



(12) BẢN MÔ TẢ SÁNG CHẾ THUỘC BẢNG ĐỘC QUYỀN SÁNG CHẾ

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

(11)



1-0024705

(51)⁷ G06F 03/12; B41J 29/38

(13) B

(21) 1-2014-00451

(22) 13/02/2014

(30) 2013-030898 20/02/2013 JP

(45) 27/07/2020 388

(43) 25/08/2014 317A

(73) CANON KABUSHIKI KAISHA (JP)

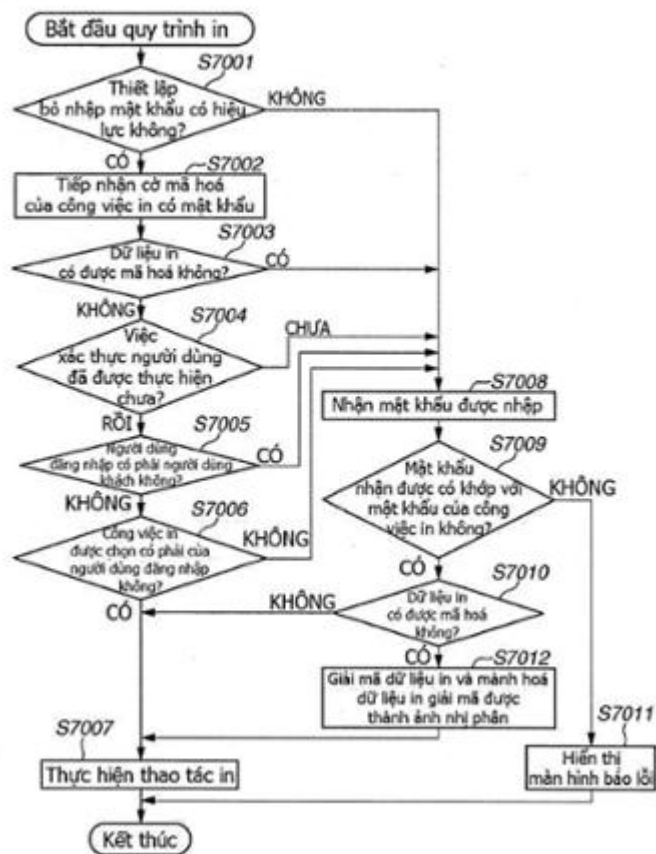
30-2, Shimomaruko 3-chome, Ohta-ku, Tokyo, 1468501, Japan

(72) Naoya Kakutani (JP).

(74) Công ty Luật TNHH Phạm và Liên danh (PHAM & ASSOCIATES)

(54) THIẾT BỊ TẠO ẢNH VÀ PHƯƠNG PHÁP TẠO ẢNH

(57) Sáng chế đề xuất thiết bị in bao gồm; khối lưu trữ được tạo cấu hình để lưu dữ liệu in có bao gồm mật khẩu khi nhận được dữ liệu in này, khối nhận được tạo cấu hình để nhận lệnh in từ người dùng đối với dữ liệu in được lưu, khối xác thực có khả năng thực hiện việc xác thực người dùng, và khối in được tạo cấu hình để thực hiện thao tác in mà không cần người dùng đã được xác thực phải nhập mật khẩu trong trường hợp chủ sở hữu của dữ liệu in được lệnh in là khớp với người dùng đã được xác thực này, và để thực hiện thao tác in đáp lại việc mật khẩu nhận được từ người dùng khớp với mật khẩu trong dữ liệu in, trong trường hợp chủ sở hữu của dữ liệu in được lệnh in không phải là người dùng đã được xác thực, hoặc trong trường hợp nhận được lệnh in mà khối xác thực không xác thực người dùng.



Lĩnh vực kĩ thuật được đề cập

Sáng chế đề cập đến thiết bị in để in dữ liệu in nhận được từ thiết bị bên ngoài.

Tình trạng kĩ thuật của sáng chế

Gần đây, hệ thống in dành riêng đã được sử dụng rộng rãi. Hệ thống in dành riêng này cho phép để dành dữ liệu in được truyền từ máy tính cá nhân (Personal Computer - PC) vào máy in hoặc máy chủ in. Trong hệ thống in dành riêng này, dữ liệu in được chứa trên đĩa cứng của máy in hoặc được lưu ở máy chủ trên mạng, và máy in sẽ bắt đầu in dữ liệu in này đáp lại thao tác cụ thể mà người dùng thực hiện trên máy in. Hệ thống in dành riêng này được sử dụng, ví dụ, trong trường hợp mà máy in là máy in dùng chung được nối mạng, và sản phẩm in được cần được ngăn không cho người khác xem được.

Công bố đơn sáng chế Nhật Bản số 1-264865 đề xuất máy in vốn nhận và tạm thời lưu lại dữ liệu in đã được bổ sung thông tin nhận dạng. Máy in này sẽ bắt đầu in nếu thông tin nhận dạng được bổ sung vào dữ liệu in là khớp với thông tin nhận dạng được nhập vào từ bảng điều khiển của máy in.

Ngoài ra, công bố đơn sáng chế Nhật Bản số 2003-182187 đề xuất thiết bị ghi ảnh vốn chỉ cho phép in công việc in của người dùng đã được xác thực. Thiết bị ghi ảnh này sẽ tích lũy các công việc in và thông tin người dùng khi nhận được công việc in được chỉ định để in riêng. Sau đó, thiết bị ghi ảnh này thực hiện việc xác thực người dùng để chỉ in công việc in của người dùng đã được xác thực.

Ngoài ra, công bố đơn sáng chế Nhật Bản số 2009-223610 đề xuất hệ thống in bao gồm máy in. Máy in này nhận dữ liệu in tương ứng với người dùng đã

được xác thực từ máy chủ in, và in dữ liệu in nhận được. Hệ thống in này cho phép máy in này xoá thông tin mật khẩu khỏi dữ liệu in để in dữ liệu in này.

Tuy nhiên, phương pháp in dành riêng nêu trên gặp phải các vấn đề như sau trong trường hợp xác thực người dùng, và máy in in dữ liệu in mà cần người dùng phải nhập thông tin nhận dạng để thực hiện thao tác in. Tức là mặc dù người dùng đã được xác thực rồi nhưng vẫn cần phải nhập thông tin nhận dạng để thực hiện công việc in. Điều này khiến thao tác người dùng trở nên phức tạp.

Ngoài ra, trong trường hợp cần xác thực người dùng để in, thì người dùng chưa được xác thực sẽ không thể ra lệnh cho máy in in dữ liệu in dành riêng. Điều này ảnh hưởng rất xấu đến khả năng sử dụng.

Bản chất kĩ thuật của sáng chế

Mục đích của sáng chế là đề xuất thiết bị in có khả năng thực hiện thao tác in dành riêng một cách có lựa chọn sau khi đã xác thực người dùng hoặc sau khi mật khẩu được người dùng nhập vào.

Một khía cạnh của sáng chế đề xuất thiết bị in bao gồm khối thu nhận được tạo cấu hình để nhận dữ liệu in bao gồm mật khẩu, khối lưu trữ được tạo cấu hình để lưu dữ liệu in mà khối thu nhận nhận được, khối nhận được tạo cấu hình để nhận lệnh in từ người dùng đối với dữ liệu in được lưu ở khối lưu trữ, khối xác thực có khả năng thực hiện việc xác thực người dùng, và khối in được tạo cấu hình để thực hiện thao tác in mà không bắt người dùng đã được xác thực phải nhập mật khẩu trong trường hợp chủ sở hữu của dữ liệu in được lệnh in là khớp với người dùng được xác thực bởi khối xác thực, và để in dữ liệu in khi mật khẩu nhận được từ người dùng là khớp với mật khẩu được bao gồm trong dữ liệu in được lưu ở khối lưu trữ trong trường hợp chủ sở hữu của dữ liệu in được lệnh in là khác với người dùng được xác thực bởi khối xác thực, hoặc trong trường hợp khối nhận nhận được lệnh in mà khối xác thực không xác thực

người dùng.

Các dấu hiệu khác của sáng chế sẽ được làm rõ hơn trong phần mô tả chi tiết sáng chế, có dựa vào các hình vẽ kèm theo.

Mô tả vắn tắt các hình vẽ

Fig.1 là hình minh hoạ tổng thể hệ thống mạng bao gồm thiết bị in là thiết bị ngoại vi đa năng và thiết bị ngoại là PC.

Fig.2 là lưu đồ minh hoạ quy trình truyền công việc in được thực hiện bởi PC nêu trên.

Fig.3A và Fig.3B là các sơ đồ minh hoạ ví dụ về màn hình thiết lập của trình điều khiển máy in của PC này.

Fig.4 là lưu đồ minh hoạ quy trình nhận công việc in được thực thi bởi thiết bị ngoại vi đa năng nêu trên.

Fig.5 là lưu đồ minh hoạ chuỗi các thao tác được thực hiện khi thiết bị ngoại vi đa năng này nhận được thao tác người dùng.

Fig.6 là lưu đồ minh hoạ quy trình đăng nhập được thực thi bởi thiết bị ngoại vi đa năng nêu trên.

Fig.7 là lưu đồ minh hoạ quy trình in được thực thi bởi thiết bị ngoại vi đa năng này.

Fig.8 là lưu đồ minh hoạ quy trình huỷ in được thực thi bởi thiết bị ngoại vi đa năng này.

Fig.9 là sơ đồ minh hoạ danh sách công việc của các công việc in có mật khẩu.

Fig.10 là sơ đồ minh hoạ ví dụ về màn hình thiết lập được sử dụng để kiểm duyệt thiết lập bỏ nhập mật khẩu.

Fig.11 là lưu đồ minh hoạ quy trình huỷ in theo phương án minh hoạ thứ hai.

Fig.12 là sơ đồ minh hoạ ví dụ về màn hình thiết lập được sử dụng để kiểm

duyet thiết lập bỏ nhập mật khẩu theo phương án minh hoạ thứ hai.

Fig.13 là sơ đồ minh hoạ ví dụ về màn hình đăng nhập được hiển thị khi người dùng đăng nhập vào thiết bị ngoại vi đa năng nêu trên.

Mô tả chi tiết sáng chế

Các phương án minh hoạ, các dấu hiệu và các khía cạnh khác nhau của sáng chế sẽ được mô tả chi tiết dưới đây, có dựa vào các hình vẽ kèm theo.

Trước hết, các thuật ngữ được sử dụng cho các phương án minh hoạ này sẽ được định nghĩa. Ở các phương án minh hoạ này, công việc để in dữ liệu in bao gồm mật khẩu được gọi là “công việc in có mật khẩu”. Công việc in có mật khẩu này sẽ khiến thao tác in bắt đầu nếu mật khẩu mà người dùng nhập vào để in là khớp với mật khẩu được bao gồm trong dữ liệu in.

Ngoài ra, ở các phương án minh hoạ này, công việc in có mật khẩu bao gồm dữ liệu định in được mã hoá sẽ được gọi là “công việc in được mã hoá có mật khẩu”.

Phương án minh hoạ thứ nhất sẽ được mô tả.

Fig.1 là hình minh hoạ tổng thể hệ thống mạng bao gồm thiết bị ngoại vi đa năng số (sau đây được gọi là MFP) 1000 và máy tính cá nhân (sau đây được gọi là PC) 2000. Trong hệ thống mạng được minh hoạ trên Fig.1, MFP 1000 và PC 2000 được nối truyền thông với nhau qua mạng 101.

Mạng 101 có thể được nối với nhiều MFP (không được minh hoạ trên hình vẽ) và các PC khác (không được minh hoạ) thông qua thiết bị chuyển tiếp (không được minh hoạ), chẳng hạn bộ chia chuyển mạch và bộ định tuyến. Ngoài ra, hệ thống mạng trên Fig.1 có thể được nối với mạng Internet qua bộ định tuyến (không được minh hoạ) được nối với mạng 101.

Trong hệ thống mạng được minh hoạ trên Fig.1, mỗi trong số MFP 1000 và PC 2000 đều có địa chỉ IP (Internet Protocol - giao thức Internet) và tên duy

nhất. Ngoài ra, hệ thống mạng này còn có tên miền duy nhất để cho biết vị trí của nó trên mạng Internet.

Theo phương án minh hoạ này, MFP 1000 được lấy làm ví dụ về thiết bị in. Tuy nhiên, thiết bị in này cũng có thể là thiết bị ngoại vi một chức năng thay vì MFP 1000, miễn là thiết bị ngoại vi một chức năng này có chức năng thực hiện công việc in có mặt khẩu.

Ngoài ra, theo phương án minh hoạ này, PC 2000 được lấy làm ví dụ về thiết bị ngoại vi. Tuy nhiên, thiết bị ngoại vi này cũng có thể là máy tính để bàn dùng chung, máy tính chủ, hoặc thiết bị đầu cuối di động, thay vì PC 2000.

Tiếp theo, cấu hình phần cứng của MFP 1000 sẽ được mô tả.

Khối điều khiển 200 kết nối máy quét 201, vốn có chức năng như thiết bị nhập ảnh, với máy in 202 vốn có chức năng như thiết bị xuất ảnh. Khối điều khiển 200 được nối với mạng 101 và đường dây công cộng 204, để thông tin được nhập vào và được xuất ra qua lại giữa khối điều khiển 200 và thiết bị ngoại vi này.

Bộ xử lý trung tâm (Central Processing Unit - CPU) 205 là bộ xử lý để điều khiển toàn bộ MFP 1000. Bộ nhớ truy cập ngẫu nhiên (Random Access Memory - RAM) 206 có chức năng như bộ nhớ làm việc của hệ thống để CPU 205 hoạt động. RAM 206 còn có chức năng như bộ nhớ để tạm thời chứa dữ liệu ảnh, tên người dùng và mật khẩu. Bộ nhớ chỉ đọc (Read Only Memory - ROM) 207 là ROM khởi động mà trong đó chương trình khởi động của hệ thống được chứa. Ổ đĩa cứng (Hard Disk Drive - HDD) 208 chứa phần mềm hệ thống, các ứng dụng và dữ liệu ảnh. Ngoài ra, HDD 208 còn chứa các chương trình được sử dụng để thực hiện các lưu đồ sẽ được mô tả dưới đây theo phương án minh hoạ này. Chương trình được chứa trong HDD 208 sẽ được nạp vào RAM 206 và được thực thi bởi CPU 205.

Mỗi bước của lưu đồ được mô tả ở phương án minh hoạ này đều được thực

thi bởi CPU 205. Ở mỗi bước, CPU 205 đều thực thi chương trình điều khiển được chứa trên HDD 208. Theo cách khác, mỗi bước của lưu đồ này cũng có thể được thực hiện bởi bộ xử lý không phải là CPU 205, hoặc bởi tổ hợp giữa bộ xử lý này với CPU 205.

Giao diện khối vận hành 209 giao tiếp với khối vận hành 210 gồm bảng cảm ứng tinh thể lỏng. Giao diện khối vận hành 209 xuất ra dữ liệu ảnh cần hiển thị trên khối vận hành 210 đến khối vận hành 210. Ngoài ra, giao diện khối vận hành 209 còn có chức năng báo cho CPU 205 biết về thông tin được người dùng hệ thống này nhập vào bằng bàn phím trên khối vận hành 210. Giao diện mạng 211 được nối với mạng 101 để nhập và xuất dữ liệu. Môđem 212 được nối với đường dây công cộng 204, và biến đổi tín hiệu số thành tín hiệu tương tự. Bộ nhớ truy cập ngẫu nhiên tĩnh (SRAM) 213 là phương tiện ghi bất biến có thể hoạt động ở tốc độ cao. Đồng hồ thời gian thực (Real Time Clock - RTC) 214 sẽ duy trì thời gian hiện thời ngay cả khi khối điều khiển 200 bị tắt nguồn. Các thiết bị này được bố trí trên buýt hệ thống 215.

