nếu điểm số tiếp cận tính được bằng 0~5 điểm, thì tài liệu được phân định cấp độ an toàn bằng 5. Nếu điểm số tiếp cận bằng 6~9 điểm, thì tài liệu được phân định cấp độ an toàn bằng 4. Nếu điểm số tiếp cận bằng 10~14 điểm, thì tài liệu được phân định cấp độ an toàn bằng 3. Nếu điểm số tiếp cận bằng 15~19 điểm, thì tài liệu được phân định cấp độ an toàn bằng 2. Nếu điểm số tiếp cận bằng 20 điểm hoặc cao hơn, thì tài liệu được phân định cấp độ an toàn bằng 1. Như đã nêu trên, tệp quy tắc thu được từ máy chủ chứa quy tắc về khả năng truy nhập của người dùng. Dựa vào quy tắc về khả năng truy nhập của người dùng đối với mỗi cấp độ an toàn của tài liệu được thể hiện cụ thể trên Fig.6(c), ví dụ, nếu tài liệu được phân định cấp độ an toàn 1 và người dùng sử dụng thiết bị khách hàng có cấp bậc

của người dùng là cấp bậc 1 hoặc cao hơn, thì người dùng có thể đọc, lưu trữ, in và soạn thảo tài liệu. Theo phương án này, đối với các tài liệu có cấp độ an toàn của tài liệu là cấp độ an toàn 1, người dùng có cấp bậc của người dùng không phải là cấp bậc 1 thì không thể đọc, lưu trữ, in hoặc soạn thảo tài liệu. Ngoài ra, theo phương án này, đối với các tài liệu có cấp độ an toàn của tài liệu là cấp độ an toàn 2, người dùng có cấp bậc của người dùng là cấp bậc 2 hoặc cao hơn thì có thể đọc, lưu trữ, in, soạn thảo tài liệu. Nếu cấp bậc của người dùng là cấp bậc 3, thì người dùng có thể đọc và in tài liệu, nhưng không thể lưu trữ và soạn thảo tài liệu. Nếu cấp bậc của người dùng là cấp bậc 4, thì người dùng chỉ có thể đọc tài liệu. Nếu cấp bậc của người dùng là cấp bậc 5, thì người dùng không thể đọc, lưu trữ, in hay soạn thảo tài liệu. Khả năng truy nhập của người dùng đối với từng cấp bậc có thể thay đổi ở thời điểm bất kỳ theo quy tắc bảo đảm an toàn thông tin kinh doanh và có thể được cập nhật ở máy chủ.

Fig.9 là hình vẽ thể hiện ví dụ về phương pháp chèn dấu mờ vào tài liệu văn bản ở bộ phận chèn dấu mờ, bộ phận chèn dấu mờ này có thể nằm ở trong bộ phận bảo đảm an toàn tài liệu của thiết bị khách hàng theo phương án thực hiện sáng chế. Fig.9(a) và Fig.9(b) thể hiện phương pháp chèn dấu mờ bằng cách giảm cỡ phông chữ của một văn bản cụ thể. Fig.9(a) là hình vẽ thể hiện văn bản được chèn dấu mờ. Giả sử rằng tài liệu có cỡ phông chữ cơ bản là 12 pt, và người dùng sử dụng tài liệu có khoá người dùng là "10011". Theo phương án này, mỗi dòng văn bản trong vùng văn bản được thể hiện trên Fig.9(a) có thể tương ứng với mỗi giá trị bit của khoá người dùng, theo thứ tự lần lượt. Do đó, dòng thứ nhất trong vùng văn bản tương ứng với bit thứ nhất của khoá người dùng, "1". Dòng thứ hai trong vùng văn bản tương ứng với bit thứ hai của khoá người dùng, "0". Dòng thứ ba trong vùng văn bản tương ứng với bit thứ ba của khoá người dùng, "0". Dòng thứ tư trong vùng văn bản tương ứng với bit thứ tư của khoá người dùng, "1". Dòng thứ năm trong vùng văn bản tương ứng với bit thứ năm của khoá người dùng, "1". Nếu đúng như vậy, thì bộ phận chèn dấu mờ 250 có thể giảm hoặc tăng cỡ phông chữ của văn bản ở trong mỗi dòng văn bản theo cỡ phông chữ đã thiết lập. Ví dụ, các văn bản được phân định bit "1" có thể giảm 1 pt. Cụ thể là, như được thể hiện trên Fig.9(b), văn bản ở hàng thứ nhất, hàng thứ tư và hàng thứ năm trong vùng văn bản tương ứng với bit "1" có thể được điều chỉnh thành cỡ phông chữ là 11 pt, trong đó 1 pt là mức giảm khi so sánh với cỡ phông chữ cơ bản. Cùng lúc này, cỡ phông chữ ở hàng thứ hai và hàng thứ

ba trong vùng văn bản tương ứng với bit "0" được giữ nguyên là 12 pt. Nếu số lượng bit trong khoá người dùng luôn cố định là 5 bit, thì giá trị khoá người dùng được áp dụng lặp lại từ dòng thứ nhất của văn bản với mỗi nhóm gồm năm dòng. Vì vậy, khoảng giữa dòng văn bản sẽ được điều chỉnh là 5 dòng, và trong trường hợp này, sẽ dễ dàng phát hiện ra dấu mờ trong tương lai. Tuy nhiên, cỡ chữ có thể được giảm hoặc tăng theo giá trị bit "1" hoặc "0" tương ứng, nhưng để phòng ngừa sự cố tràn hệ thống, phương pháp giảm cỡ phông chữ thường được ưu tiên sử dụng.

Tiếp theo, Fig.9(c) và Fig.9(d) thể hiện phương pháp chèn dấu mờ trong phương pháp thay đổi độ rộng phông chữ của một văn bản cụ thể. Do đó, Fig.9(c) là hình vẽ thể hiện văn bản được chèn dấu mờ. Theo phương án thực hiện sáng chế, các phụ âm hoặc các nguyên âm được sử dụng nhiều nhất được tìm trong văn bản, và các bit của khoá người dùng tương ứng với các văn bản lặp lại có chứa các phụ âm hoặc các nguyên âm đó, theo thứ tự lần lượt. Bằng cách thay đổi đường bao của văn bản, độ rộng phông chữ sẽ thay đổi để hẹp hơn hoặc rộng hơn. Đường bao phông chữ làm thay đổi độ rộng phông chữ theo khoá người dùng như đã nêu trên có thể được thực hiện đối với toàn bộ vùng văn bản. Ví dụ, như được thể hiện trên Fig.9(d), giả sử rằng khoá người dùng là "10011" và phụ âm được tìm thấy nhiều nhất là "ㄱ", 1, 0, 0, 1 và 1 có thể lần lượt tương ứng với các chữ "가", "각", "각", "과", và "과", các chữ này đều có phụ âm "ㄱ", và độ rộng phông chữ của văn bản tương ứng với bit "1" có thể sẽ thay đổi để hẹp hơn hoặc rộng hơn. Trong trường hợp màn hình hiển thị tài liệu bị rò rỉ do in màn hình hoặc chụp ảnh màn hình, v.v., cho bên thứ ba, thì tài liệu đã chèn dấu mờ bằng cách sử dụng phương pháp nêu trên có thể lại theo dõi giá trị của khoá người dùng chỉ dựa vào độ rộng phông chữ. Vì vậy, sẽ dễ dàng theo dõi đường rò rỉ, và do đó có thể tăng cường các biện pháp bảo đảm an toàn bổ sung.