Giao diện buýt hình ảnh 216, vốn có chức năng như cầu buýt, kết nối buýt hệ thống 215 với buýt hình ảnh 217 để truyền dữ liệu ảnh với tốc độ cao và thực hiện việc biến đổi cấu trúc dữ liệu. Buýt hình ảnh 217 bao gồm buýt PCI (Peripheral Component Interconnect - giao diện kết nối thành phần ngoại vi) hoặc buýt IEEE (Institute of Electrical and Electronics Engineers - viện kỹ thuật điện và điện tử) 1394. Các thiết bị sau đây được bố trí trên buýt hình ảnh 217.

Bộ xử lý ảnh màn hình (Raster Image Processor - RIP) 218 màn hình hoá mã PDL (Page Description Language - ngôn ngữ mô tả trang) thành ảnh nhị phân. Khối giao diện thiết bị 219 kết nối các thiết bị nhập/xuất hình ảnh là máy quét 201 và máy in 202 với khối điều khiển 200. Khối giao diện thiết bị 219 thực hiện việc biến đổi đồng bộ/dị bộ đối với dữ liệu ảnh. Khối xử lý ảnh máy quét 220 thì điều chỉnh, xử lý và chỉnh sửa dữ liệu ảnh được nhập vào. Khối xử lý ảnh máy in 221

thì thực hiện các thao tác chẳng hạn như điều chỉnh máy in và chuyển đổi độ phân giải đối với dữ liệu ảnh cần in ra. Khối xử lý mã hoá 222 thì mã hoá dữ liệu được nhập vào. Khối xử lý giải mã 223 thì giải mã dữ liệu mã hoá nếu dữ liệu nhận được (bao gồm dữ liệu in) đã được mã hoá.

Tiếp theo, cấu hình phần cứng của PC 2000 sẽ được mô tả. PC 2000 bao gồm CPU 26, bộ nhớ chính 27, ổ đĩa 21, khối vận hành 23, khối truyền thông 25, và khối hiển thị 24. CPU 26 là bộ xử lý để điều khiển các hoạt động của PC 2000. CPU 26 nạp các chương trình trên đĩa 21 vào bộ nhớ chính 27 và thực hiện các tiến trình khác nhau. Ổ đĩa 21 chứa các chương trình khác nhau (không được minh hoạ trên hình vẽ), chẳng hạn hệ điều hành (Operating System - OS) và ứng dụng tạo tài liệu. Ngoài ra, ổ đĩa 21 còn chứa chương trình điều khiển máy in (dưới đây được gọi là trình điều khiển máy in) 22 tương ứng với MFP 1000.

Khối truyền thông 25 truyền và nhận các thông tin khác nhau qua lại giữa các thiết bị được nối với mạng 101. Khối vận hành 23 là, ví dụ, chuột và bàn phím, và có chức năng như thiết bị nhập liệu để nhận dữ liệu nhập từ người dùng. Khối hiển thị 24 là, ví dụ, màn hình tinh thể lỏng, và có chức năng như thiết bị xuất để xuất ra dữ liệu đã được CPU 26 xử lý.

Fig.2 là lưu đồ minh hoạ các thao tác được thực hiện khi PC 2000 truyền công việc in có mật khẩu đến MFP 1000. Mỗi bước của lưu đồ trên Fig.2 đều được thực hiện bởi CPU 26 bằng cách thực thi chương trình vốn được nạp từ đĩa 21 vào bộ nhớ chính 27.

Ở bước S2001, PC 2000 nhận lệnh in từ người dùng thông qua khối thao tác 23, để MFP 1000 thực hiện thao tác in. Khi nhận được lệnh in thì CPU 26 kích hoạt trình điều khiển máy in 22 tương ứng với MFP 1000, và hiển thị màn hình thiết lập in 0301, như được minh hoạ trên Fig.3A, trên khối hiển thị 24 của PC.

Fig.3A là hình minh hoạ ví dụ của màn hình được hiển thị bởi trình điều

hiển máy in 22 ở bước S2001. Hộp đánh dấu 0302 được hiển thị trên màn hình thiết lập in 0301 trên Fig.3A. Với hộp đánh dấu 0302 này, người dùng sẽ thiết lập xem có kiểm duyệt thao tác in đối với công việc in có mật khẩu hay không. Ngoài ra, hộp đánh dấu 0303, nút OK 0304 và nút CANCEL 0305 cũng được hiển thị trên màn hình thiết lập in 0301. Hộp đánh dấu 0303 được sử dụng để thiết lập xem có mã hoá dữ liệu hay không.

Người dùng đặt dấu chọn vào hộp đánh dấu 0302 nếu người dùng muốn thêm mật khẩu vào công việc in, và truyền công việc in thu được đến MFP 1000. Nếu dấu chọn được đặt vào hộp đánh dấu 0302 thì người dùng cũng có thể đặt dấu chọn vào hộp đánh dấu 0303. Khi dấu chọn được đặt vào hộp đánh dấu 0303 thì dữ liệu in (dữ liệu định in) sẽ được mã hoá, và dữ liệu in được mã hoá này được truyền đến MFP 1000. Ở đây, mật khẩu nhận được từ người dùng thông qua màn hình như được minh hoạ trên Fig.3B sẽ được sử dụng làm khoá mã hoá.

Ngoài ra, các thiết lập in, chẳng hạn khổ giấy, số lượng bản in, và việc có thêm nhãn hay không, cũng có thể được thiết lập trên màn hình thiết lập in 0301. Trình điều khiển máy in 22 tạo ra công việc in bao gồm các thiết lập in này. Theo ví dụ được minh hoạ trên Fig.3A, các thiết lập in là như sau: thao tác in đối với công việc in có mật khẩu là có hiệu lực; khổ giấy in là A4; số lượng bản in là 1; và không cần thêm nhãn.

Ở bước S2002, trình điều khiển máy in 22 tiếp nhận thao tác người dùng được thực hiện trên màn hình thiết lập in 0301, và ghi các thiết lập in này vào RAM (không được minh hoạ) của PC 2000. Khi CPU 26 dò thấy nút OK 0304 được nhấn thì tiến trình tiến đến bước S2003. Ở đây, việc nhấn nút OK 304 hiển thị việc đã thiết lập xong công việc in.

Ở bước S2003, trình điều khiển máy in 22 xác định xem có cần tạo ra công việc in có mật khẩu hay không, dựa trên thiết lập nhận được ở bước S2002.

Nếu trình điều khiển máy in 22 xác định được rằng cần tạo ra công việc in có mật khẩu ("CÓ" ở bước S2003) thì tiến trình tiến đến bước S2004. Ở bước S2004, trình điều khiển máy in 22 hiển thị tên người dùng và màn hình nhập mật khẩu cho công việc 0321, như được minh họa trên Fig.3B, trên khối hiển thị 24 của PC, và nhận tên người dùng và mật khẩu từ người dùng. Ngược lại, nếu trình điều khiển máy in 22 xác định được rằng không cần tạo ra công việc in có mật khẩu ("KHÔNG" ở bước S2003), tức là cần tạo ra công việc in bình thường, thì tiến trình tiến đến bước S2008. Ở bước S2008, trình điều khiển máy in 22 tạo ra công việc in bình thường theo thiết lập in đã được thiết lập, và truyền dữ liệu in và công việc in tạo ra được này đến MFP 1000.

Fig.3B minh họa tên người dùng và màn hình nhập mật khẩu cho công việc 0321 được hiển thị ở bước S2004. Người dùng nhập tên người dùng vào trường nhập tên người dùng 0322 và nhập mật khẩu vào trường nhập mật khẩu 0323 trên màn hình được minh họa trên Fig.3B. Tên người dùng và mật khẩu được nhập vào sẽ được thêm vào công việc in, và công việc in thu được sẽ được truyền đến MFP 1000.

Tên người dùng được nhập vào trường nhập tên người dùng 0322 là danh tính (Identification - ID) người dùng (tức bộ nhận dạng người dùng) để nhận dạng chủ sở hữu của công việc in. Sau đó, tên người dùng này được sử dụng để đối chiếu người dùng đã đăng nhập vào MFP 1000 với chủ sở hữu của công việc (tuy nhiên, tên người dùng này sẽ không được sử dụng để đối chiếu nếu việc xác thực người dùng không được thực hiện ở MFP 1000). Tên người dùng được đặt trước làm giá trị ban đầu ở PC 2000 được nhập vào màn hình được minh họa trên Fig.3B. Tuy nhiên, tên người dùng cũng có thể được thay đổi nếu cần trên màn hình được minh họa trên Fig.3B.

Mật khẩu được nhập vào trường nhập mật khẩu 0323 là thông tin cần thiết khi MFP 1000 bắt đầu in sau đó. Tức là công việc in được thêm mật khẩu (công việc in có mật khẩu) sẽ được giữ ở trạng thái chờ trong MFP 1000 trong lúc MFP 1000 đang đợi nhập mật khẩu. MFP 1000 bắt đầu in khi mật khẩu (được nhập từ người dùng trên màn hình được minh hoạ trên Fig.3B) được nhập vào bằng khối thao tác 210. Theo đó, công việc in có mật khẩu chỉ có thể được in ra bởi người biết mật khẩu đã được thêm vào công việc này. Điều này có thể giảm bớt khả năng đánh cắp của người không biết mật khẩu khi nhìn lướt vào sản phẩm được in. Mặt khác, người dùng không chỉ cần phải nhập mật khẩu vào PC 2000 mà còn cần phải nhập mật khẩu vào MFP 1000 đối với công việc in có mật khẩu. Mặc dù điều này giữ được tính bảo mật nhưng người dùng phải mất thêm công sức để nhập mật khẩu vào MFP 1000. Do đó, theo phương án minh hoạ này, việc nhập mật khẩu vào MFP 1000 có thể được bỏ bớt nếu người dùng đã được xác thực trước khi đăng nhập vào MFP 1000. Việc bỏ bớt thao tác nhập mật khẩu này sẽ được mô tả chi tiết dưới đây. Theo phương án minh hoạ này, người dùng nhập vào mật khẩu bằng cách sử dụng màn hình được minh hoạ trên Fig.3B. Tuy nhiên, trình điều khiển máy in 22 cũng có thể tạo ra mật khẩu duy nhất cho mỗi công việc. Trong trường hợp này, mật khẩu được tạo ra bởi trình điều khiển máy in 22 sẽ được hiển thị và được thông báo cho người dùng. Ngoài ra, trình điều khiển máy in 22 cũng có thể yêu cầu MFP 1000 tạo ra mật khẩu. Trong trường hợp này, trình điều khiển máy in 22 nhận mật khẩu mà MFP 1000 tạo ra và thông báo cho người dùng biết về mật khẩu nhận được.

Phần mô tả này lại dựa vào Fig.2. Ở bước S2004, trình điều khiển máy in 22 nhận tên người dùng và mật khẩu mà người dùng nhập vào qua khối vận hành 23 của PC. Tên người dùng và mật khẩu nhận được ở bước S2004 là tên người dùng và mật khẩu được nhập vào trường nhập tên người dùng 0322 và trường nhập mật khẩu 0323 (xem Fig.3B), vốn được hiển thị trên khối hiển thị 24 của

PC. Khi khởi vận hành 23 của PC nhận được sự kiện nhấn nút OK 0324, vốn biểu thị rằng việc thiết lập công việc in có mật khẩu đã hoàn tất, thì tiến trình tiến đến bước S2005.

Ở bước S2005, trình điều khiển máy in 22 xác định xem dữ liệu định in có cần được mã hoá hay không, dựa trên thiết lập mã hoá nhận được ở bước S2002. Nếu trình điều khiển máy in 22 xác định được rằng dữ liệu định in là cần phải được mã hoá ("CÓ" ở bước S2005) thì tiến trình tiến đến bước S2007. Nếu trình điều khiển máy in 22 xác định được rằng dữ liệu định in là không cần phải được mã hoá ("KHÔNG" ở bước S2005) thì tiến trình tiến đến bước S2006.

Ở bước S2006, trình điều khiển máy in 22 tạo ra công việc in có mật khẩu bao gồm dữ liệu định in (dữ liệu in), tên người dùng và mật khẩu, và truyền công việc in được tạo ra đến MFP 1000. Công việc in này còn bao gồm tên miền của PC 2000 và các thông tin khác. Tên người dùng thì được sử dụng để đối chiếu người dùng đã đăng nhập vào MFP 1000 với chủ sở hữu của công việc, còn mật khẩu thì được sử dụng khi MFP 1000 bắt đầu in.

Ở bước S2007, trình điều khiển máy in 22 mã hoá dữ liệu in với mật khẩu nhận được ở bước S2004 dưới dạng khoá mã hoá. Ở đây, trình điều khiển máy in 22 sử dụng thuật toán, chẳng hạn thuật toán SHA (Secure Hash Algorithm - thuật toán băm bảo mật) 256 làm phương pháp mã hoá với mật khẩu nêu trên. Trình điều khiển máy in 22 truyền công việc in (công việc in được mã hoá có mật khẩu) bao gồm cờ mã hoá, vốn biểu thị rằng dữ liệu in đã được mã hoá, dữ liệu in đã mã hoá, tên người dùng và mật khẩu, đến MFP 1000.

Ở bước S2008, trình điều khiển máy in 22 tạo ra công việc in bao gồm dữ liệu in, tên người dùng và mật khẩu nêu trên dưới dạng công việc in có mật khẩu, và truyền công việc in tạo ra được này đến MFP 1000.

Do đó, theo quy trình được minh hoạ trên Fig.2, công việc in này được truyền từ trình điều khiển máy in 22 của PC 2000 đến MFP 1000.

Fig.4 là lưu đồ minh hoạ các thao tác được thực hiện khi MFP 1000 nhận công việc in. Mỗi bước được minh hoạ trên Fig.4 đều được thực hiện bởi CPU 205 bằng cách thực thi chương trình được nạp từ HDD 208 vào RAM 206. Tiến trình trên Fig.4 bắt đầu khi MFP 1000 nhận công việc in từ PC 2000 (hoặc thiết bị ngoài khác).

Ở bước S4001, CPU 205 nhận công việc in được truyền từ PC 2000 qua giao diện mạng 211. Sau đó, CPU 205 trích xuất ra dữ liệu in và thiết lập in từ công việc in nhận được.

Ở bước S4002, CPU 205 xác định xem công việc in nhận được có phải là công việc in có mật khẩu hay không, dựa trên thiết lập in được trích xuất ở bước S4001. Cụ thể là CPU 205 sẽ kiểm tra xem công việc in có mật khẩu này có bao gồm mật khẩu công việc hay không. Nếu công việc in có mật khẩu này bao gồm mật khẩu công việc thì CPU 205 xác định rằng công việc nhận được là công việc in có mật khẩu ("CÓ" ở bước S4002), và tiến trình tiến đến bước S4003. Ngược lại, nếu CPU 205 xác định được rằng công việc nhận được không phải là công việc in có mật khẩu ("KHÔNG" ở bước S4002) thì tiến trình tiến đến bước S4004.