Fig.10 là hình vẽ thể hiện các quy trình xử lý được thực hiện ở bộ phận thực hiện quy trình xử lý an toàn 260, bộ phận thực hiện quy trình xử lý an toàn này có thể nằm ở trong bộ phận bảo đảm an toàn tài liệu của thiết bị khách hàng theo phương án thực hiện sáng chế. Bộ phận thực hiện quy trình xử lý an toàn 260 có thể thực hiện quy trình xử lý an toàn theo quy tắc an toàn với mỗi cấp độ an toàn được thiết lập cho tệp quy tắc theo cấp độ an toàn của tài liệu được xác định bằng bộ phận xác định cấp độ an toàn 240, quy

trình xử lý an toàn này có một trong số các cách xoá hoàn toàn, cách ly, mã hoá và thông báo. Trong trường hợp xử lý bằng cách xoá hoàn toàn, tài liệu không thể khôi phục được, và trong trường hợp xử lý bằng cách cách ly, việc truy nhập không được phép không thể thực hiện được vì tài liệu dịch chuyển đến một vị trí cụ thể. Ví dụ, do kết quả của việc tải tài liệu từ máy chủ xuống thiết bị khách hàng và người dùng chỉnh sửa tài liệu, nên khi tìm kiếm tài liệu tương ứng, nếu các từ có hệ số quan trọng bằng 5 hoặc cao hơn được tiếp cận ít nhất 9 lần, thì quy trình xử lý bằng cách xoá hoàn toàn có thể được thực hiện, và nếu các từ có hệ số quan trọng bằng 5 hoặc cao hơn được tiếp cận ít nhất 6 lần, thì quy trình xử lý bằng cách cách ly có thể được thực hiện. Ngoài ra, khi các từ có hệ số quan trọng bằng 5 hoặc cao hơn được tiếp cận không phải ít nhất 6 lần, nếu điểm số tiếp cận được tính là cao hơn hoặc bằng 3 điểm và thấp hơn hoặc bằng 30 điểm, thì tài liệu tương ứng được mã hoá và tải lên máy chủ, và sau đó có thể được quản lý và lưu trữ trên máy chủ. Nếu điểm số tiếp cận là thấp hơn hoặc bằng 2 điểm, thì các thay đổi của tài liệu tương ứng được ghi dưới dạng thông tin nhật ký, và có thể được thông báo.

Fig.11 là hình vẽ thể hiện cấu trúc của tệp được tạo ra ở bộ phận tạo ra tệp tài liệu 270, bộ phận tạo ra tệp tài liệu này có thể nằm ở trong bộ phận bảo đảm an toàn tài liệu của thiết bị khách hàng theo phương án thực hiện sáng chế. Bộ phận tạo ra tệp tài liệu 270 có thể chèn thông tin bảo đảm an toàn vào phần đầu 1110 của tệp trong phần thân 1100 của tài liệu đã mã hoá, tức là, tạo ra tệp mã hoá 1120 đã chèn thông tin liên quan đến khả năng truy nhập của người dùng.

Fig.12 là hình vẽ thể hiện bộ phận lưu trữ tài liệu 205 trong thiết bị khách hàng theo phương án thực hiện sáng chế. Bộ phận lưu trữ tài liệu 205 có thể có bộ phận tải lên/tải xuống 1220 để tải tài liệu lên máy chủ và tải tài liệu xuống thiết bị khách hàng, và bộ phận sao lưu tài liệu 1240 để sao lưu tài liệu khi tạo ra tài liệu.

Fig.13a là lưu đồ thể hiện phương pháp tạo ra tệp tài liệu điện tử trên thiết bị khách hàng để nâng cao độ an toàn của thông tin kinh doanh theo phương án thực hiện sáng chế. Thiết bị khách hàng bắt đầu thực hiện phương pháp này khi tệp tài liệu điện tử được tải xuống hoặc tạo ra (bước S1300). Bộ phận theo dõi trong thiết bị khách hàng theo dõi việc tạo ra tệp tài liệu điện tử trên thiết bị khách hàng và/hoặc các thay đổi của tệp tài liệu điện tử được tải xuống từ máy chủ (bước S1302). Thiết bị khách hàng có thể thu nhận tệp quy

tắc từ máy chủ (bước S1304). Như được thể hiện trên Fig.5, tệp quy tắc có thể chứa các biểu thức chính quy, các từ khoá, quy tắc an toàn và thông tin thiết lập cấp độ an toàn của tài liệu. Thông tin thiết lập cấp độ an toàn của tài liệu có thể chứa hệ số quan trọng của các từ liên quan đến thông tin kinh doanh, quy tắc về cấp độ an toàn của tài liệu và quy tắc về khả năng truy nhập của người dùng xác định khả năng truy nhập của người dùng đối với tài liệu theo cấp độ an toàn của tài liệu dựa vào điểm số tiếp cận. Bước thu nhận tệp quy tắc từ máy chủ không chỉ có thể được thực hiện khi tạo ra và/hoặc thay đổi tệp tài liệu điện tử được theo dõi ở thiết bị khách hàng, mà còn có thể được thực hiện định kỳ không liên quan đến việc tạo ra và/hoặc thay đổi tệp tài liệu điện tử.

Thiết bị khách hàng có thể tìm kiếm dữ liệu văn bản từ tệp tài liệu điện tử được theo dõi bằng bộ phận lọc trong bộ phận tìm kiếm (bước S1306), và có thể tìm kiếm các từ liên quan đến thông tin kinh doanh từ dữ liệu văn bản tìm được bằng bộ phận phát hiện trong bộ phận tìm kiếm (bước S1308). Bộ phận đếm trong bộ phận xác định cấp độ an toàn của thiết bị khách hàng có thể đếm số lần tìm thấy các từ liên quan đến thông tin kinh doanh, và bộ phận tính điểm số tính điểm số tiếp cận của tệp tài liệu điện tử bằng cách tính tổng của tích số giữa số lần tìm thấy của các từ liên quan đến thông tin kinh doanh và hệ số quan trọng của các từ liên quan đến thông tin kinh doanh dựa vào hệ số quan trọng của các từ liên quan đến thông tin kinh doanh trong số các thông tin thiết lập cấp độ an toàn của tài liệu có trong tệp quy tắc (bước S1310).

Bộ phận phân định cấp độ an toàn trong thiết bị khách hàng phân định cấp độ an toàn của tài liệu liên quan đến khả năng truy nhập của người dùng cho tệp tài liệu điện tử dựa vào quy tắc về khả năng truy nhập của người dùng có trong tệp quy tắc theo điểm số tiếp cận tính được ở trên (bước S1312). Bộ phận chèn dấu mờ trong thiết bị khách hàng thu nhận thông tin cá nhân của người dùng liên quan đến người dùng sử dụng thiết bị khách hàng từ máy chủ, và chèn dấu mờ vào văn bản của tệp tài liệu điện tử được hiển thị trên thiết bị khách hàng dựa vào thông tin cá nhân của người dùng thu được (bước S1314). Bước chèn dấu mờ có thể bao gồm ít nhất một trong số các bước thay đổi cỡ phông chữ của văn bản và thay đổi độ rộng phông chữ của văn bản theo thông tin cá nhân của người dùng.

Sau đó, đối với tệp tài liệu điện tử có cấp độ an toàn được xác định và dấu mờ được

chèn, bộ phận thực hiện quy trình xử lý an toàn trong thiết bị khách hàng có thể thực hiện quy trình xử lý an toàn theo quy tắc an toàn đối với từng cấp độ an toàn, quy trình xử lý an toàn này có một trong số các cách xoá, cách ly, mã hoá và thông báo về tài liệu tương ứng, và bộ phận tạo ra tệp tài liệu có thể tạo ra tệp tài liệu có phần đầu đã chèn thông tin bảo đảm an toàn (bước S1316).

Fig.13b là lưu đồ thể hiện phương pháp tải tệp tài liệu điện tử từ máy chủ xuống thiết bị khách hàng để nâng cao độ an toàn của thông tin kinh doanh. Trước hết, trong trường hợp có yêu cầu đăng nhập từ thiết bị khách hàng, máy chủ xác minh thông tin đăng nhập của người dùng trên thiết bị khách hàng (bước S1320). Máy chủ còn xem xét sơ đồ tổ chức và thông tin cá nhân của người dùng từ cơ sở dữ liệu nhân sự (bước S1322), và xem xét tệp quy tắc chứa thông tin thiết lập cấp độ an toàn của tài liệu và quy tắc an toàn từ cơ sở dữ liệu quy tắc trên máy chủ (bước S1324). Bộ phận quản lý an toàn trong máy chủ phân định cấp độ an toàn của tài liệu liên quan đến khả năng truy nhập của người dùng cho tệp tài liệu điện tử dựa vào thông tin thiết lập cấp độ an toàn của tài liệu, và dấu mờ có thể được chèn vào tệp tài liệu điện tử dựa vào thông tin cá nhân của người dùng (bước S1326). Bộ phận quản lý an toàn trong máy chủ mã hoá tệp tài liệu điện tử sau khi phân định cấp độ an toàn của tài liệu và chèn dấu mờ (bước S1328). Sau đó, tệp tài liệu điện tử đã mã hoá có thể được truyền từ máy chủ đến thiết bị khách hàng và được tải xuống bằng thiết bị khách hàng theo yêu cầu tải xuống từ thiết bị khách hàng (bước S1330). Thiết bị khách hàng đã tải tệp tài liệu điện tử từ máy chủ xác định xem nó có thể lưu trữ các thay đổi của tệp tài liệu điện tử theo khả năng truy nhập của người dùng hoặc nó có thể tạo ra tệp tài liệu điện tử mới, v.v. hay không (bước S1332). Nếu xác định rằng không thể thay đổi tệp tài liệu điện tử, thì bản ghi nhật ký của người dùng được truyền đến máy chủ, và nếu xác định rằng có thể thay đổi tệp tài liệu điện tử, thì phương pháp này chuyển đến bước S1300, và tệp tài liệu điện tử có thể được tạo ra trên thiết bị khách hàng để nâng cao độ an toàn của thông tin kinh doanh.