Ở bước S4003, CPU 205 xuất ra dữ liệu in nhận được cho khối RIP 218. Sau đó, CPU 205 liên kết dữ liệu ảnh nhị phân, mà khối RIP 218 đã mã hoá, với trạng thái chờ nhập mật khẩu, và lưu dữ liệu nhận được vào HDD 208. Dữ liệu ảnh nhị phân được lưu ở bước S4003 sẽ không được xuất ra máy in 202 cho đến khi mật khẩu công việc và mật khẩu được nhập, vốn được nhập qua khối thao tác 210, được được đối chiếu với nhau. Tức là công việc in có mật khẩu nhận được này sẽ được để dành, thay vì được in ở bước này. Ngoài ra, ở bước S4003, tên miền, tên người dùng và mật khẩu công việc trong các thiết lập in sẽ được quản lý bằng cách được liên kết với dữ liệu ảnh nhị phân.

Nếu CPU 205 xác định được rằng công việc nhận được không phải là công

việc in có mật khẩu ("KHÔNG" ở bước S4002), tức là dữ liệu nhận được chỉ là công việc in bình thường, thì tiến trình tiến đến bước S4004. Ở bước S4004, CPU 205 xuất dữ liệu in nhận được đến khối RIP 218, sau đó xuất dữ liệu ảnh nhị phân đã được mảnh hoá bởi khối RIP 218 đến máy in 202. Theo đó, máy in 202 in hình ảnh lên tấm vật liệu in (giấy in) dựa trên dữ liệu ảnh nhị phân được xuất ra này.

Chuỗi các thao tác này được thực hiện khi MFP 1000 nhận được công việc in.

Phương án minh hoạ này đã được mô tả bằng cách sử dụng trường hợp ví dụ mà trong đó công việc in không có mật khẩu (công việc in bình thường) được in mà không được để dành. Tuy nhiên, MFP 1000 cũng có thể được thiết lập ở chế độ dành riêng ép buộc. Trong trường hợp này, dữ liệu in sẽ được để dành bởi tiến trình như bước S4003 ngay cả khi mật khẩu không được thêm vào công việc in.

Ở bước S4003, trên thực tế, CPU 205 kiểm tra xem công việc in nhận được có bao gồm cờ mã hoá hay không, và xác định xem dữ liệu in trong công việc in này có được mã hoá hay không, mặc dù thao tác này không được minh hoạ trên Fig.4. Nếu CPU 205 xác định được rằng có cờ mã hoá thì điều này có nghĩa là dữ liệu in trong công việc in là được mã hoá. Theo đó, dữ liệu in này sẽ không thể được mảnh hoá thành ảnh nhị phân, trừ khi dữ liệu in này được giải mã bằng mật khẩu. Do đó, CPU 205 sẽ lưu nguyên dữ liệu in được mã hoá này vào HDD 208.

Ngược lại, nếu không có cờ mã hoá trong công việc in thì điều này có nghĩa là dữ liệu in trong công việc in chỉ là văn bản thuần. Do đó, CPU 205 chuyển dữ liệu in là văn bản thuần này đến khối RIP 218 để mảnh hoá dữ liệu in này thành ảnh nhị phân. Sau đó, CPU 205 lưu ảnh nhị phân này vào HDD 208. Theo đó, trong trường hợp mà dữ liệu in không được mã hoá thì nó sẽ được mảnh hoá

thành ảnh nhị phân khi nhận được công việc in có mật khẩu. Điều này có thể rút ngắn khoảng thời gian từ lúc người dùng đi đến chỗ MFP 1000 để ra lệnh in đến lúc sản phẩm được in được nhả ra.

Fig.5 là lưu đồ minh họa các thao tác được thực hiện khi MFP 1000 thực hiện hoặc huỷ thao tác in đối với công việc in có mật khẩu. Tương tự như trên Fig.4, mỗi bước được minh họa trên Fig.5 đều được thực hiện bởi CPU 205 bằng cách thực thi chương trình được nạp từ HDD 208 vào RAM 206.

Ở bước S5001, CPU 205 tiếp nhận giá trị thiết lập của MFP 1000 từ SRAM 213, và xác định xem có cần xác thực người dùng hay không, dựa trên giá trị thiết lập tiếp nhận được này. Giả sử rằng thiết lập để xác định sự cần thiết của việc xác thực người dùng là đã được người quản trị hệ thống đăng kí trước ở MFP 1000. Ngoài ra, thông tin xác thực (ID người dùng, mật khẩu) của mỗi người dùng là đã được người quản trị hệ thống đăng kí trước ở MFP 1000 hoặc máy chủ xác thực (không được minh họa trên hình vẽ) trên mạng. Thông tin xác thực này được sử dụng khi việc xác thực người dùng được thực hiện.

Nếu CPU 205 xác định được rằng việc xác thực người dùng là cần thiết ("CÓ" ở bước S5001) thì ở bước S5002, CPU 205 thực hiện quy trình đăng nhập. Quy trình đăng nhập này sẽ được mô tả chi tiết dựa vào Fig.6. Khi người dùng đăng nhập vào MFP 1000 bằng quy trình đăng nhập này thì thông tin về người dùng đăng nhập sẽ được ghi vào RAM 206. Sau đó, tiến trình tiến đến bước S5003. Ngược lại, nếu CPU 205 xác định được rằng việc xác thực người dùng là không cần thiết ("KHÔNG" ở bước S5001) thì tiến trình sẽ tiến đến bước S5003 mà không thực hiện quy trình đăng nhập ở bước S5002.

Ở bước S5003, CPU 205 tiếp nhận giá trị thiết lập của MFP 1000 từ SRAM 213 và xác định xem việc xác thực người dùng đã được MFP 1000 thực hiện hay chưa. Ở đây, CPU 205 thực hiện thao tác xác định này bằng cách dựa vào giá trị thiết lập được sử dụng trong tiến trình ở bước S5001. Tức là, nếu giá trị thiết lập

tiếp nhận được ở bước S5001 từ SRAM 213 cho thấy rằng việc xác thực người dùng là cần thiết, thì thao tác xác thực người dùng là đã được thực hiện ở bước S5002. Do đó, CPU 205 xác định rằng việc xác thực người dùng là đã được thực hiện ("RỒI" ở bước S5003). Ngược lại, nếu giá trị thiết lập tiếp nhận được ở bước S5001 từ SRAM 213 cho thấy rằng việc xác thực người dùng là không cần thiết thì CPU 205 xác định rằng thao tác xác thực người dùng là chưa được thực hiện ("CHƯA" ở bước S5003).

Ở bước S5004, CPU 205 kiểm tra điều kiện hiển thị của danh sách công việc. Ví dụ, CPU 205 tiếp nhận thiết lập sàng lọc đối với danh sách công việc từ SRAM 213. Dựa trên thiết lập sàng lọc này, CPU 205 xác định xem sẽ hiển thị tất cả các công việc in hay chỉ hiển thị công việc in của người dùng đăng nhập thôi. Thiết lập sàng lọc này biểu thị thiết lập để xác định phạm vi in và phạm vi huỷ in của công việc trên danh sách công việc in 9002 được minh hoạ trên Fig.9. Nếu thiết lập sàng lọc này là có hiệu lực thì chỉ có công việc in của người dùng đăng nhập mới được hiển thị trên danh sách công việc in 9002. Trong trường hợp này, người dùng đăng nhập chỉ có thể in các công việc in có mật khẩu của riêng mình mà thôi. Ngược lại, nếu thiết lập sàng lọc nêu trên là không có hiệu lực thì tất cả các công việc in đã được để dành trong trạng thái chờ nhập mật khẩu trên HDD 208 sẽ được hiển thị trên danh sách công việc in 9002. Trong trường hợp này, người dùng đăng nhập không chỉ có thể in các công việc in của riêng mình mà còn có thể in cả các công việc in mà những người khác đã nhập vào MFP 1000. Tức là theo phương án minh hoạ này, người dùng không phải là người dùng đã nhập công việc cũng có thể đăng nhập vào MFP 1000 và nhận sản phẩm được in của công việc này (tuy nhiên, vì thao tác in đối với công việc in này bị ngăn cấm bằng mật khẩu nên người dùng nhận được công việc in này cần phải biết mật khẩu).

Theo cách khác, ở bước S5004, CPU 205 có thể kiểm tra quyền hạn của

người dùng đăng nhập và xác định xem người dùng đăng nhập này có quyền người quản trị hay không. Nếu người dùng đăng nhập có quyền người quản trị thì các công việc in của tất cả người dùng có thể được hiển thị. Nếu người dùng đăng nhập không có quyền người quản trị thì chỉ có công việc của người dùng đăng nhập này là có thể được hiển thị.

Ở bước S5005, CPU 205 tiếp nhận tên người dùng của người dùng đăng nhập từ RAM 206, và tên người dùng (ID người dùng) của công việc in đang được quản lý ở trạng thái chờ nhập mật khẩu. Khi quy trình đăng nhập hoàn tất thì ngữ cảnh đăng nhập, bao gồm tên người dùng để nhận dạng người dùng đăng nhập, được ghi vào RAM 206. Quy trình đăng nhập này được mô tả dưới đây dựa vào Fig.6. CPU 205 nhận dạng người dùng đăng nhập dựa trên ngữ cảnh đăng nhập được ghi trong RAM 206. Theo đó, ở bước S5005, CPU 205 hiển thị, trên khối vận hành 210, danh sách công việc của các công việc in có mật khẩu vốn bao gồm tên người dùng tương ứng với tên người dùng của người dùng đăng nhập.

Ở bước S5006, CPU 205 hiển thị, trên khối vận hành 210, danh sách tất cả các công việc in có mật khẩu được lưu trong trạng thái chờ nhập mật khẩu trên HDD 208 của MFP 1000.

Fig.9 minh hoạ màn hình ví dụ của danh sách công việc được hiển thị ở bước S5005 hoặc bước S5006. Danh sách công việc in 9002 là danh sách các công việc in có mật khẩu được lưu trong MFP 1000. Tuy nhiên, trong trường hợp danh sách các công việc in được hiển thị ở bước S5005, thì chỉ có công việc in của người dùng đăng nhập mới được hiển thị.

Nút PRINT 9003 được sử dụng để ra lệnh cho MFP 1000 bắt đầu in công việc in được chọn. Nút CANCEL 9004 được sử dụng để huỷ in đối với công việc in được chọn.

Ngoài ra, danh sách công việc in 9002 còn hiển thị trạng thái dấu chọn công

việc in, số thứ tự nhận được, thời điểm nhận được công việc in, tên công việc in, tên người dùng của người đã nhập công việc in (tức chủ sở hữu của công việc in), và trạng thái công việc.

Theo ví dụ được minh hoạ trên Fig.9, có năm công việc in có mật khẩu trong danh sách công việc in 9002. Trong số năm công việc in này, công việc in có mật khẩu với số thứ tự nhận được là 0001 đang được chọn. Ở ví dụ được minh hoạ trên Fig.9, bốn công việc in có mật khẩu không mã hoá, với các số thứ tự nhận được từ 0001 đến 0004, và một công việc in có mật khẩu được mã hoá, với số thứ tự nhận được là 0005, được hiển thị. Biểu tượng mã hoá 9006 biểu thị sự hiện diện của công việc in được mã hoá.

Loại công việc được thể hiện trên danh sách công việc in 9002 chỉ là công việc in có mật khẩu. Tuy nhiên, công việc in bình thường cũng có thể được hiển thị trên màn hình này.

Ở bước S5007, CPU 205 nhận thao tác chọn công việc định in của người dùng. Người dùng chọn công việc định in từ danh sách công việc in 9002 được hiển thị ở bước S5005 hoặc bước S5006. Khi người dùng chọn công việc định in, dấu chọn sẽ được đặt vào hộp đánh dấu chọn 9005 vốn tương ứng với công việc được chọn. Điều này sẽ đặt công việc định in vào trạng thái được chọn. Khi trạng thái của ít nhất một công việc trong số các công việc được liệt kê trên danh sách công việc in 9002 được thay đổi sang trạng thái được chọn, thì nút CANCEL 9004 và nút PRINT 9003 sẽ trở nên có thể được thao tác. Ở bước S5007, CPU 205 tiếp tục nhận thao tác của người dùng đối với nút CANCEL 9004 hoặc nút PRINT 9003 thông qua khối vận hành 210. Ví dụ, nếu người dùng cần in công việc in được chọn thì người dùng sẽ nhấn nút PRINT 9003 để ra lệnh in. Ngược lại, nếu người dùng cần huỷ in đối với công việc in này thì người dùng sẽ nhấn nút CANCEL 9004. Ở bước S5007, CPU 205 xác định xem lệnh nhận được là lệnh in hay lệnh huỷ in. Nếu lệnh nhận được là lệnh in ("IN"

ở bước S5007) thì tiến trình tiến đến bước S5008, trong đó, quy trình in như được minh hoạ trên Fig.7 được thực hiện. Ngược lại, nếu lệnh nhận được là lệnh huỷ ("HUỖ" ở bước S5007) thì tiến trình tiến đến bước S5009, trong đó, quy trình huỷ như được minh hoạ trên Fig.8 được thực hiện.

Các thao tác được thực hiện khi người dùng đăng nhập vào MFP 1000 và sử dụng chức năng in dành riêng đã được mô tả.

Tiếp theo, quy trình đăng nhập vốn được thực hiện khi người dùng đăng nhập vào MFP 1000 ở bước S5002, quy trình in đối với công việc in có mật khẩu ở bước S5008, và quy trình huỷ in ở bước S5009 của lưu đồ được minh hoạ trên Fig.5, sẽ được mô tả chi tiết lần lượt dựa vào Fig.6, Fig.7 và Fig.8.

Fig.6 là lưu đồ chi tiết minh hoạ quy trình đăng nhập được thực hiện ở bước S5002 vốn đã được minh hoạ trên Fig.5.

Ở bước S6001, CPU 205 hiển thị màn hình đăng nhập trên khối vận hành 210.

Fig.13 là sơ đồ minh hoạ ví dụ của màn hình đăng nhập được hiển thị ở bước S6001. Màn hình ví dụ này được hiển thị khi người dùng đăng nhập vào MFP 1000 theo phương pháp xác thực bản phím. Các thông báo, trường nhập tên người dùng 1301, trường nhập mật khẩu 1302, nút LOGIN (nút đăng nhập) 1303 và nút Guest LOGIN (nút đăng nhập khách) 1304 được hiển thị trên màn hình đăng nhập này.

Người dùng có thể đăng nhập vào MFP 1000 dưới dạng người dùng đăng nhập. Trong trường hợp này, người dùng nhập tên người dùng và mật khẩu lần lượt vào trường nhập tên người dùng 1301 và trường nhập mật khẩu 1302. Sau đó, người dùng nhấn nút LOGIN 1303. Ngược lại, người dùng cũng có thể đăng nhập vào MFP 1000 dưới dạng người dùng khách. Trong trường hợp này, người dùng khách nhấn nút Guest LOGIN 1304 mà không cần nhập tên người dùng và mật khẩu. Theo cách khác, một chuỗi kí tự đơn giản, chẳng hạn "guest" cũng có

thể được nhập vào làm thông tin xác thực nếu người dùng khách đăng nhập vào MFP 1000.

Ở bước S6002, CPU 205 kiểm tra xem nút LOGIN 1303 được nhấn hay nút Guest LOGIN 1304 được nhấn, để xác định xem người dùng đăng nhập vào MFP 1000 dưới dạng người dùng đăng nhập hay người dùng khách. Nếu CPU 205 xác định được rằng người dùng đăng nhập vào MFP 1000 dưới dạng người dùng khách ("CÓ" ở bước S6002) thì tiến trình tiến đến bước S6005. Nếu CPU 205 xác định được rằng người dùng không đăng nhập vào MFP 1000 dưới dạng người dùng khách ("KHÔNG" ở bước S6002) thì tiến trình tiến đến bước S6003.

Ở bước S6003, CPU 205 tiếp nhận thông tin xác thực nhận được qua màn hình đăng nhập ở bước S6002. Thông tin xác thực tiếp nhận được này được ghi vào RAM 206 thông qua giao diện khối vận hành 209.

Ở bước S6004, CPU 205 thực hiện việc xác thực người dùng dựa trên thông tin xác thực tiếp nhận được ở bước S6002. Việc xác thực người dùng có thể được thực hiện bởi MFP 1000 hoặc máy chủ xác thực ngoài trên mạng, chẳng hạn máy chủ dịch vụ thư mục và máy chủ LDAP (Lightweight Directory Access Protocol - giao thức truy cập nhanh các dịch vụ thư mục). Nếu MFP 1000 thực hiện việc xác thực người dùng thì nó sẽ đối chiếu tên người dùng và mật khẩu được nhập với cơ sở dữ liệu xác thực được lưu trên HDD 208. Nếu máy chủ xác thực ngoài thực hiện việc xác thực người dùng, thì CPU 205 sẽ gửi yêu cầu xác thực, bao gồm thông tin xác thực tiếp nhận được, đến máy chủ xác thực ngoài, và nhận kết quả xác thực từ máy chủ xác thực này. Kết quả nhận được sẽ cho biết việc xác thực người dùng có thành công hay không.

Việc xác thực người dùng có thể được thực hiện bằng các phương pháp xác thực khác, chẳng hạn xác thực dấu vân tay, xác thực khuôn mặt, và xác thực người dùng bằng thẻ IC (Integrated Circuit - mạch tích hợp).

Nếu CPU 205 xác định được rằng việc xác thực người dùng là thành công

("CÓ" ở bước S6004), thì ở bước S6005, CPU 205 cho phép người dùng đăng nhập vào MFP 1000, và lưu ngữ cảnh đăng nhập, gồm tên người dùng tiếp nhận được ở bước S6003, vào RAM 206. Sau đó, tiến trình kết thúc. Ngữ cảnh đăng nhập này bao gồm các thông tin chẳng hạn như thời điểm đăng nhập và ngày hết hạn, ngoài tên người dùng ra. Nếu người dùng đăng nhập vào MFP 1000 dưới dạng người dùng khách, thì CPU 205 lưu thông tin biểu thị người dùng khách này vào RAM 206.

Nếu CPU 205 xác định được rằng việc xác thực người dùng là không thành công ("KHÔNG" ở bước S6004), thì CPU 205 hiển thị thông báo lỗi trên khối vận hành 210, và không cho phép người dùng sử dụng MFP 1000. Sau đó, tiến trình quay trở về bước S6001.

Quy trình đăng nhập đã được mô tả chi tiết.

Fig.7 là lưu đồ minh họa quy trình chính của phương án minh họa này. Lưu đồ này tương ứng với quy trình in ở bước S5008 đã được minh họa trên Fig.5.

Ở bước S7001, CPU 205 tiếp nhận thiết lập bỏ nhập mật khẩu (xem Fig.10) của MFP 1000 từ SRAM 213, và xác định chế độ hoạt động của MFP 1000. Cụ thể là, nếu thiết lập bỏ nhập mật khẩu tiếp nhận được từ SRAM 213 là có hiệu lực ("CÓ" ở bước S7001), thì CPU 205 xác định được rằng MFP 1000 đang được vận hành trong chế độ mà trong đó người dùng có thể bỏ nhập mật khẩu (dưới đây được gọi là "chế độ bỏ nhập mật khẩu"). Sau đó, tiến trình tiến đến bước S7002. Ngược lại, nếu giá trị thiết lập tiếp nhận được từ SRAM 213 là không có hiệu lực ("KHÔNG" ở bước S7001), thì CPU 205 xác định được rằng MFP 1000 đang được vận hành trong chế độ mà trong đó người dùng cần phải nhập mật khẩu (dưới đây được gọi là "chế độ cần nhập mật khẩu"). Sau đó, tiến trình tiến đến bước S7008.

Fig.10 là sơ đồ minh họa màn hình thiết lập 10001 được sử dụng để đặt thiết lập bỏ nhập mật khẩu. Màn hình thiết lập 10001 này được CPU 205 hiển thị trên

khởi vận hành 210. Khi người quản trị hệ thống chọn nút VALID 10002 hoặc nút INVALID 10003 trên màn hình thiết lập 10001 rồi nhấn nút OK 10004, thì CPU 205 sẽ ghi giá trị thiết lập, vốn cho biết việc cho phép hoặc vô hiệu hoá việc nhập mật khẩu, vào SRAM 213.

Ở bước S7002, CPU 205 tiếp nhận, từ HDD 208, cờ mã hoá của công việc in có mật khẩu đã được ra lệnh in. Ở bước S7003, CPU 205 xác định xem cờ mã hoá của công việc in có mật khẩu đã được ra lệnh in là có hiệu lực (tức là dữ liệu in đã được mã hoá) hay không.

Nếu CPU 205 xác định được rằng dữ liệu in có được mã hoá ("CÓ" ở bước S7003), thì dữ liệu in này sẽ không thể được giải mã nếu không nhận được mật khẩu từ người dùng, ngay cả khi MFP 1000 đang được vận hành trong chế độ bỏ nhập mật khẩu. Theo đó, tiến trình tiến đến bước S7008. Ở bước S7008, CPU 205 hiển thị màn hình nhập mật khẩu để nhận mật khẩu từ người dùng. Ngược lại, nếu dữ liệu in không được mã hoá ("KHÔNG" ở bước S7003), thì tiến trình tiến đến bước S7004.

Ở bước S7004, CPU 205 tiếp nhận giá trị thiết lập của MFP 1000 từ SRAM 213 và xác định xem việc xác thực người dùng đã được thực hiện hay chưa. Ở đây, CPU 205 thực hiện thao tác xác định này bằng cách dựa vào giá trị thiết lập được sử dụng trong tiến trình ở bước S5001, vốn đã được minh hoạ trên Fig.5. Tức là nếu giá trị thiết lập tiếp nhận được từ SRAM 213 cho thấy rằng việc xác thực người dùng là cần thiết, thì thao tác xác thực người dùng là đã được thực hiện ở bước S5002. Do đó, CPU 205 xác định rằng việc xác thực người dùng là đã được thực hiện ("RỒI" ở bước S7004). Sau đó, tiến trình tiến đến bước S7005. Ngược lại, nếu giá trị thiết lập tiếp nhận được từ SRAM 213 cho thấy rằng việc xác thực người dùng là không cần thiết thì CPU 205 xác định rằng việc xác thực người dùng là chưa được thực hiện ("CHƯA" ở bước S7004). Sau đó, tiến trình tiến đến bước S7008.

Ở bước S7005, CPU 205 tiếp nhận ngữ cảnh đăng nhập được chứa trong RAM 206, và kiểm tra quyền hạn của người dùng đăng nhập.

Theo phương án minh hoạ này, có ba loại quyền hạn người dùng đăng nhập là: quyền hạn người quản trị, quyền hạn người dùng bình thường, và quyền hạn người dùng khách. Tuy nhiên, các quyền hạn này chỉ là các ví dụ. Các quyền hạn này được ứng dụng quản lý việc xác thực người dùng của MFP 1000 đăng kí trước.

Người dùng mà có quyền người quản trị thì có thể sử dụng thiết lập quản trị của MFP 1000. Theo phương án minh hoạ này, chỉ có người dùng có quyền người quản trị mới có thể đặt thiết lập bỏ nhập mật khẩu và thiết lập để xem có thực hiện việc xác thực người dùng hay không. Người dùng mà có quyền hạn người dùng bình thường thì có thể sử dụng các mục không phải là thiết lập quản trị và các chức năng khác nhau của MFP 1000. Người dùng khách thì có thể sử dụng một số lượng giới hạn trong số các chức năng và các thiết lập của MFP 1000. Số lượng các mục mà người dùng khách có thể sử dụng được là ít hơn so với người dùng bình thường, và các mục mà người dùng khách có thể sử dụng được thì có các dấu hiệu như sau. Cụ thể là, nếu người dùng đăng nhập vào MFP 1000 dưới dạng người dùng khách, thì người dùng này sẽ chỉ được MFP 1000 coi là người dùng khách mà thôi, bất kể người dùng này là ai. Do đó, ngay cả khi người dùng mà có quyền hạn người dùng khách đăng nhập vào MFP 1000 thì MFP 1000 cũng không thể nhận dạng được từng người.

Phần mô tả này lại dựa vào Fig.7. Nếu CPU 205 xác định được rằng người dùng đăng nhập là có quyền hạn người dùng khách ("CÓ" ở bước S7005), thì tiến trình tiến đến bước S7008. Nếu CPU 205 xác định được rằng người dùng đăng nhập là có quyền hạn khác (tức quyền hạn người quản trị hoặc quyền hạn người dùng bình thường) ("KHÔNG" ở bước S7005), thì tiến trình tiến đến bước S7006.

Ở bước S7006, CPU 205 kiểm tra xem tên người dùng của công việc in được chọn ở bước S5007 có khớp với tên người dùng của người dùng đăng nhập hay không, và xác định xem công việc in đã được ra lệnh in có phải là của người dùng đăng nhập này hay không. Nếu tên người dùng của công việc in này không khớp với tên người dùng của người dùng đăng nhập ("KHÔNG" ở bước S7006), thì tiến trình tiến đến bước S7008. Ở bước S7008, CPU 205 hiển thị màn hình nhập mật khẩu (không được minh họa trên hình vẽ) trên khối vận hành 210 để nhận mật khẩu từ người dùng.

Nếu tên người dùng của công việc in này khớp với tên người dùng của người dùng đăng nhập ("CÓ" ở bước S7006), thì ở bước S7007, MFP 1000 in công việc in này mà không cần nhận mật khẩu từ người dùng. Tức là nếu thiết lập bỏ nhập mật khẩu là có hiệu lực thì MFP 1000 có thể thực hiện thao tác in mà không cần nhận mật khẩu, miễn là công việc in có mật khẩu này thuộc về người dùng đăng nhập (tức là chủ sở hữu của công việc in này là người dùng đăng nhập này). Điều này có thể cho phép người dùng đăng nhập đỡ mất công nhập mật khẩu khi in công việc in có mật khẩu của chính mình.

Trong quy trình nêu trên, nếu thiết lập bỏ nhập mật khẩu là có hiệu lực, và người dùng đăng nhập là người dùng khách, thì MFP 1000 sẽ luôn luôn đòi người dùng phải nhập mật khẩu khi in. Do MFP 1000 không thể nhận dạng được từng người dùng khách riêng rẽ nên MFP 1000 sẽ không thể xác định được công việc in của người dùng khách này trong số các công việc in có mật khẩu. Do đó, khi nhận được lệnh in đối với công việc in có mật khẩu từ người dùng khách, thì MFP 1000 sẽ luôn đòi người dùng nhập mật khẩu ngay cả khi thiết lập bỏ nhập mật khẩu là có hiệu lực.

Ở bước S7009, CPU 205 so sánh mật khẩu nhận được từ người dùng qua khối khối vận hành 210 với mật khẩu của công việc in có mật khẩu, và xác định xem các mật khẩu này có khớp nhau không. Nếu các mật khẩu này là khớp nhau

("CÓ" ở bước S7009) thì tiến trình tiến đến bước S7010.

Nếu CPU 205 xác định được rằng các mật khẩu này không khớp nhau ("KHÔNG" ở bước S7009), thì ở bước S7011, CPU 205 hiển thị màn hình báo lỗi trên khối vận hành 210. Ở đây, màn hình báo lỗi biểu thị rằng mật khẩu nhận được từ người dùng là không khớp với mật khẩu của công việc in có mật khẩu.

Ở bước S7010, CPU 205 tiếp nhận cờ mã hoá của công việc in có mật khẩu, và xác định xem công việc được ra lệnh in có phải là công việc in được mã hoá có mật khẩu hay không. Nếu công việc được ra lệnh in này không phải là công việc in được mã hoá có mật khẩu ("KHÔNG" ở bước S7010), thì ở bước S7007, MFP 1000 in công việc in có mật khẩu này.

Nếu công việc được ra lệnh in này là công việc in được mã hoá có mật khẩu ("CÓ" ở bước S7010) thì tiến trình tiến đến bước S7012. Ở bước S7012, CPU 205 giải mã dữ liệu in đã mã hoá nhờ sử dụng mật khẩu nhận được ở bước S7008, và xuất dữ liệu in đã được giải mã đến khối RIP 218. Khối RIP 218 mã hoá dữ liệu in đã được giải mã này thành ảnh nhị phân. Sau đó, ở bước S7007, máy in 202 của MFP 1000 in ảnh lên giấy in dựa trên dữ liệu ảnh nhị phân được xuất ra từ khối RIP 218.

Các thao tác của quy trình in đã được mô tả dựa vào Fig.7. Theo phương án minh họa này, ngay cả khi người dùng không thể bỏ nhập mật khẩu đối với công việc in có mật khẩu, thì công việc in có mật khẩu này vẫn có thể được in bằng cách nhập mật khẩu theo cách thông thường. Quy trình này cho phép người dùng ra lệnh cho MFP 1000 in ngay cả công việc in có mật khẩu của người dùng khác, bằng cách nhập vào mật khẩu trong trường hợp mà chức năng bỏ nhập mật khẩu là có hiệu lực và thiết lập sàng lọc danh sách công việc là không có hiệu lực ở MFP 1000. Do đó, khả năng sử dụng MFP 1000 có thể được tăng cường.

Tiếp theo, quy trình huỷ công việc in có mật khẩu sẽ được mô tả dựa vào lưu đồ được minh họa trên Fig.8.

Lưu đồ trên Fig.8 minh hoạ quy trình huỷ ở bước S5009 đã được minh hoạ trên Fig.5.

Ở bước S8001, CPU 205 tiếp nhận thiết lập của MFP 1000 từ SRAM 213 và xác định xem việc xác thực người dùng đã được thực hiện hay chưa. Nếu việc xác thực người dùng chưa được thực hiện ("CHƯA" ở bước S8001), thì ở bước S8004, CPU 205 xoá dữ liệu của công việc in có mật khẩu đã được lệnh huỷ khỏi HDD 208. Nếu việc xác thực người dùng đã được thực hiện ("RỒI" ở bước S8001), thì ở bước S8002, CPU 205 tiếp nhận tên người dùng của công việc in có mật khẩu đã được lệnh huỷ và tên người dùng của người dùng đăng nhập.

Sau đó, ở bước S8003, CPU 205 xác định xem tên người dùng của công việc in có mật khẩu đã được lệnh huỷ có khớp với tên người dùng của người dùng đăng nhập hay không. Nếu tên người dùng của công việc in có mật khẩu đã được lệnh huỷ này khớp với tên người dùng của người dùng đăng nhập ("CÓ" ở bước S8003), thì ở bước S8004, CPU 205 xoá dữ liệu của công việc in có mật khẩu đã được lệnh huỷ này khỏi HDD 208. Sau đó, tiến trình tiến đến bước S8005.

Ở bước S8005, CPU 205 xoá công việc in có mật khẩu đã được chọn để huỷ khỏi danh sách công việc in 9002 vốn được hiển thị trên khối vận hành 210. Sau đó, quy trình huỷ công việc in trên Fig.8 kết thúc.

Nếu tên người dùng của công việc in có mật khẩu đã được lệnh huỷ nêu trên không khớp với tên người dùng của người dùng đăng nhập ("KHÔNG" ở bước S8003) thì CPU 205 hiển thị màn hình báo lỗi trên khối vận hành 210. Màn hình báo lỗi này cho biết rằng việc thực hiện công việc in được chọn là không thể huỷ được. Sau đó, quy trình huỷ công việc in trên Fig.8 kết thúc.