Nhờ phương pháp, thiết bị và hệ thống tạo ra tệp tài liệu điện tử trên thiết bị khách hàng để nâng cao độ an toàn của thông tin kinh doanh theo sáng chế, có thể kiểm soát khả năng truy nhập tài liệu đối với từng người dùng và tạo ra các biện pháp bảo đảm an toàn sơ bộ mạnh hơn để ngăn chặn sự rò rỉ thông tin kinh doanh trước khi áp dụng biện

pháp bảo đảm an toàn phù hợp cho mỗi tài liệu, bằng cách tìm xem tài liệu điện tử có trong công ty có chứa thông tin bí mật của công ty hay không sử dụng kỹ thuật tìm kiếm tài liệu điện tử, tính điểm số tiếp cận dựa vào mức độ tiếp cận và xác định cấp độ an toàn của tài liệu tương ứng, và kiểm soát khả năng truy nhập của người dùng theo từng cấp độ an toàn của tài liệu, tức là, khắc phục được các vấn đề còn tồn tại của phương pháp DRM và phương pháp DLP.

Ngoài ra, có thể theo dõi đường rò rỉ thông tin khi tài liệu bị rò rỉ ra ngoài do thao tác chụp ảnh, v.v., cho bên thứ ba, bằng cách chèn dấu mờ vào tài liệu dựa vào một giá trị cụ thể có thể phân biệt từng người dùng và tạo ra sự phân quyền đối với tài liệu được hiển thị trên màn hình cho từng người dùng xem, và do đó tạo ra các biện pháp bảo đảm an toàn bổ sung cho công ty để triển khai nhiều loại thiết bị cỡ nhỏ.

Ngoài ra, sáng chế có ưu điểm là nâng cao độ an toàn của thông tin kinh doanh một cách hiệu quả hơn theo xu hướng mở rộng phạm vi sử dụng các thiết bị cỡ nhỏ và các thiết bị di động trong môi trường kinh doanh, v.v., bằng cách cho phép tệp tài liệu điện tử được tạo ra trên thiết bị khách hàng, chứ không phải trên máy chủ, để nâng cao độ an toàn của thông tin kinh doanh.

Sáng chế được mô tả dựa vào các phương án ưu tiên nêu trên để làm ví dụ thực hiện sáng chế. Tuy nhiên, người có hiểu biết trung bình về lĩnh vực kỹ thuật này có thể tìm ra nhiều phương án cải biến và thay đổi khác nhau để thực hiện sáng chế mà vẫn không bị coi là nằm ngoài phạm vi của sáng chế, như được xác định bằng các điểm yêu cầu bảo hộ dưới đây.

YÊU CẦU BẢO HỘ

1. Phương pháp tạo ra tệp tài liệu điện tử trên thiết bị khách hàng để nâng cao độ an toàn của thông tin kinh doanh bao gồm các bước:

theo dõi việc tạo ra tệp tài liệu điện tử trên thiết bị khách hàng và các thay đổi của tệp tài liệu điện tử đó;

thu nhận tệp quy tắc từ máy chủ, tệp quy tắc này chứa các biểu thức chính quy, các từ khoá, quy tắc an toàn và thông tin thiết lập cấp độ an toàn của tài liệu, thông tin thiết lập cấp độ an toàn của tài liệu này chứa hệ số quan trọng của các từ liên quan đến thông tin kinh doanh, quy tắc về cấp độ an toàn của tài liệu và quy tắc về khả năng truy nhập của người dùng xác định khả năng truy nhập của người dùng đối với tài liệu theo cấp độ an toàn của tài liệu;

tìm kiếm dữ liệu văn bản từ tệp tài liệu điện tử;

tìm kiếm các từ liên quan đến thông tin kinh doanh từ dữ liệu văn bản tìm được;

tính điểm số tiếp cận, điểm số tiếp cận này biểu thị tổng của tích số giữa số lần tìm thấy của các từ liên quan đến thông tin kinh doanh và hệ số quan trọng của các từ liên quan đến thông tin kinh doanh;

phân định cấp độ an toàn của tài liệu cho tệp tài liệu điện tử dựa vào điểm số tiếp cận;

thu nhận thông tin cá nhân của người dùng sử dụng thiết bị khách hàng từ máy chủ và chèn dấu mờ vào văn bản của tệp tài liệu điện tử được hiển thị trên thiết bị khách hàng dựa vào thông tin cá nhân của người dùng thu được;

dựa vào cấp độ an toàn của tài liệu đã được phân định cho tệp tài liệu điện tử, thực hiện quy trình xử lý an toàn theo quy tắc an toàn, quy trình xử lý an toàn này có một trong số các cách xoá, cách ly, mã hoá và thông báo; và

tạo ra tệp tài liệu điện tử được bảo vệ bằng cách chèn thông tin về khả năng truy nhập vào phần đầu của tệp tài liệu điện tử.

2. Phương pháp theo điểm 1, trong đó bước chèn dấu mờ bao gồm bước thay đổi ít nhất

một thông số trong số cỡ phông chữ và độ rộng phông chữ của văn bản theo thông tin cá nhân của người dùng.

3. Phương pháp theo điểm 1, trong đó phương pháp này còn bao gồm bước tải tệp tài liệu điện tử từ máy chủ xuống thiết bị khách hàng trước khi theo dõi, và trong đó bước tải tệp tài liệu điện tử xuống thiết bị khách hàng bao gồm các bước:

ở máy chủ, xác minh thông tin đăng nhập của người dùng trên thiết bị khách hàng;

xem xét sơ đồ tổ chức và thông tin cá nhân của người dùng từ cơ sở dữ liệu nhân sự trên máy chủ;

xem xét tệp quy tắc chứa quy tắc an toàn và thông tin thiết lập cấp độ an toàn của tài liệu từ cơ sở dữ liệu quy tắc trên máy chủ;

phân định cấp độ an toàn của tài liệu kết hợp với khả năng truy nhập của người dùng cho tệp tài liệu điện tử dựa vào thông tin thiết lập cấp độ an toàn của tài liệu và chèn dấu mờ vào tệp tài liệu điện tử dựa vào thông tin cá nhân của người dùng;

mã hóa tệp tài liệu điện tử sau khi phân định cấp độ an toàn của tài liệu và chèn dấu mờ; và

truyền tệp tài liệu điện tử đã mã hóa từ máy chủ đến thiết bị khách hàng.