Phương án minh hoạ thứ nhất đã được mô tả. Theo phương án minh hoạ thứ nhất này, trong trường hợp mà người dùng đăng nhập ra lệnh cho MFP 1000 in công việc in có mật khẩu, thì CPU 205 sẽ điều khiển MFP 1000 sao cho thao tác

in có thể được bắt đầu mà không cần nhập mật khẩu của công việc in.

Ngoài ra, theo phương án minh hoạ thứ nhất, CPU 205 điều khiển MFP 1000 sao cho người dùng chưa đăng nhập cũng có thể ra lệnh cho MFP 1000 in công việc in dành riêng (tuy nhiên, trong trường hợp người dùng chưa đăng nhập này ra lệnh thực thi công việc, thì CPU 205 sẽ điều khiển MFP 1000 sao cho thao tác in chỉ có thể được bắt đầu sau khi người dùng chưa đăng nhập này đã được yêu cầu nhập mật khẩu). Phương pháp điều khiển này cho phép giảm công sức nhập mật khẩu cho người dùng, và cho phép MFP 1000 thực hiện thao tác in bằng cách xác thực người dùng một lần tại thời điểm đăng nhập của người dùng. Ngoài ra, người dùng chưa đăng nhập cũng có thể cho phép MFP 1000 bắt đầu in công việc in dành riêng với điều kiện là người dùng chưa đăng nhập phải nhập mật khẩu. Do đó, khả năng sử dụng MFP có thể được tăng cường.

Ngoài ra, theo phương án minh hoạ thứ nhất, trong trường hợp MFP 1000 nhận được lệnh in mà không xác thực người dùng, thì CPU 205 sẽ luôn đòi nhập mật khẩu. Điều này có thể duy trì được tính bảo mật.

Ngoài ra, theo phương án minh hoạ thứ nhất, người dùng đăng nhập của MFP 1000 có thể cho phép in công việc in có mật khẩu của người khác (chỉ khi người dùng đăng nhập đã biết mật khẩu của công việc in này). Điều này có thể tăng cường khả năng sử dụng MFP.

Tiếp theo, phương án minh hoạ thứ hai sẽ được mô tả. Theo phương án minh hoạ thứ nhất, MFP chỉ có thể huỷ công việc in có mật khẩu của người dùng đăng nhập theo quy trình huỷ công việc in có mật khẩu (xem Fig.8). Theo phương án minh hoạ thứ hai, MFP 1000 có thể huỷ công việc in có mật khẩu của người dùng không phải là người dùng đăng nhập nếu đúng mật khẩu được nhập vào, để tiếp tục tăng cường khả năng sử dụng. Chức năng này được gọi là chức năng nhập mật khẩu trong trường hợp huỷ, theo phương án minh hoạ thứ hai.

Phương án minh hoạ thứ hai sẽ được mô tả bằng cách sử dụng trường hợp

mà MFP 1000, vốn có chức năng nhập mật khẩu trong trường hợp huỷ, được điều khiển khi người dùng đăng nhập ra lệnh huỷ công việc in có mật khẩu của chính mình hoặc của người khác. Trong trường hợp này, thao tác huỷ được ra lệnh theo sự có mặt hay vắng mặt của chức năng quản lý xác thực người dùng và điều kiện vai trò của người dùng đăng nhập.

Việc MFP 1000 điều khiển quy trình huỷ công việc in có mật khẩu sẽ được mô tả chi tiết dựa vào Fig.11 và Fig.12. Theo phương án minh hoạ này, cấu hình của MFP 1000, quy trình truyền công việc in có mật khẩu của trình điều khiển máy in, quy trình đăng nhập của MFP 1000, quy trình in công việc in có mật khẩu, và quy trình nhận công việc in, là tương tự như đã được mô tả ở phương án minh hoạ thứ nhất, nên chúng sẽ không được mô tả nữa.

Quy trình được minh hoạ trên Fig.11 của phương án minh hoạ thứ hai có thêm các bước từ S11006 đến S11015 so với quy trình được minh hoạ trên Fig.8 của phương án minh hoạ thứ nhất. Các bước thêm này liên quan đến việc điều khiển được thực hiện khi thiết lập mật khẩu trong trường hợp huỷ là có hiệu lực. Các bước từ S11006 đến S11015 này sẽ được mô tả chi tiết dưới đây. Trên lưu đồ được minh hoạ trên Fig.11 của phương án minh hoạ này, tiến trình từ bước S11001 đến S11005 là tương tự như tiến trình từ bước S8001 đến S8005 của lưu đồ trên Fig.8 của phương án minh hoạ thứ nhất. Ngoài ra, quy trình in dành riêng, quy trình đăng nhập và quy trình in của phương án minh hoạ này là tương tự như quy trình tương ứng trên Fig.5, Fig.6 và Fig.7 của phương án minh hoạ thứ nhất.

Phương án minh hoạ thứ hai sẽ được mô tả với những điểm khác biệt giữa quy trình của phương án minh hoạ thứ nhất và quy trình của phương án minh hoạ thứ hai.

Ở bước S11006, CPU 205 tiếp nhận thiết lập nhập mật khẩu, trong trường hợp huỷ được thiết lập đối với MFP 1000, từ SRAM 213, và xác định xem thiết

lập nhập mật khẩu tiếp nhận được trong trường hợp huỷ là có có hiệu lực hay không.

Fig.12 minh hoạ màn hình thiết lập chức năng in dành riêng có mật khẩu 12001 theo phương án minh hoạ thứ hai. Màn hình thiết lập 12001 này được hiển thị trên khối vận hành 210. Thiết lập bỏ nhập mật khẩu và thiết lập nhập mật khẩu trong trường hợp huỷ có thể được thiết lập trên màn hình thiết lập 12001 này. Thiết lập bỏ nhập mật khẩu trên Fig.12 là tương tự như đã được minh hoạ trên Fig.10 của phương án minh hoạ thứ nhất. Màn hình thiết lập 12001 trên Fig.12 có thêm thiết lập của chức năng nhập mật khẩu trong trường hợp huỷ so với màn hình thiết lập trên Fig.10. Cái này được gọi là “thiết lập nhập mật khẩu trong trường hợp huỷ” theo phương án minh hoạ này. Thiết lập nhập mật khẩu trong trường hợp huỷ trên Fig.12 sẽ được mô tả.

Thiết lập nhập mật khẩu trong trường hợp huỷ được thiết lập bằng cách sử dụng nút VALID 12006 và nút INVALID 12007 trên màn hình thiết lập 12001. Nút VALID 12006 được sử dụng để cho phép thiết lập nhập mật khẩu trong trường hợp huỷ, còn nút INVALID 12007 được sử dụng để vô hiệu hoá thiết lập nhập mật khẩu trong trường hợp huỷ. Người dùng chọn nút VALID 12006 hoặc nút INVALID 12007 nhờ sử dụng khối vận hành 210. Thiết lập nhập mật khẩu trong trường hợp huỷ bao gồm tùy chọn nút VALID 12006 và nút INVALID 12007. Sự thay đổi thiết lập nhập mật khẩu trong trường hợp huỷ được CPU 205 lưu vào SRAM 213 khi nút thiết lập 12004 của chức năng in dành riêng có mật khẩu được chọn.

Phần mô tả này lại dựa vào quy trình được minh hoạ trên Fig.11. Nếu CPU 205 xác định được rằng thiết lập nhập mật khẩu trong trường hợp huỷ là không có hiệu lực ("KHÔNG" ở bước S11006) thì tiến trình tiến đến bước S11001. Nếu CPU 205 xác định được rằng thiết lập nhập mật khẩu trong trường hợp huỷ là có hiệu lực ("CÓ" ở bước S11006) thì tiến trình tiến đến bước S11007.

Ở bước S11007, CPU 205 tiếp nhận thiết lập của MFP 1000 từ SRAM 213, và xác định xem MFP 1000 có quản lý việc xác thực người dùng hay không. Nếu CPU 205 xác định được rằng MFP 1000 không quản lý việc xác thực người dùng ("CHƯA" ở bước S11007) thì tiến trình tiến đến bước S11011. Ở bước S11011, CPU 205 hiển thị màn hình nhập mật khẩu trên khối vận hành 210 và nhận mật khẩu được nhập từ người dùng. Sau đó, tiến trình tiến đến bước S11012.

Ở bước S11012, CPU 205 tiếp nhận mật khẩu từ công việc in có mật khẩu đã được lệnh huỷ. Sau đó, tiến trình tiến đến bước S11013.

Ở bước S11013, CPU 205 so sánh mật khẩu được nhập từ người dùng qua khối vận hành 210 với mật khẩu tiếp nhận được của công việc in có mật khẩu. Sau đó, tiến trình tiến đến bước S11014.

Ở bước S11014, CPU 205 xác định xem mật khẩu mà người dùng nhập vào có khớp với mật khẩu của công việc in có mật khẩu hay không. Nếu hai mật khẩu này khớp nhau ("CÓ" ở bước S11014), thì ở bước S11004, CPU 205 huỷ công việc in có mật khẩu đã được lệnh huỷ. Sau đó, tiến trình tiến đến bước S11005.

Nếu CPU 205 xác định được rằng mật khẩu mà người dùng nhập vào không khớp với mật khẩu của công việc in có mật khẩu ("KHÔNG" ở bước S11014), thì ở bước S11015, CPU 205 hiển thị màn hình thông tin (không được minh hoạ) thông báo rằng hai mật khẩu này là không khớp nhau. Sau đó, CPU 205 kết thúc quy trình huỷ công việc in có mật khẩu này.

Nếu CPU 205 xác định được rằng MFP 1000 có quản lý việc xác thực người dùng ("RỒI" ở bước S11007) thì tiến trình tiến đến bước S11008.

Ở bước S11008, CPU 205 tiếp nhận vai trò của người dùng đăng nhập vào MFP 1000 và xác định vai trò của người dùng đăng nhập này. Nếu CPU 205 xác định được rằng người dùng đăng nhập là người dùng bình thường ("người dùng

bình thường" ở bước S11008), thì ở bước S11009, CPU 205 tiếp nhận thông tin người dùng của công việc in có mật khẩu đã được lệnh huỷ và thông tin người dùng của người dùng đăng nhập này.

Sau đó, ở bước S11010, CPU 205 xác định xem thông tin người dùng của công việc in có mật khẩu đã được lệnh huỷ có khớp với thông tin người dùng của người dùng đăng nhập hay không. Nếu CPU 205 xác định được rằng thông tin người dùng của công việc in có mật khẩu đã được lệnh huỷ là khớp với thông tin người dùng của người dùng đăng nhập ("CÓ" ở bước S11010), thì ở bước S11004, CPU 205 huỷ công việc in có mật khẩu đã được lệnh huỷ này. Sau đó, tiến trình tiến đến bước S11005.

Do đó, theo quy trình này, nếu thiết lập nhập mật khẩu trong trường hợp huỷ là có hiệu lực và việc xác thực người dùng là được thực hiện ở MFP 1000, thì người dùng đăng nhập có thể ra lệnh huỷ công việc in có mật khẩu của mình mà không cần phải nhập mật khẩu. Điều này có thể giảm công sức xác thực cho người dùng đăng nhập khi người dùng đăng nhập huỷ công việc in có mật khẩu của mình, giảm công sức cho MFP 1000 khi thiết lập nhập mật khẩu trong trường hợp huỷ là có hiệu lực.

Nếu CPU 205 xác định được rằng người dùng đăng nhập là người quản trị ("người quản trị" ở bước S11008), thì ở bước S11004, CPU 205 huỷ công việc in có mật khẩu đã được lệnh huỷ nêu trên. Sau đó, tiến trình tiến đến bước S11005.

Theo quy trình này, nếu người dùng đăng nhập có vai trò người quản trị đối với MFP 1000 mà trong đó thiết lập nhập mật khẩu trong trường hợp huỷ là có hiệu lực, thì MFP 1000 sẽ huỷ in đối với công việc in có mật khẩu mà không cần nhập mật khẩu. Trong trường hợp này, MFP 1000 sẽ huỷ cả công việc in có mật khẩu không phải của người dùng đăng nhập. Đây là trường hợp theo phương án minh họa này, vì người dùng đăng nhập có vai trò như người quản trị được

mong muốn là sẽ xoá bỏ các công việc in của những người khác khỏi MFP 1000 khi các công việc in này không còn được cần đến nữa, xét về mặt quản lý MFP. Do đó, người dùng đăng nhập có vai trò như người quản trị có thể xoá bỏ bất kì công việc in có mật khẩu nào.

Nếu người dùng đăng nhập được xác định là người dùng khách ("người dùng khách" ở bước S11008), thì tiến trình tiến đến bước S11011. Ở bước S11011, CPU 205 hiển thị màn hình nhập mật khẩu trên khối vận hành 210 và nhận mật khẩu từ người dùng.

Theo quy trình này, nếu người dùng đăng nhập là người dùng khách đối với MFP 1000 mà trong đó thiết lập nhập mật khẩu trong trường hợp huỷ là có hiệu lực, thì MFP 1000 sẽ luôn yêu cầu người dùng khách nhập mật khẩu trong trường hợp huỷ. Do MFP 1000 không thể nhận dạng được từng người dùng khách riêng rẽ nên MFP 1000 sẽ không thể xác định được công việc in của người dùng khách này trong số các công việc in có mật khẩu. Do đó, ngay cả khi thiết lập nhập mật khẩu trong trường hợp huỷ là có hiệu lực, thì MFP 1000 cũng luôn luôn yêu cầu người dùng khách nhập vào mật khẩu. MFP 1000 đưa ra yêu cầu này khi nhận được lệnh huỷ đối với công việc in có mật khẩu từ người dùng khách.

Phương án minh hoạ thứ hai đã được mô tả. Theo phương án minh hoạ thứ hai, thì công việc xác thực với việc nhập mật khẩu sẽ được giảm bớt đối với MFP 1000 mà trong đó thiết lập nhập mật khẩu trong trường hợp huỷ là có hiệu lực. Điều này có thể giảm công sức cho người dùng khi in công việc in có mật khẩu.

Theo phương án minh hoạ thứ nhất, người quản trị hệ thống sẽ xác định thiết lập bỏ nhập mật khẩu thông qua màn hình được minh hoạ trên Fig.10. Tuy nhiên, thiết lập bỏ nhập mật khẩu này có thể được xác định một cách tự động theo thiết lập xác thực người dùng. Ví dụ, nếu thiết lập xác thực người dùng là không có

hiệu lực, thì MFP 1000 có thể được vận hành một cách ép buộc trong chế độ cần nhập mật khẩu bằng cách làm cho nút VALID 10002 trên màn hình thiết lập 10001 trên Fig.10 không thể chọn được (ví dụ, nút VALID 10002 được hiển thị theo cách bị chìm xuống). Trong trường hợp này, CPU 205 xác định xem có thực hiện việc xác thực người dùng hay không, bằng cách dựa vào giá trị thiết lập được chứa trong SRAM 213. Nếu CPU 205 xác định được rằng việc xác thực người dùng là không cần thiết thì CPU 205 sẽ tự động vô hiệu hoá thiết lập bỏ nhập mật khẩu. Theo đó, điều này có thể giảm bớt công việc thiết lập cho người quản trị hệ thống.

Việc xác thực người dùng có thể không phải lúc nào cũng được thực hiện tại thời điểm đăng nhập của người dùng. Ví dụ, trong trường hợp mà MFP có các chức năng chẳng hạn như sao chép, quét và in, thì sự cần thiết đối với việc xác thực người dùng có thể được thiết lập riêng rẽ theo các chức năng (điều này được gọi là xác thực theo chức năng). Nếu MFP có thể thực hiện việc xác thực theo chức năng này thì việc xác thực người dùng có thể được thực hiện khi cần sử dụng chức năng in. Trong trường hợp này, thiết lập bỏ nhập mật khẩu có thể được kích hoạt một cách tự động.

Theo phương án minh họa này, việc bỏ nhập mật khẩu được xác định tùy theo việc công việc in có mật khẩu định in có phải là của người dùng đăng nhập hay không. Tuy nhiên, việc bỏ nhập mật khẩu cũng có thể được xác định bằng các phương pháp khác. Ví dụ, việc bỏ nhập mật khẩu có thể được xác định tùy theo việc người dùng có phải là người dùng đăng nhập với quyền hạn người quản trị hay không. Trong trường hợp này, việc nhập mật khẩu sẽ được lược bỏ nếu người dùng có quyền hạn người quản trị, còn việc nhập mật khẩu sẽ là bắt buộc nếu người dùng là người dùng bình thường hoặc người dùng khách.

Theo cách khác, việc nhập mật khẩu cũng có thể được lược bỏ đối với những người dùng trong một nhóm (hoặc một phòng ban) nào đó của người

dùng đăng nhập. Ví dụ, MFP tiếp nhận ID nhóm (ID phòng ban) của người dùng đăng nhập và ID nhóm được xác định từ tên người dùng trong công việc định in. Nếu hai ID này khớp nhau thì việc nhập mật khẩu có thể được lược bỏ.

Theo phương án minh hoạ này, khi cần in thì người dùng nhập vào mật khẩu sau khi chọn một công việc. Tuy nhiên, người dùng cũng có thể nhập vào mật khẩu trước khi chọn công việc này. Trong trường hợp này, MFP có thể nhận mật khẩu mà người dùng nhập vào, và xác định công việc in bao gồm mật khẩu nhận được. Sau đó, MFP có thể in công việc in xác định được này. Tức là MFP có thể tự động xác định và in một hoặc nhiều công việc in mà có mật khẩu khớp với mật khẩu được nhập, để người dùng không cần phải chọn công việc in. Ngoài ra, MFP cũng có thể tự động xác định và in chỉ công việc in của người dùng đăng nhập và có mật khẩu khớp với mật khẩu được nhập mà thôi.

Ngoài ra, sự cần thiết đối với việc xác thực người dùng và việc cho phép thiết lập bỏ nhập mật khẩu là có thể được xác định một cách có lựa chọn. Ví dụ, nếu MFP được thiết lập là thực hiện việc xác thực người dùng thì thiết lập bỏ nhập mật khẩu có thể bị vô hiệu hoá một cách tự động. Ngược lại, nếu MFP được thiết lập là không thực hiện việc xác thực người dùng thì thiết lập bỏ nhập mật khẩu có thể được kích hoạt một cách tự động. Ngoài ra, các thiết lập bỏ nhập mật khẩu và các thiết lập xác thực người dùng là có thể được thay đổi theo lệnh của người quản trị hệ thống.

Theo phương án minh hoạ này, MFP nhận mật khẩu từ người dùng nếu người dùng đăng nhập không phải là chủ sở hữu của công việc in, và nhận được lệnh in mà không xác thực người dùng (cả "CHƯA" ở bước S7004 lẫn "KHÔNG" ở bước S7006 trên Fig.7). Tuy nhiên, phương án minh hoạ này bao gồm phương án mà trong đó MFP nhận mật khẩu từ người dùng nếu bất kì một trong hai trường hợp này xảy ra. Nói cách khác, phương án minh hoạ này bao gồm phương án mà trong đó mật khẩu chỉ được nhận từ người dùng nếu nhận

được lệnh in mà không xác thực người dùng, và phương án mà trong đó mật khẩu chỉ được nhận từ người dùng nếu người dùng đăng nhập không phải là chủ sở hữu của công việc in.

Các phương án thực hiện của sáng chế còn có thể được thực hiện bằng máy tính của hệ thống hoặc thiết bị vốn đọc ra và thực thi các lệnh thực thi được bằng máy tính được ghi trên phương tiện lưu trữ (ví dụ, phương tiện lưu trữ bất biến đọc được bằng máy tính) để thực hiện các chức năng của một hoặc nhiều phương án trong số (các) phương án thực hiện nêu trên của sáng chế, và bằng phương pháp được thực hiện bởi máy tính của hệ thống hoặc thiết bị này bằng cách, ví dụ, đọc ra và thực thi các lệnh thực thi được bằng máy tính từ phương tiện lưu trữ để thực hiện các chức năng của một hoặc nhiều phương án trong số (các) phương án thực hiện nêu trên. Máy tính này có thể bao gồm một hoặc nhiều bộ xử lý trung tâm (CPU), bộ vi xử lý (Micro Processing Unit MPU) hoặc hệ mạch khác, và có thể bao gồm mạng các máy tính riêng rẽ hoặc các bộ xử lý máy tính riêng rẽ. Các lệnh thực thi được bằng máy tính nêu trên có thể được cung cấp cho máy tính, ví dụ, từ mạng hoặc phương tiện lưu trữ. Phương tiện lưu trữ nêu trên có thể bao gồm, ví dụ, một hoặc nhiều phương tiện trong số đĩa cứng, bộ nhớ truy cập ngẫu nhiên (RAM), bộ nhớ chỉ đọc (Read Only Memory - ROM), bộ lưu trữ của các hệ thống tính toán phân tán, đĩa quang (chẳng hạn đĩa CD, đĩa DVD hoặc đĩa Blu-ray (BD)TM), thiết bị nhớ flash, thẻ nhớ, và các phương tiện tương tự.

Mặc dù sáng chế đã được mô tả dựa vào các phương án minh họa, nhưng cần hiểu rằng sáng chế không giới hạn ở các phương án minh họa này. Phạm vi của các điểm yêu cầu bảo hộ sau đây bao trùm tất cả các phương án cải biến và các kết cấu, chức năng tương đương.

Yêu cầu bảo hộ

1. Thiết bị tạo ảnh mà sử dụng bộ hiển thị có khả năng hiển thị thông tin và sử dụng bộ tạo ảnh để tạo ảnh trên tấm, thiết bị tạo ảnh này bao gồm:

phương tiện để thu nhận công việc in cụ thể mà liên quan tới người dùng cụ thể và trong đó mật khẩu cụ thể được thiết lập;

phương tiện để hiển thị trên bộ hiển thị màn hình xác nhận có khả năng hiển thị sự nhập thông tin xác nhận người dùng hoặc lệnh bỏ qua sự nhập thông tin xác nhận người dùng;

phương tiện để hiển thị trên bộ hiển thị màn hình danh sách công việc thứ nhất, trên đó chỉ công việc in liên quan tới người dùng cụ thể được thể hiện, dựa trên sự nhập thông tin xác nhận người dùng cho người dùng cụ thể trên màn hình xác nhận, để tiếp nhận sự lựa chọn công việc in cụ thể trên màn hình danh sách công việc thứ nhất, và để làm cho bộ tạo ảnh thực hiện việc tạo ảnh dựa trên công việc in cụ thể theo lệnh in mà không được chủ ý với sự nhập mật khẩu cụ thể bất kỳ; và

phương tiện để hiển thị màn hình danh sách công việc thứ hai, trên đó không chỉ công việc in liên quan tới người dùng cụ thể mà cả công việc in liên quan tới người dùng khác được thể hiện, dựa trên lệnh bỏ qua trên màn hình xác

nhận, để tiếp nhận sự lựa chọn công việc in cụ thể trên màn hình danh sách công việc thứ hai, và để làm cho bộ tạo ảnh thực hiện việc tạo ảnh dựa trên công việc in cụ thể theo lệnh in mà được chú ý với sự nhập mật khẩu cụ thể.

2. Thiết bị tạo ảnh sử dụng bộ hiển thị có khả năng hiển thị thông tin và sử dụng bộ tạo ảnh để tạo ảnh trên tấm, thiết bị tạo ảnh này bao gồm:

phương tiện để thu nhận công việc in cụ thể mà liên quan tới người dùng cụ thể và trong đó mật khẩu cụ thể được thiết lập;

phương tiện để hiển thị trên bộ hiển thị màn hình xác nhận có khả năng hiển thị sự nhập thông tin xác nhận người dùng hoặc lệnh bỏ qua sự nhập thông tin xác nhận người dùng;

phương tiện để hiển thị trên bộ hiển thị màn hình danh sách công việc thứ nhất, trên đó công việc in liên quan tới người dùng cụ thể được thể hiện, dựa trên sự nhập thông tin xác nhận người dùng cho người dùng cụ thể trên màn hình xác nhận và trên đó công việc in liên quan tới người dùng khác với người dùng cụ thể không được thể hiện, để tiếp nhận sự lựa chọn công việc in cụ thể trên màn hình danh sách công việc thứ nhất, và để làm cho bộ tạo ảnh thực hiện

việc tạo ảnh dựa trên công việc in cụ thể theo lệnh in mà không được chú ý với sự nhập mật khẩu cụ thể bất kỳ; và

phương tiện để hiển thị màn hình danh sách công việc thứ hai, trên đó không chỉ công việc in liên quan tới người dùng cụ thể mà cả công việc in liên quan tới người dùng khác được thể hiện, dựa trên lệnh bỏ qua trên màn hình xác nhận, để tiếp nhận sự lựa chọn công việc in cụ thể trên màn hình danh sách công việc thứ hai, và để làm cho bộ tạo ảnh thực hiện việc tạo ảnh dựa trên công việc in cụ thể theo lệnh in mà được chú ý với sự nhập mật khẩu cụ thể.

3. Thiết bị tạo ảnh sử dụng bộ hiển thị có khả năng hiển thị thông tin và sử dụng bộ tạo ảnh tạo ảnh trên tấm, thiết bị tạo ảnh này bao gồm:

phương tiện để thu nhận công việc in cụ thể mà liên quan tới người dùng cụ thể và trong đó mật khẩu cụ thể được thiết lập;

phương tiện để hiển thị trên bộ hiển thị màn hình xác nhận có khả năng chỉ dẫn sự lựa chọn sự nhập thông tin xác nhận người dùng hoặc sự sử dụng của khách;

phương tiện để hiển thị trên bộ hiển thị màn hình danh sách công việc thứ nhất, trên đó chỉ công việc in liên quan tới người dùng cụ thể được thể hiện, dựa

trên sự nhập thông tin xác nhận người dùng cho người dùng cụ thể trên màn hình xác nhận, để tiếp nhận sự lựa chọn công việc in cụ thể trên màn hình danh sách công việc thứ nhất, và để làm cho bộ tạo ảnh thực hiện việc tạo ảnh dựa trên công việc in cụ thể theo lệnh in mà không được chú ý với sự nhập mật khẩu cụ thể bất kỳ; và

phương tiện để hiển thị màn hình danh sách công việc thứ hai, trên đó không chỉ công việc in liên quan tới người dùng cụ thể mà cả công việc in liên quan tới người dùng khác được thể hiện, dựa trên lệnh lựa chọn của sự sử dụng của khách trên màn hình xác nhận, để tiếp nhận sự lựa chọn công việc in cụ thể trên màn hình danh sách công việc thứ hai, và để làm cho bộ tạo ảnh thực hiện việc tạo ảnh dựa trên công việc in cụ thể theo lệnh in mà được chú ý với sự nhập mật khẩu cụ thể.

4. Thiết bị tạo ảnh sử dụng bộ hiển thị có khả năng hiển thị thông tin và sử dụng bộ tạo ảnh để tạo ảnh trên tấm, thiết bị tạo ảnh này bao gồm:

phương tiện để thu nhận công việc in cụ thể mà liên quan tới người dùng cụ thể và trong đó mật khẩu cụ thể được thiết lập;

phương tiện để hiển thị trên bộ hiển thị màn hình xác nhận có khả năng chỉ dẫn lựa chọn sự nhập thông tin xác nhận người dùng hoặc sự sử dụng của khách;

phương tiện để hiển thị trên bộ hiển thị màn hình danh sách công việc thứ nhất, trên đó công việc in liên quan tới người dùng cụ thể được thể hiện, dựa trên sự nhập thông tin xác nhận người dùng cho người dùng cụ thể trên màn hình xác nhận và trên đó công việc in liên quan tới người dùng khác với người dùng cụ thể không được thể hiện, để tiếp nhận sự lựa chọn công việc in cụ thể trên màn hình danh sách công việc thứ nhất, và để làm cho bộ tạo ảnh thực hiện việc tạo ảnh dựa trên công việc in cụ thể theo lệnh in mà không được chủ ý với sự nhập mật khẩu cụ thể bất kỳ; và

phương tiện để hiển thị màn hình danh sách công việc thứ hai, trên đó không chỉ công việc in liên quan tới người dùng cụ thể mà cả công việc in liên quan tới người dùng khác được thể hiện, dựa trên lệnh lựa chọn của sự sử dụng của khách trên màn hình xác nhận, để tiếp nhận sự lựa chọn công việc in cụ thể trên màn hình danh sách công việc thứ hai, và để làm cho bộ tạo ảnh thực hiện việc tạo ảnh dựa trên công việc in cụ thể theo lệnh in mà được chủ ý với sự nhập mật khẩu cụ thể.

5. Thiết bị tạo ảnh theo điểm bất kỳ trong số các điểm từ 1 tới 4, trong đó còn bao gồm phương tiện để thiết lập xem quá trình xác nhận sử dụng thông tin xác nhận người dùng có cần được thực hiện hay không.

6. Thiết bị tạo ảnh theo điểm bất kỳ trong số các điểm từ 1 tới 5, trong đó còn bao gồm phương tiện thiết lập để thiết lập xem sự bỏ qua việc nhập mật khẩu ở thời điểm thực hiện việc in có được cho phép hay không.

7. Thiết bị tạo ảnh theo điểm bất kỳ trong số các điểm từ 1 tới 6, trong đó còn bao gồm phương tiện để thiết lập xem sự bỏ qua việc nhập mật khẩu ở thời điểm dừng việc in có được cho phép hay không.

8. Thiết bị tạo ảnh theo điểm 6 hoặc 7, trong đó phương tiện thiết lập không chấp nhận sự thiết lập bỏ qua việc nhập mật khẩu dựa trên sự thiết lập để không thực hiện quá trình xác nhận sử dụng thông tin xác nhận người dùng.

9. Thiết bị tạo ảnh theo điểm bất kỳ trong số các điểm từ 1 tới 8, trong đó dữ liệu được mã hóa trong công việc in cụ thể.

10. Thiết bị tạo ảnh theo điểm bất kỳ trong số các điểm từ 1 tới 9, trong đó thông tin xác nhận người dùng là sự kết hợp của tên người dùng và mật khẩu người dùng.

11. Thiết bị tạo ảnh theo điểm bất kỳ trong số các điểm từ 1 tới 9, trong đó thông tin xác nhận người dùng được nhập bằng cách sử dụng thẻ mạch tích hợp (IC).

12. Thiết bị tạo ảnh theo điểm bất kỳ trong số các điểm từ 1 tới 9, trong đó thông tin xác nhận người dùng là thông tin khuôn mặt của người dùng.

13. Thiết bị tạo ảnh theo điểm bất kỳ trong số các điểm từ 1 tới 9, trong đó thông tin xác nhận người dùng là thông tin vân tay của người dùng.