4. Hệ thống tạo ra tệp tài liệu điện tử để nâng cao độ an toàn của thông tin kinh doanh bao gồm:

máy chủ có bộ phận xác định quy tắc trên máy chủ được kết nối với cơ sở dữ liệu quy tắc và bộ phận quản lý an toàn được kết nối với cơ sở dữ liệu nhân sự; và

thiết bị khách hàng được kết nối với máy chủ qua mạng,

thiết bị khách hàng này có:

bộ phận theo dõi được tạo cấu hình để theo dõi việc tạo ra tệp tài liệu điện tử và các thay đổi của tệp tài liệu điện tử đó;

bộ phận điều khiển được tạo cấu hình để thu nhận tệp quy tắc từ cơ sở dữ liệu quy tắc trên máy chủ, tệp quy tắc này chứa các biểu thức chính quy, các từ khóa, quy tắc an toàn và thông tin thiết lập cấp độ an toàn của tài liệu, thông tin thiết lập cấp độ an toàn của tài liệu này chứa hệ số quan trọng của các từ liên quan đến thông

tin kinh doanh, quy tắc về cấp độ an toàn của tài liệu và quy tắc về khả năng truy nhập của người dùng xác định khả năng truy nhập của người dùng đối với tài liệu theo cấp độ an toàn của tài liệu; và

bộ phận bảo đảm an toàn tài liệu, bộ phận bảo đảm an toàn tài liệu này có:

bộ phận tìm kiếm được tạo cấu hình để tìm kiếm dữ liệu văn bản từ tệp tài liệu điện tử và tìm kiếm các từ liên quan đến thông tin kinh doanh từ dữ liệu văn bản tìm được;

bộ phận xác định cấp độ an toàn được tạo cấu hình để tính điểm số tiếp cận và phân định cấp độ an toàn của tài liệu cho tệp tài liệu điện tử dựa vào điểm số tiếp cận, điểm số tiếp cận này biểu thị tổng của tích số giữa số lần tìm thấy của các từ liên quan đến thông tin kinh doanh và hệ số quan trọng của các từ liên quan đến thông tin kinh doanh;

bộ phận chèn dấu mờ được tạo cấu hình để chèn dấu mờ vào văn bản của tệp tài liệu điện tử được hiển thị trên thiết bị khách hàng dựa vào thông tin cá nhân của người dùng thu được từ máy chủ;

bộ phận thực hiện quy trình xử lý an toàn được tạo cấu hình để thực hiện quy trình xử lý an toàn trên tài liệu điện tử theo quy tắc an toàn dựa vào cấp độ an toàn của tài liệu đã được phân định, quy trình xử lý an toàn này có một trong số các cách xoá, cách ly, mã hoá và thông báo; và

bộ phận tạo ra tệp tài liệu được tạo cấu hình để tạo ra tệp tài liệu điện tử được bảo vệ bằng cách chèn thông tin về khả năng truy nhập vào phần đầu của tệp tài liệu điện tử.

5. Hệ thống theo điểm 4, trong đó bộ phận chèn dấu mờ còn được tạo cấu hình để thay đổi ít nhất một thông số trong số cỡ phông chữ và độ rộng phông chữ của văn bản theo thông tin cá nhân của người dùng.

6. Hệ thống theo điểm 4, trong đó máy chủ được tạo cấu hình để:

xác minh thông tin đăng nhập của người dùng trên thiết bị khách hàng;

xem xét sơ đồ tổ chức và thông tin cá nhân của người dùng từ cơ sở dữ liệu nhân

sự;

xem xét tệp quy tắc chứa quy tắc an toàn và thông tin thiết lập cấp độ an toàn của tài liệu từ cơ sở dữ liệu quy tắc;

phân định cấp độ an toàn của tài liệu kết hợp với khả năng truy nhập của người dùng cho tệp tài liệu điện tử dựa vào thông tin thiết lập cấp độ an toàn của tài liệu và chèn dấu mờ vào tệp tài liệu điện tử dựa vào thông tin cá nhân của người dùng;

mã hoá tệp tài liệu điện tử sau khi phân định cấp độ an toàn của tài liệu và chèn dấu mờ; và

trong đó thiết bị khách hàng còn có bộ phận lưu trữ tài liệu được tạo cấu hình để tải tệp tài liệu điện tử đã mã hoá từ máy chủ xuống thiết bị khách hàng.

7. Thiết bị khách hàng tạo ra tệp tài liệu điện tử để nâng cao độ an toàn của thông tin kinh doanh bao gồm:

phương tiện theo dõi việc tạo ra tệp tài liệu điện tử và các thay đổi của tệp tài liệu điện tử đó;

phương tiện thu nhận tệp quy tắc từ máy chủ, tệp quy tắc này chứa các biểu thức chính quy, các từ khoá, quy tắc an toàn và thông tin thiết lập cấp độ an toàn của tài liệu, thông tin thiết lập cấp độ an toàn của tài liệu này chứa hệ số quan trọng của các từ liên quan đến thông tin kinh doanh, quy tắc về cấp độ an toàn của tài liệu và quy tắc về khả năng truy nhập của người dùng xác định khả năng truy nhập của người dùng đối với tài liệu theo cấp độ an toàn của tài liệu;

phương tiện tìm kiếm dữ liệu văn bản từ tệp tài liệu điện tử;

phương tiện tìm kiếm các từ liên quan đến thông tin kinh doanh từ dữ liệu văn bản tìm được;

phương tiện tính điểm số tiếp cận, điểm số tiếp cận này biểu thị tổng của tích số giữa số lần tìm thấy của các từ liên quan đến thông tin kinh doanh và hệ số quan trọng của các từ liên quan đến thông tin kinh doanh;

phương tiện phân định cấp độ an toàn của tài liệu cho tệp tài liệu điện tử dựa vào điểm số tiếp cận;

phương tiện thu nhận thông tin cá nhân của người dùng sử dụng thiết bị khách hàng từ máy chủ và chèn dấu mờ vào văn bản của tệp tài liệu điện tử được hiển thị trên thiết bị khách hàng dựa vào thông tin cá nhân của người dùng thu được;

phương tiện thực hiện quy trình xử lý an toàn theo quy tắc an toàn dựa vào cấp độ an toàn của tài liệu đã được phân định, quy trình xử lý an toàn này có một trong số các cách xoá, cách ly, mã hoá và thông báo; và

phương tiện tạo ra tệp tài liệu điện tử được bảo vệ bằng cách chèn thông tin về khả năng truy nhập vào phần đầu của tệp tài liệu điện tử.

Fig.1

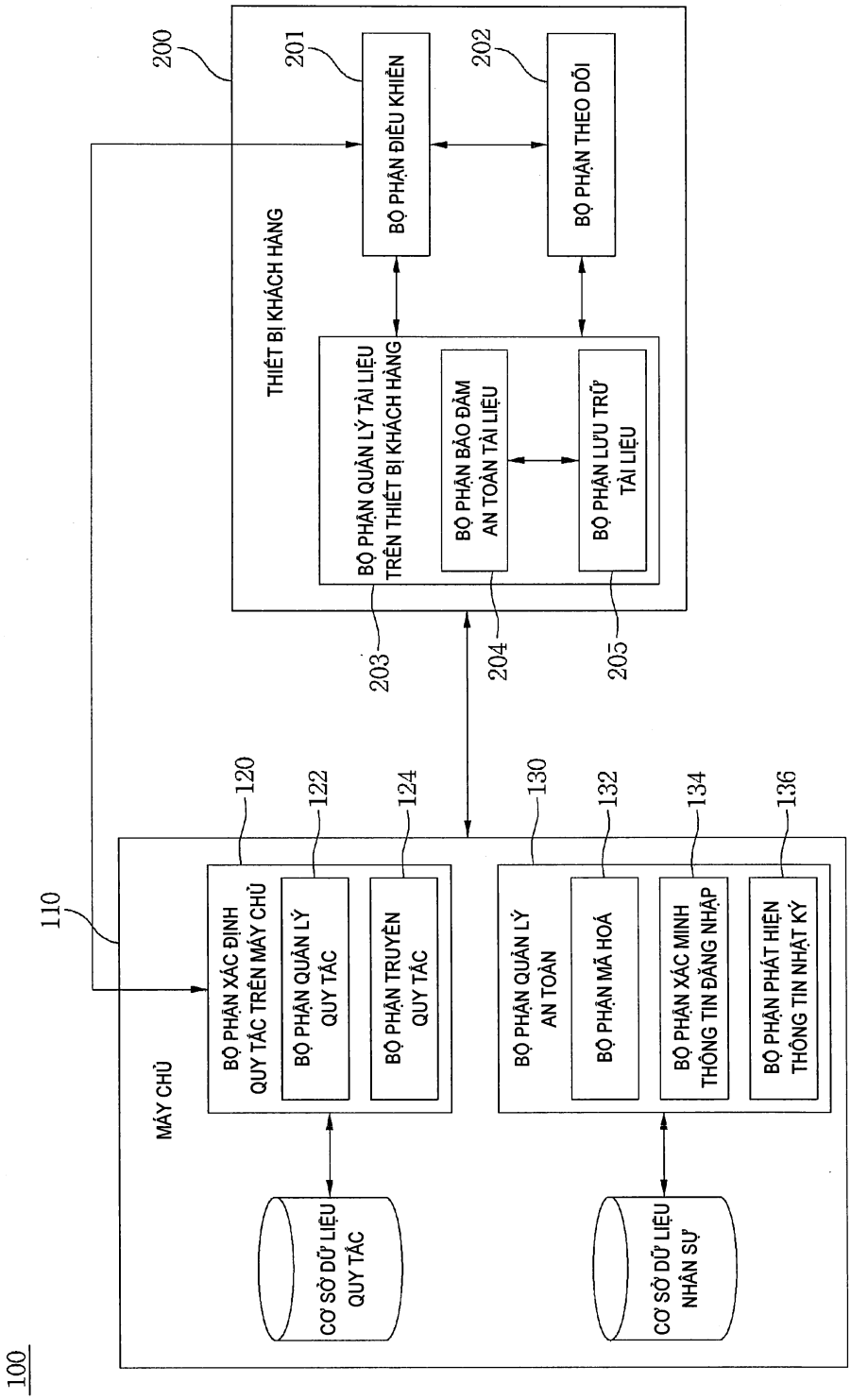

100
110
MÁY CHỦ
BỘ PHẬN XÁC ĐỊNH QUY TẮC TRÊN MÁY CHỦ
BỘ PHẬN QUẢN LÝ QUY TẮC
BỘ PHẬN TRUYỀN QUY TẮC
BỘ PHẬN QUẢN LÝ AN TOÀN
BỘ PHẬN MÃ HOÁ
BỘ PHẬN XÁC MINH THÔNG TIN ĐĂNG NHẬP
BỘ PHẬN PHÁT HIỆN THÔNG TIN NHẬT KÝ
CƠ SỞ DỮ LIỆU QUY TẮC
CƠ SỞ DỮ LIỆU NHÂN SỰ
120
122
124
130
132
134
136
THIẾT BỊ KHÁCH HÀNG
200
BỘ PHẬN ĐIỀU KHIỂN
201
BỘ PHẬN THEO DÕI
202
BỘ PHẬN QUẢN LÝ TÀI LIỆU TRÊN THIẾT BỊ KHÁCH HÀNG
BỘ PHẬN BẢO ĐẢM AN TOÀN TÀI LIỆU
BỘ PHẬN LƯU TRỮ TÀI LIỆU
203
204
205

Fig.2

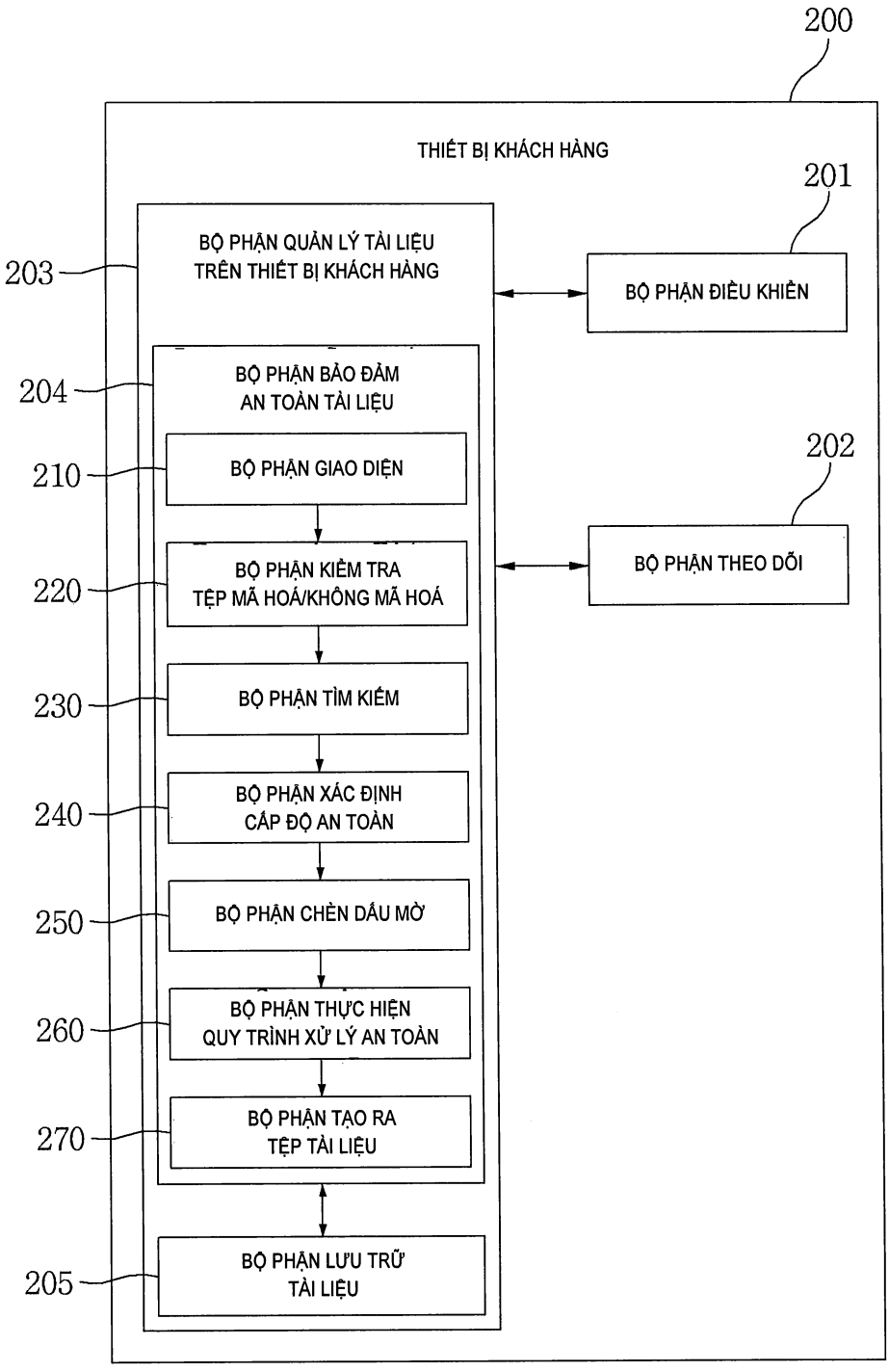

200
THIẾT BỊ KHÁCH HÀNG
201
BỘ PHẬN QUẢN LÝ TÀI LIỆU TRÊN THIẾT BỊ KHÁCH HÀNG
203
BỘ PHẬN ĐIỀU KHIỂN
BỘ PHẬN BẢO ĐẢM AN TOÀN TÀI LIỆU
204
202
210
BỘ PHẬN GIAO DIỆN
BỘ PHẬN KIỂM TRA TỆP MÃ HOÁ/KHÔNG MÃ HOÁ
220
BỘ PHẬN THEO DÕI
230
BỘ PHẬN TÌM KIẾM
240
BỘ PHẬN XÁC ĐỊNH CẤP ĐỘ AN TOÀN
250
BỘ PHẬN CHÈN DẤU MỜ
260
BỘ PHẬN THỰC HIỆN QUY TRÌNH XỬ LÝ AN TOÀN
270
BỘ PHẬN TẠO RA TỆP TÀI LIỆU
205
BỘ PHẬN LƯU TRỮ TÀI LIỆU