14. Phương pháp tạo ảnh sử dụng bộ hiển thị có khả năng hiển thị thông tin và sử dụng bộ tạo ảnh để tạo ảnh trên tấm, phương pháp tạo ảnh này bao gồm các bước:

bước để thu nhận công việc in cụ thể mà liên quan tới người dùng cụ thể và trong đó mật khẩu cụ thể được thiết lập;

bước để hiển thị trên bộ hiển thị màn hình xác nhận có khả năng hiển thị sự nhập thông tin xác nhận người dùng hoặc lệnh bỏ qua của sự nhập thông tin xác nhận người dùng;

bước để hiển thị trên bộ hiển thị màn hình danh sách công việc thứ nhất, trên đó chỉ công việc in liên quan tới người dùng cụ thể được thể hiện, dựa trên sự nhập thông tin xác nhận người dùng cho người dùng cụ thể trên màn hình xác nhận, để tiếp nhận sự lựa chọn công việc in cụ thể trên màn hình danh sách công việc thứ nhất, và để làm cho bộ tạo ảnh thực hiện việc tạo ảnh dựa trên công việc in cụ thể theo lệnh in mà không được chú ý với sự nhập mật khẩu cụ thể bất kỳ; và

bước để hiển thị màn hình danh sách công việc thứ hai, trên đó không chỉ công việc in liên quan tới người dùng cụ thể mà cả công việc in liên quan tới người dùng khác được thể hiện, dựa trên lệnh bỏ qua trên màn hình xác nhận, để

tiếp nhận sự lựa chọn công việc in cụ thể trên màn hình danh sách công việc thứ hai, và để làm cho bộ tạo ảnh thực hiện việc tạo ảnh dựa trên công việc in cụ thể theo lệnh in mà được chủ ý với sự nhập mật khẩu cụ thể.

15. Phương pháp tạo ảnh sử dụng bộ hiển thị có khả năng hiển thị thông tin và sử dụng bộ tạo ảnh tạo ảnh trên tấm, phương pháp tạo ảnh này bao gồm các bước:

bước để thu nhận công việc in cụ thể mà liên quan tới người dùng cụ thể và trong đó mật khẩu cụ thể được thiết lập;

bước để hiển thị trên bộ hiển thị màn hình xác nhận có khả năng hiển thị sự nhập thông tin xác nhận người dùng hoặc lệnh bỏ qua của sự nhập thông tin xác nhận người dùng;

bước để hiển thị trên bộ hiển thị màn hình danh sách công việc thứ nhất, trên đó công việc in liên quan tới người dùng cụ thể được thể hiện, dựa trên sự nhập thông tin xác nhận người dùng cho người dùng cụ thể trên màn hình xác nhận và trên đó công việc in liên quan tới người dùng khác với người dùng cụ thể không được thể hiện, để tiếp nhận sự lựa chọn công việc in cụ thể trên màn hình danh sách công việc thứ nhất, và để làm cho bộ tạo ảnh thực hiện việc tạo

ảnh dựa trên công việc in cụ thể theo lệnh in mà không được chú ý với sự nhập mật khẩu cụ thể bất kỳ; và

bước để hiển thị màn hình danh sách công việc thứ hai, trên đó không chỉ công việc in liên quan tới người dùng cụ thể mà cả công việc in liên quan tới người dùng khác được thể hiện, dựa trên lệnh bỏ qua trên màn hình xác nhận, để tiếp nhận sự lựa chọn công việc in cụ thể trên màn hình danh sách công việc thứ hai, và để làm cho bộ tạo ảnh thực hiện việc tạo ảnh dựa trên công việc in cụ thể theo lệnh in mà được chú ý với sự nhập mật khẩu cụ thể.

16. Phương pháp tạo ảnh sử dụng bộ hiển thị có khả năng hiển thị thông tin và sử dụng bộ tạo ảnh tạo ảnh trên tấm, phương pháp tạo ảnh này bao gồm các bước:

bước để thu nhận công việc in cụ thể mà liên quan tới người dùng cụ thể và trong đó mật khẩu cụ thể được thiết lập;

bước để hiển thị trên bộ hiển thị màn hình xác nhận có khả năng chỉ dẫn lựa chọn sự nhập thông tin xác nhận người dùng hoặc sự sử dụng của khách;

bước để hiển thị trên bộ hiển thị màn hình danh sách công việc thứ nhất, trên đó chỉ công việc in liên quan tới người dùng cụ thể được thể hiện, dựa trên

sự nhập thông tin xác nhận người dùng cho người dùng cụ thể trên màn hình xác nhận, để tiếp nhận sự lựa chọn công việc in cụ thể trên màn hình danh sách công việc thứ nhất, và để làm cho bộ tạo ảnh thực hiện việc tạo ảnh dựa trên công việc in cụ thể theo lệnh in mà không được chú ý với sự nhập mật khẩu cụ thể bất kỳ; và

bước để hiển thị màn hình danh sách công việc thứ hai, trên đó không chỉ công việc in liên quan tới người dùng cụ thể mà cả công việc in liên quan tới người dùng khác được thể hiện, dựa trên lệnh lựa chọn của sự sử dụng của khách trên màn hình xác nhận, để tiếp nhận sự lựa chọn công việc in cụ thể trên màn hình danh sách công việc thứ hai, và để làm cho bộ tạo ảnh thực hiện việc tạo ảnh dựa trên công việc in cụ thể theo lệnh in mà được chú ý với sự nhập mật khẩu cụ thể.

17. Phương pháp tạo ảnh sử dụng bộ hiển thị có khả năng hiển thị thông tin và sử dụng bộ tạo ảnh để tạo ảnh trên tấm, phương pháp tạo ảnh này bao gồm các bước:

bước để thu nhận công việc in cụ thể mà liên quan tới người dùng cụ thể và trong đó mật khẩu cụ thể được thiết lập;

bước để hiển thị trên bộ hiển thị màn hình xác nhận có khả năng chỉ dẫn lựa chọn sự nhập thông tin xác nhận người dùng hoặc sự sử dụng của khách;

bước để hiển thị trên bộ hiển thị màn hình danh sách công việc thứ nhất, trên đó công việc in liên quan tới người dùng cụ thể được thể hiện, dựa trên sự nhập thông tin xác nhận người dùng cho người dùng cụ thể trên màn hình xác nhận và trên đó công việc in liên quan tới người dùng khác với người dùng cụ thể không được thể hiện, để tiếp nhận sự lựa chọn công việc in cụ thể trên màn hình danh sách công việc thứ nhất, và để làm cho bộ tạo ảnh thực hiện việc tạo ảnh dựa trên công việc in cụ thể theo lệnh in mà không được chú ý với sự nhập mật khẩu cụ thể bất kỳ; và

bước để hiển thị màn hình danh sách công việc thứ hai, trên đó không chỉ công việc in liên quan tới người dùng cụ thể mà cả công việc in liên quan tới người dùng khác được thể hiện, dựa trên lệnh lựa chọn của khách trên màn hình xác nhận, để tiếp nhận sự lựa chọn công việc in cụ thể trên màn hình danh sách công việc thứ hai, và để làm cho bộ tạo ảnh thực hiện việc tạo ảnh dựa trên công việc in cụ thể theo lệnh in mà được chú ý với sự nhập mật khẩu cụ thể.