Fig.3

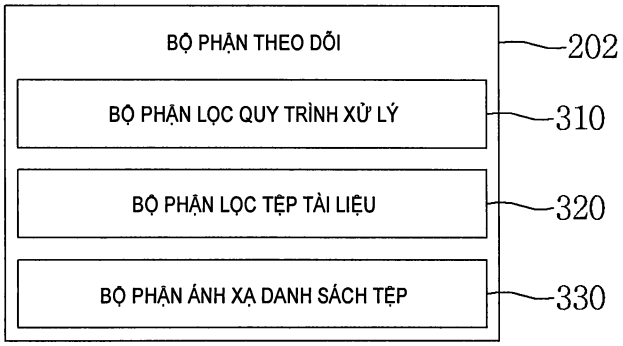

BỘ PHẬN THEO DÕI
202
BỘ PHẬN LỌC QUY TRÌNH XỬ LÝ
310
BỘ PHẬN LỌC TỆP TÀI LIỆU
320
BỘ PHẬN ÁNH XẠ DANH SÁCH TỆP
330

Fig.4

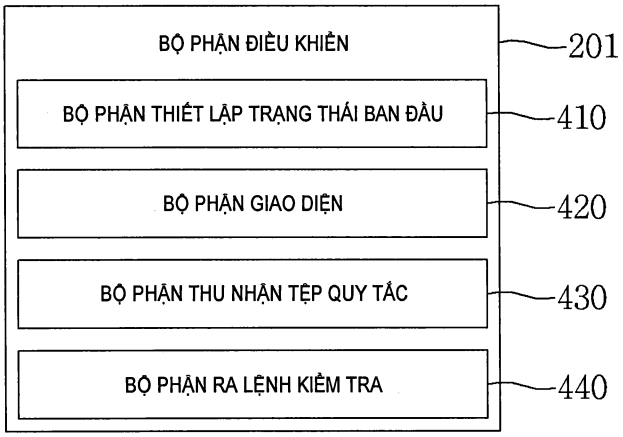

BỘ PHẬN ĐIỀU KHIỂN
201
BỘ PHẬN THIẾT LẬP TRẠNG THÁI BAN ĐẦU
410
BỘ PHẬN GIAO DIỆN
420
BỘ PHẬN THU NHẬN TỆP QUY TẮC
430
BỘ PHẬN RA LỆNH KIỂM TRA
440

Fig.5

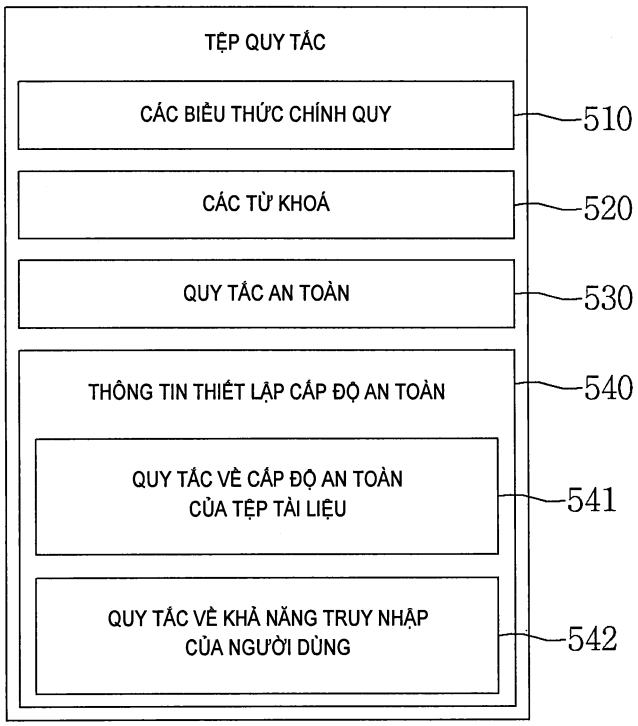

TỆP QUY TẮC
CÁC BIỂU THỨC CHÍNH QUY
510
CÁC TỪ KHOÁ
520
QUY TẮC AN TOÀN
530
THÔNG TIN THIẾT LẬP CẤP ĐỘ AN TOÀN
540
QUY TẮC VỀ CẤP ĐỘ AN TOÀN CỦA TỆP TÀI LIỆU
541
QUY TẮC VỀ KHẢ NĂNG TRUY NHẬP CỦA NGƯỜI DÙNG
542

Fig.6

HỆ SỐ QUAN TRỌNG	TỪ
1	"NĂM VÀO CÔNG TY"
2	
3	. . . . .
4	. . . . .
5	"SỐ NHẬN DẠNG CỦA BAN LÃNH ĐẠO VÀ NHÂN VIÊN"

(a)

CẤP BẬC CỦA NGƯỜI DÙNG	VỊ TRÍ
1	BAN LÃNH ĐẠO
2	TRƯỞNG NHÓM HOẶC PHÓ PHÒNG
3	TRƯỞNG BỘ PHẬN
4	PHÓ BỘ PHẬN
5	NHÂN VIÊN BÌNH THƯỜNG

(b)

ĐIỂM SỐ TIẾP CẬN	CẤP ĐỘ AN TOÀN	KHẢ NĂNG TRUY NHẬP
20 HOẶC CAO HƠN	1	CẤP BẬC 1 HOẶC THẤP HƠN: ĐỌC (O), LƯU TRỮ (O), IN (O), SOẠN THẢO (O) CẤP BẬC 2: ĐỌC (X), LƯU TRỮ (X), IN (X), SOẠN THẢO (X) CẤP BẬC 3: ĐỌC (X), LƯU TRỮ (X), IN (X), SOẠN THẢO (X) CẤP BẬC 4: ĐỌC (X), LƯU TRỮ (X), IN (X), SOẠN THẢO (X) CẤP BẬC 5: ĐỌC (X), LƯU TRỮ (X), IN (X), SOẠN THẢO (X)
15 ~ 19	2	CẤP BẬC 2 HOẶC THẤP HƠN: ĐỌC (O), LƯU TRỮ (O), IN (O), SOẠN THẢO (O) CẤP BẬC 3: ĐỌC (O), LƯU TRỮ (X), IN (O), SOẠN THẢO (X) CẤP BẬC 4: ĐỌC (O), LƯU TRỮ (X), IN (X), SOẠN THẢO (X) CẤP BẬC 5: ĐỌC (X), LƯU TRỮ (X), IN (X), SOẠN THẢO (X)
10 ~ 14	3	CẤP BẬC 3 HOẶC THẤP HƠN: ĐỌC (O), LƯU TRỮ (O), IN (O), SOẠN THẢO (O) CẤP BẬC 4: ĐỌC (O), LƯU TRỮ (X), IN (O), SOẠN THẢO (O) CẤP BẬC 5: ĐỌC (O), LƯU TRỮ (X), IN (O), SOẠN THẢO (X)
6 ~ 9	4	CẤP BẬC 4 HOẶC THẤP HƠN: ĐỌC (O), LƯU TRỮ (O), IN (O), SOẠN THẢO (O) CẤP BẬC 5: ĐỌC (O), LƯU TRỮ (X), IN (O), SOẠN THẢO (O)
0 ~ 5	5	CẤP BẬC 5 HOẶC THẤP HƠN: ĐỌC (O), LƯU TRỮ (O), IN (O), SOẠN THẢO (O)

(c)

Fig.7

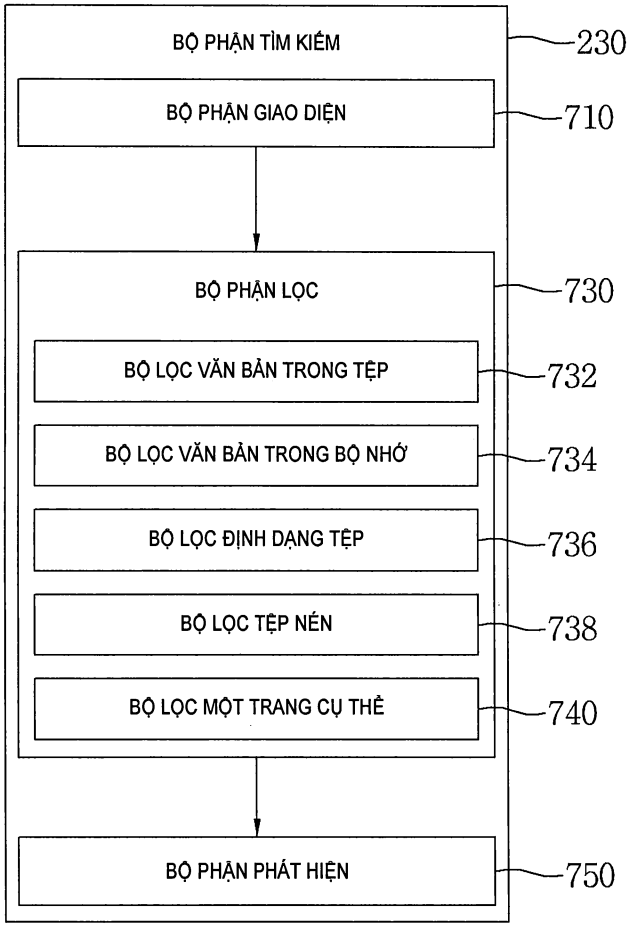

BỘ PHẬN TÌM KIẾM
230
BỘ PHẬN GIAO DIỆN
710
BỘ PHẬN LỌC
730
BỘ LỌC VĂN BẢN TRONG TỆP
732
BỘ LỌC VĂN BẢN TRONG BỘ NHỚ
734
BỘ LỌC ĐỊNH DẠNG TỆP
736
BỘ LỌC TỆP NÉN
738
BỘ LỌC MỘT TRANG CỤ THỂ
740
BỘ PHẬN PHÁT HIỆN
750

Fig.8

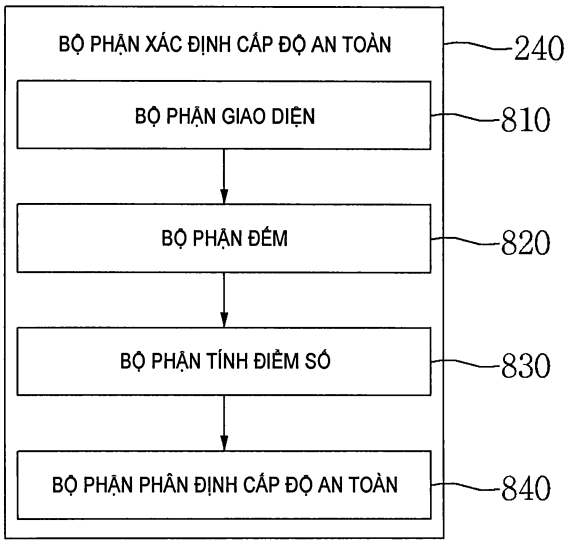

BỘ PHẬN XÁC ĐỊNH CẤP ĐỘ AN TOÀN
240
BỘ PHẬN GIAO DIỆN
810
BỘ PHẬN ĐẾM
820
BỘ PHẬN TÍNH ĐIỂM SỐ
830
BỘ PHẬN PHÂN ĐỊNH CẤP ĐỘ AN TOÀN
840

Fig.9

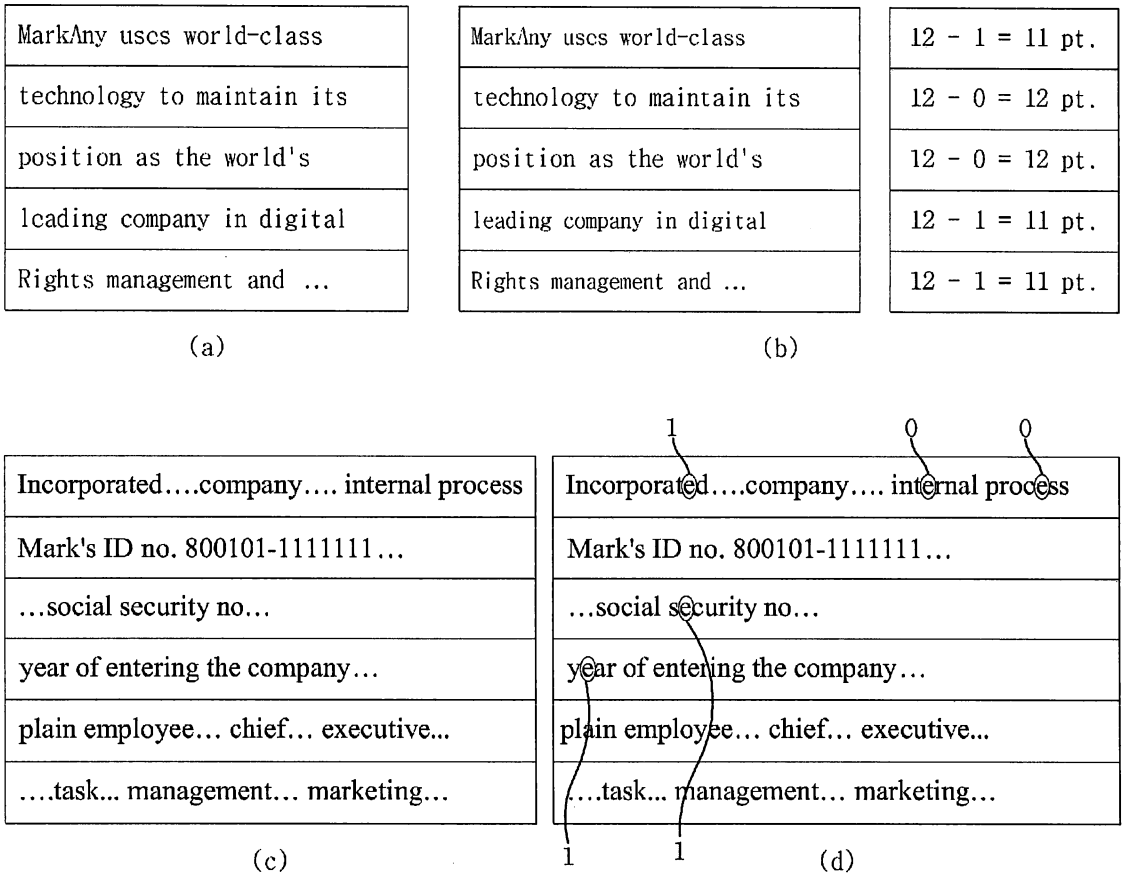

MarkAny uses world-class
technology to maintain its
position as the world's
leading company in digital
Rights management and ...
(a)
MarkAny uses world-class
technology to maintain its
position as the world's
leading company in digital
Rights management and ...
12 - 1 = 11 pt.
12 - 0 = 12 pt.
12 - 0 = 12 pt.
12 - 1 = 11 pt.
12 - 1 = 11 pt.
(b)
Incorporated....company.... internal process
Mark's ID no. 800101-1111111...
...social security no...
year of entering the company...
plain employee... chief... executive...
....task... management... marketing...
(c)
1
0
0
Incorporated....company.... internal process
Mark's ID no. 800101-1111111...
...social security no...
year of entering the company...
plain employee... chief... executive...
....task... management... marketing...
1
1
(d)

Fig.10

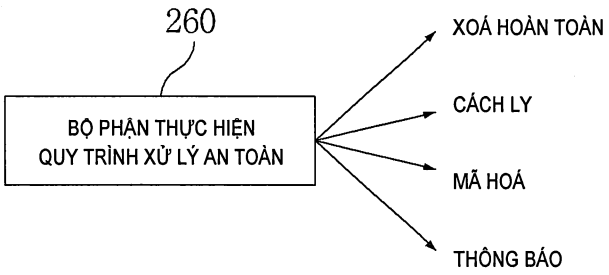

260
BỘ PHẬN THỰC HIỆN
QUY TRÌNH XỬ LÝ AN TOÀN
XOÁ HOÀN TOÀN
CÁCH LY
MÃ HOÁ
THÔNG BÁO

Fig.11

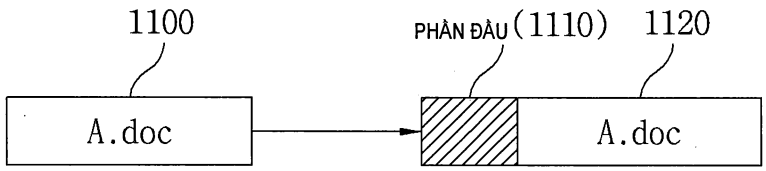

1100
PHẦN ĐẦU (1110)
1120
A.doc
A.doc

Fig.12

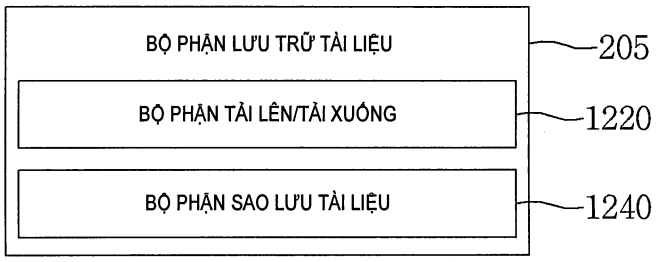

BỘ PHẬN LƯU TRỮ TÀI LIỆU
205
BỘ PHẬN TẢI LÊN/TẢI XUỐNG
1220
BỘ PHẬN SAO LƯU TÀI LIỆU
1240

Fig.13a

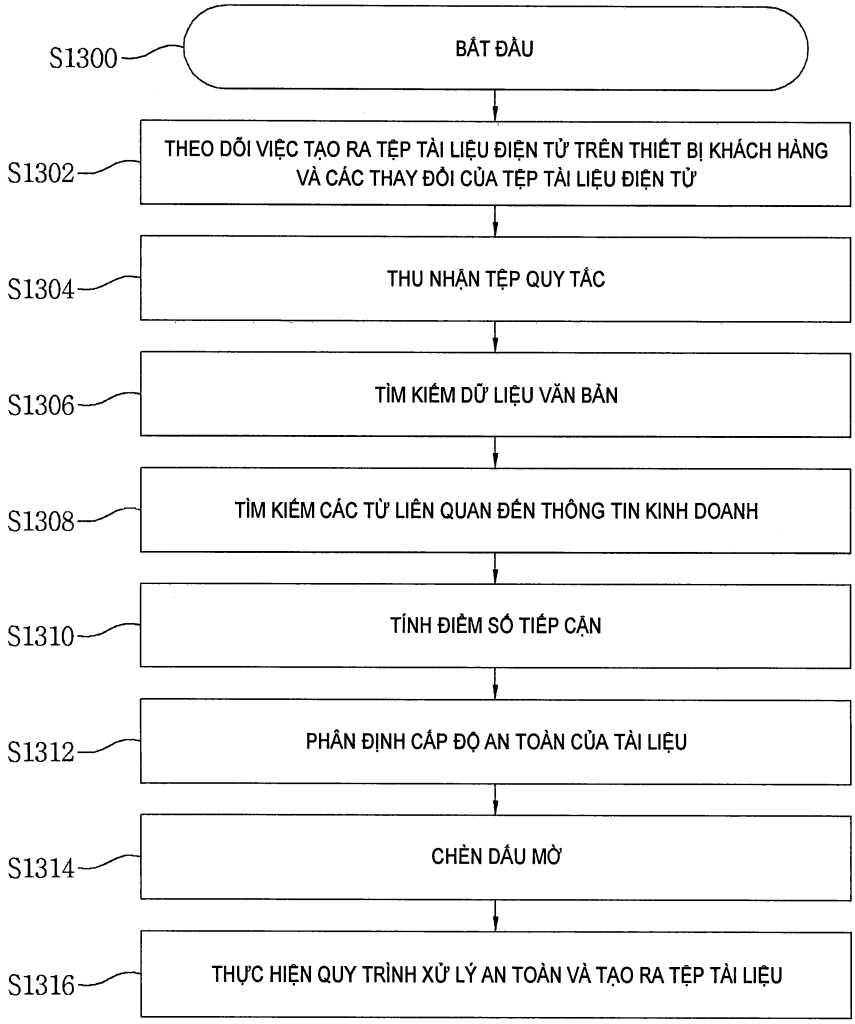
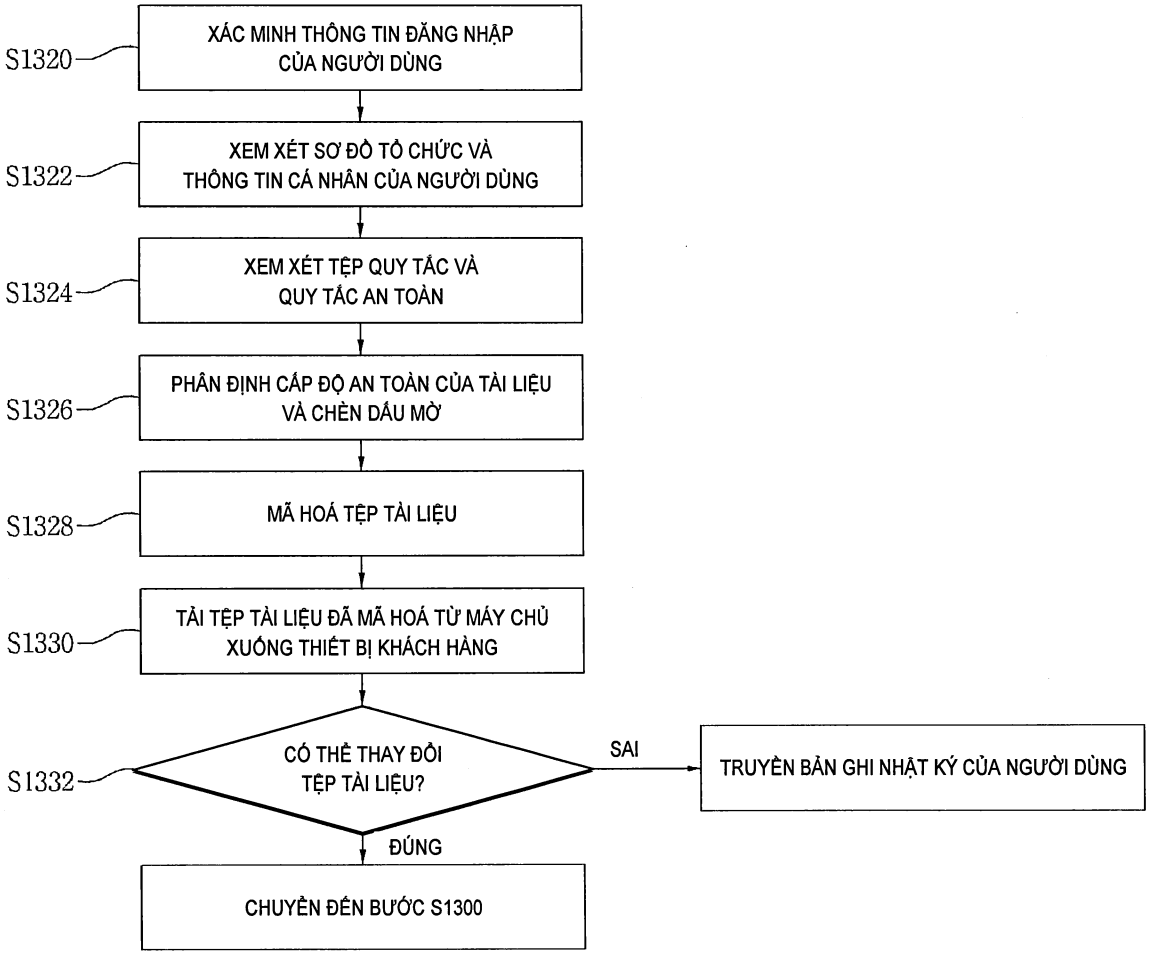

S1300
BẮT ĐẦU
S1302
THEO DÕI VIỆC TẠO RA TỆP TÀI LIỆU ĐIỆN TỬ TRÊN THIẾT BỊ KHÁCH HÀNG VÀ CÁC THAY ĐỔI CỦA TỆP TÀI LIỆU ĐIỆN TỬ
S1304
THU NHẬN TỆP QUY TẮC
S1306
TÌM KIẾM DỮ LIỆU VĂN BẢN
S1308
TÌM KIẾM CÁC TỪ LIÊN QUAN ĐẾN THÔNG TIN KINH DOANH
S1310
TÍNH ĐIỂM SỐ TIẾP CẬN
S1312
PHÂN ĐỊNH CẤP ĐỘ AN TOÀN CỦA TÀI LIỆU
S1314
CHÈN DẤU MỜ
S1316
THỰC HIỆN QUY TRÌNH XỬ LÝ AN TOÀN VÀ TẠO RA TỆP TÀI LIỆU

Fig.13b


S1320
XÁC MINH THÔNG TIN ĐĂNG NHẬP CỦA NGƯỜI DÙNG
S1322
XEM XÉT SƠ ĐỒ TỔ CHỨC VÀ THÔNG TIN CÁ NHÂN CỦA NGƯỜI DÙNG
S1324
XEM XÉT TỆP QUY TẮC VÀ QUY TẮC AN TOÀN
S1326
PHÂN ĐỊNH CẤP ĐỘ AN TOÀN CỦA TÀI LIỆU VÀ CHÈN DẤU MỜ
S1328
MÃ HOÁ TỆP TÀI LIỆU
S1330
TẢI TỆP TÀI LIỆU ĐÃ MÃ HOÁ TỪ MÁY CHỦ XUỐNG THIẾT BỊ KHÁCH HÀNG
S1332
CÓ THỂ THAY ĐỔI TỆP TÀI LIỆU?
SAI
TRUYỀN BẢN GHI NHẬT KÝ CỦA NGƯỜI DÙNG
ĐÚNG
CHUYỂN ĐẾN BƯỚC S1300