FIG.1

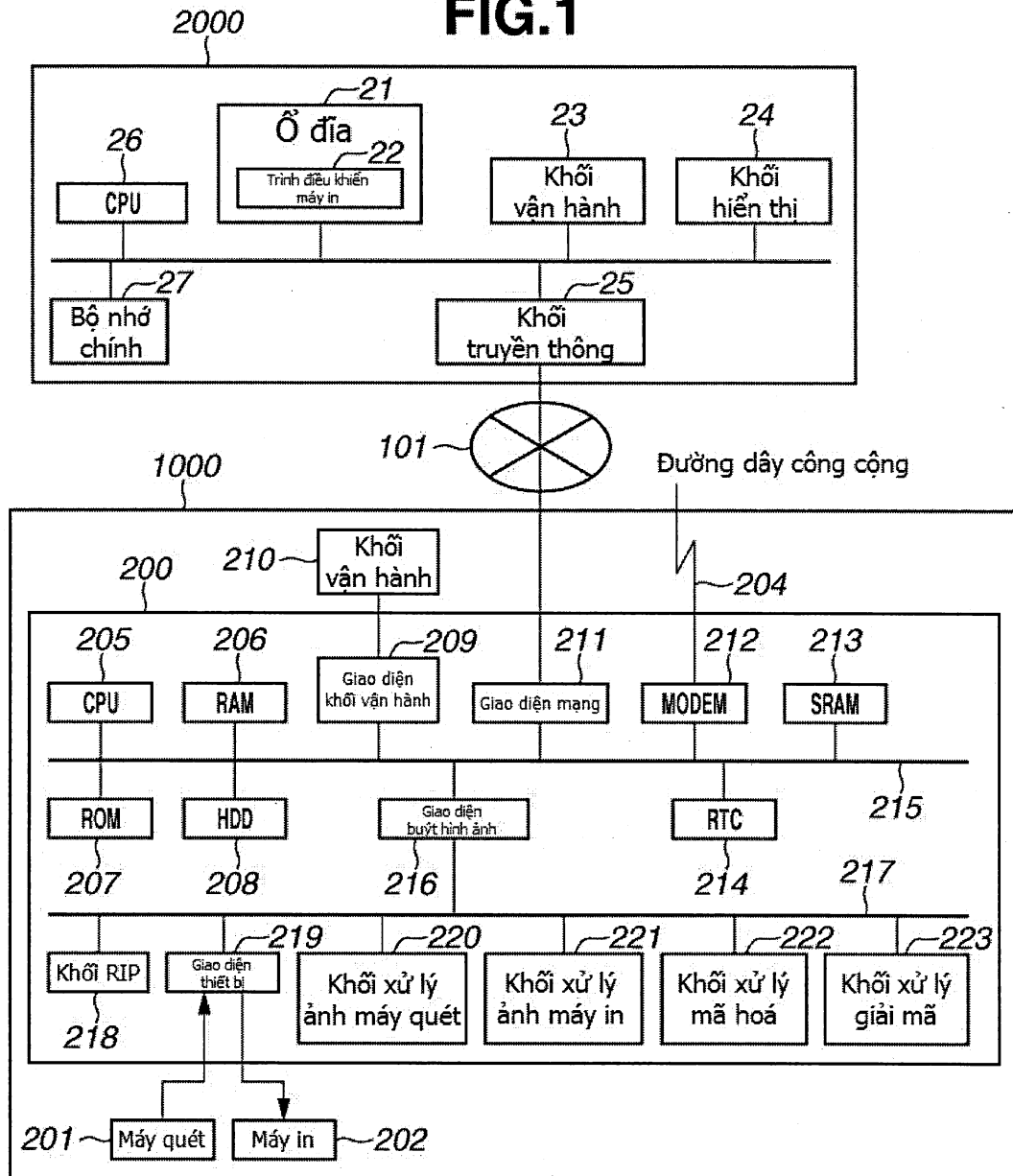


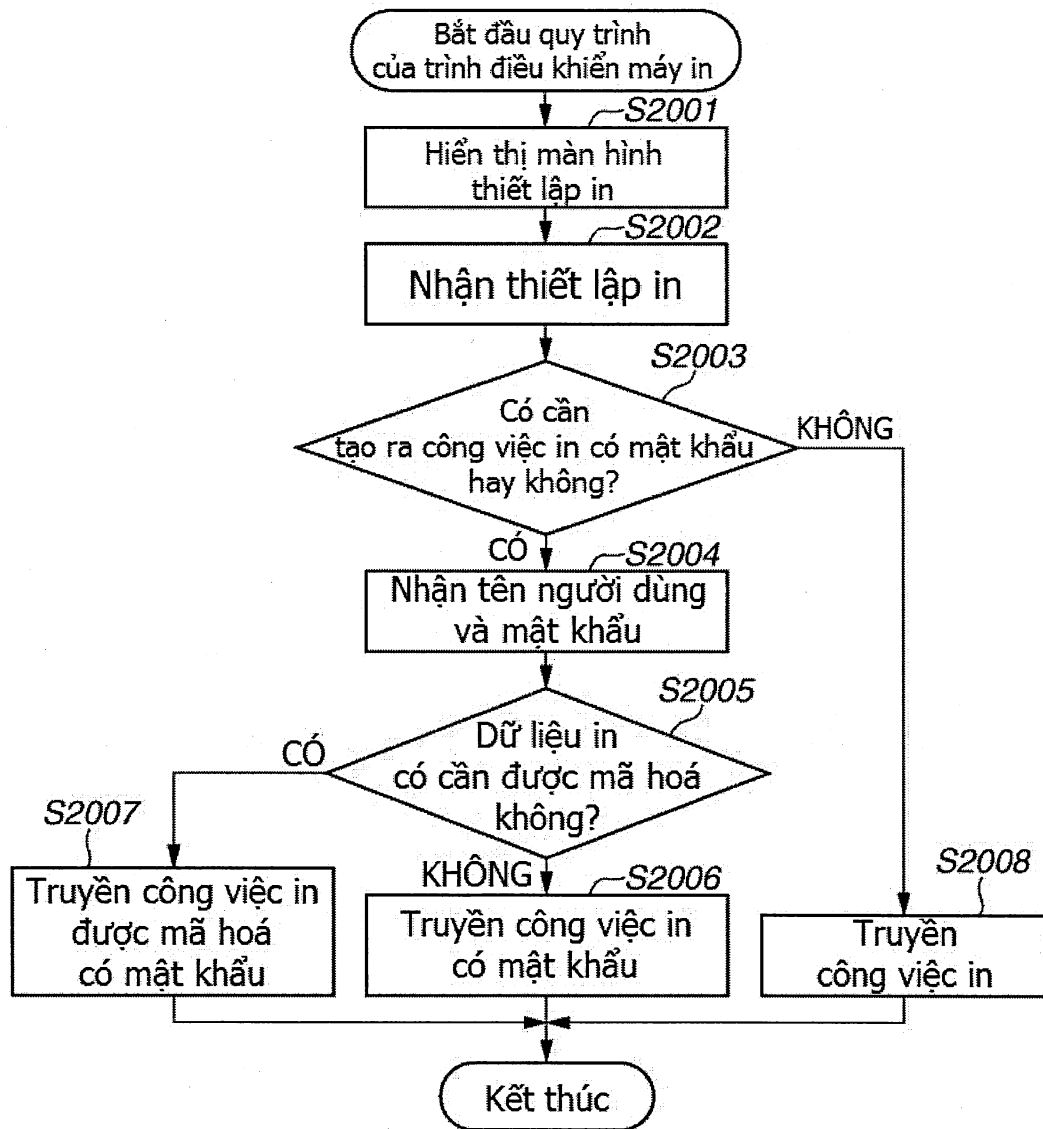
FIG.2

FIG.3A

0301

MÀN HÌNH THIẾT LẬP IN

KÍCH CỠ GIẤY: A4
 SỐ BẢN: 1
 NHÂN: KHÔNG

0302 ☒ THÊM MẬT KHẨU VÀO VIỆC IN

0303 ☐ DỮ LIỆU MÃ HÓA

OK

CANCEL

0304 0305

FIG.3B

0321

MÀN HÌNH NHẬP MẬT KHẨU CÔNG VIỆC VÀ TÊN NGƯỜI DÙNG

TÊN NGƯỜI DÙNG

NGƯỜI DÙNG A

0322

MẬT KHẨU CÔNG VIỆC

0323

OK

CANCEL

0324 0325

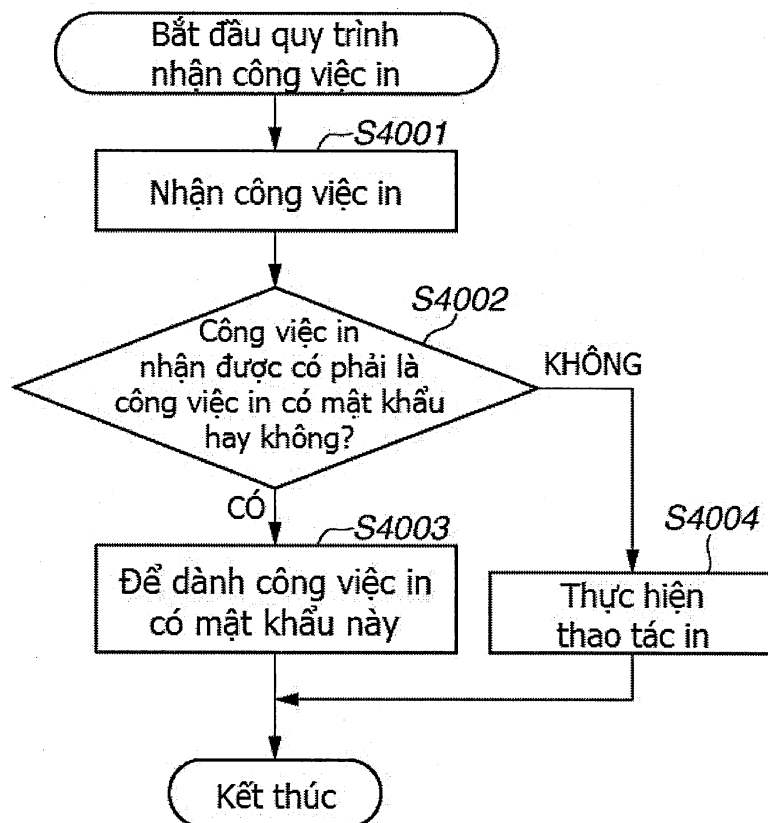
FIG.4

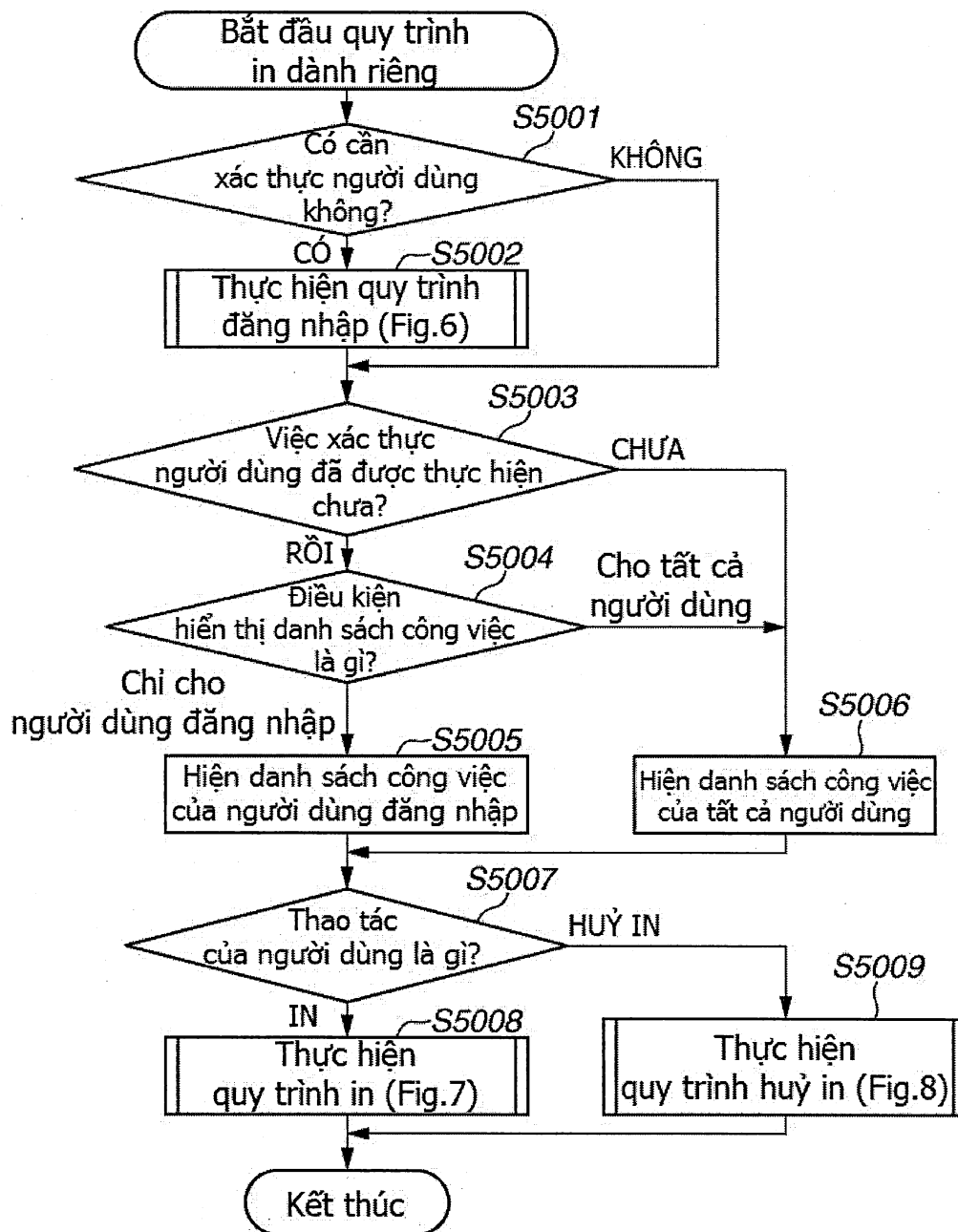
FIG.5

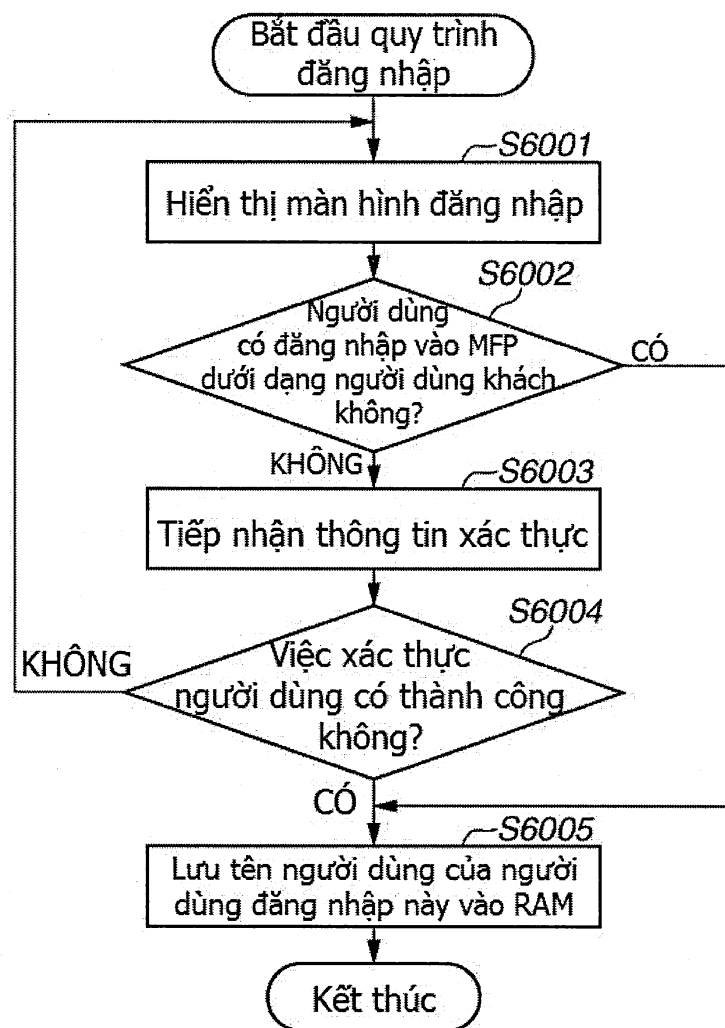
FIG.6

FIG.7

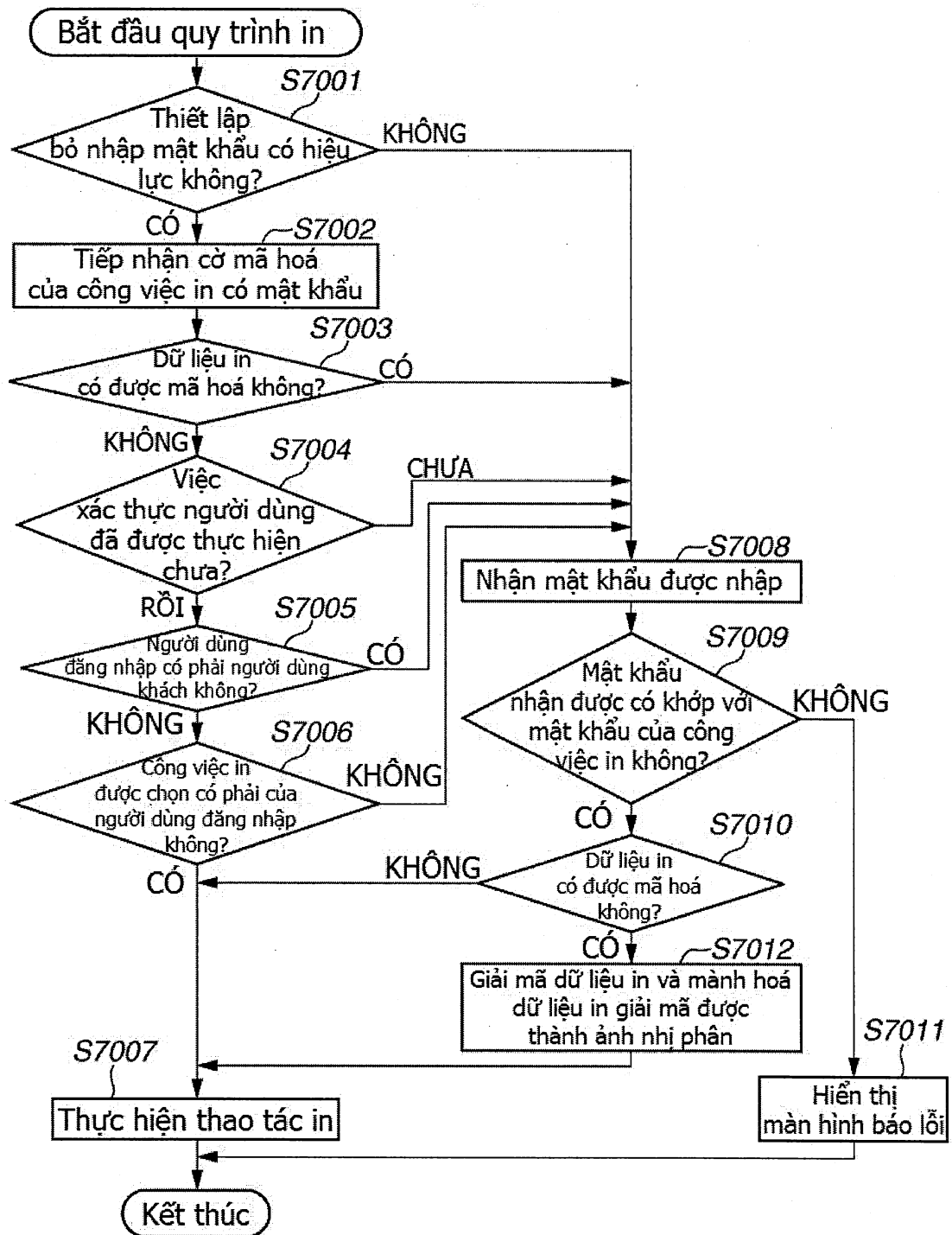


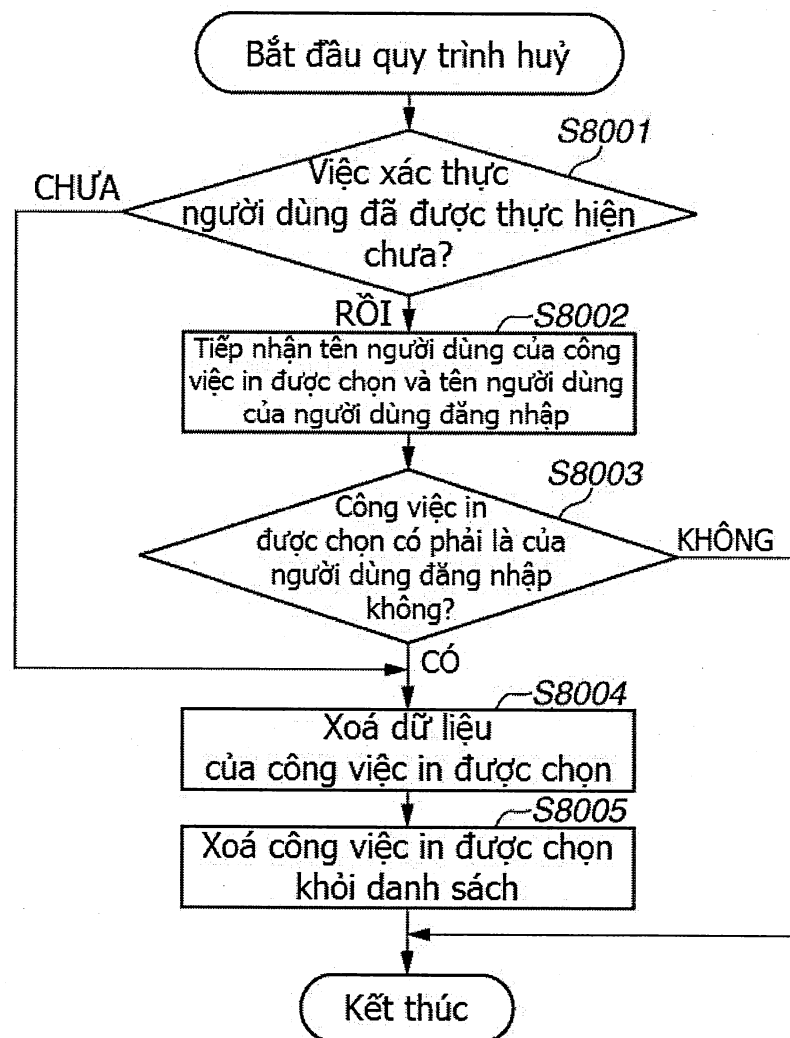
FIG.8

FIG.9

9001

DANH SÁCH CÁC CÔNG VIỆC IN THÊM MẬT KHẨU

CHỌN	SỐ TIẾP NHẬN	THỜI GIAN	TÊN CÔNG VIỆC	TÊN NGƯỜI DÙNG	TRẠNG THÁI
☒	0001	16:10	TÀI LIỆU1	NGƯỜI DÙNG1	CHỜ NHẬP MẬT KHẨU
☐	0002	16:20	TÀI LIỆU2	NGƯỜI DÙNG1	CHỜ NHẬP MẬT KHẨU
☐	0003	16:30	TÀI LIỆU3	NGƯỜI DÙNG1	CHỜ NHẬP MẬT KHẨU
☐	0004	16:40	TÀI LIỆU4	NGƯỜI DÙNG1	CHỜ NHẬP MẬT KHẨU
☐	0005	16:50	TÀI LIỆU5	NGƯỜI DÙNG1	CHỜ NHẬP MẬT KHẨU

9005

9006

CANCEL 9004

PRINT 9003

FIG.10

10001

THIẾT LẬP BỎ NHẬP MẬT KHẨU

10002 ☒ VALID 10003 ☐ INVALID

10004 10005

FIG.11

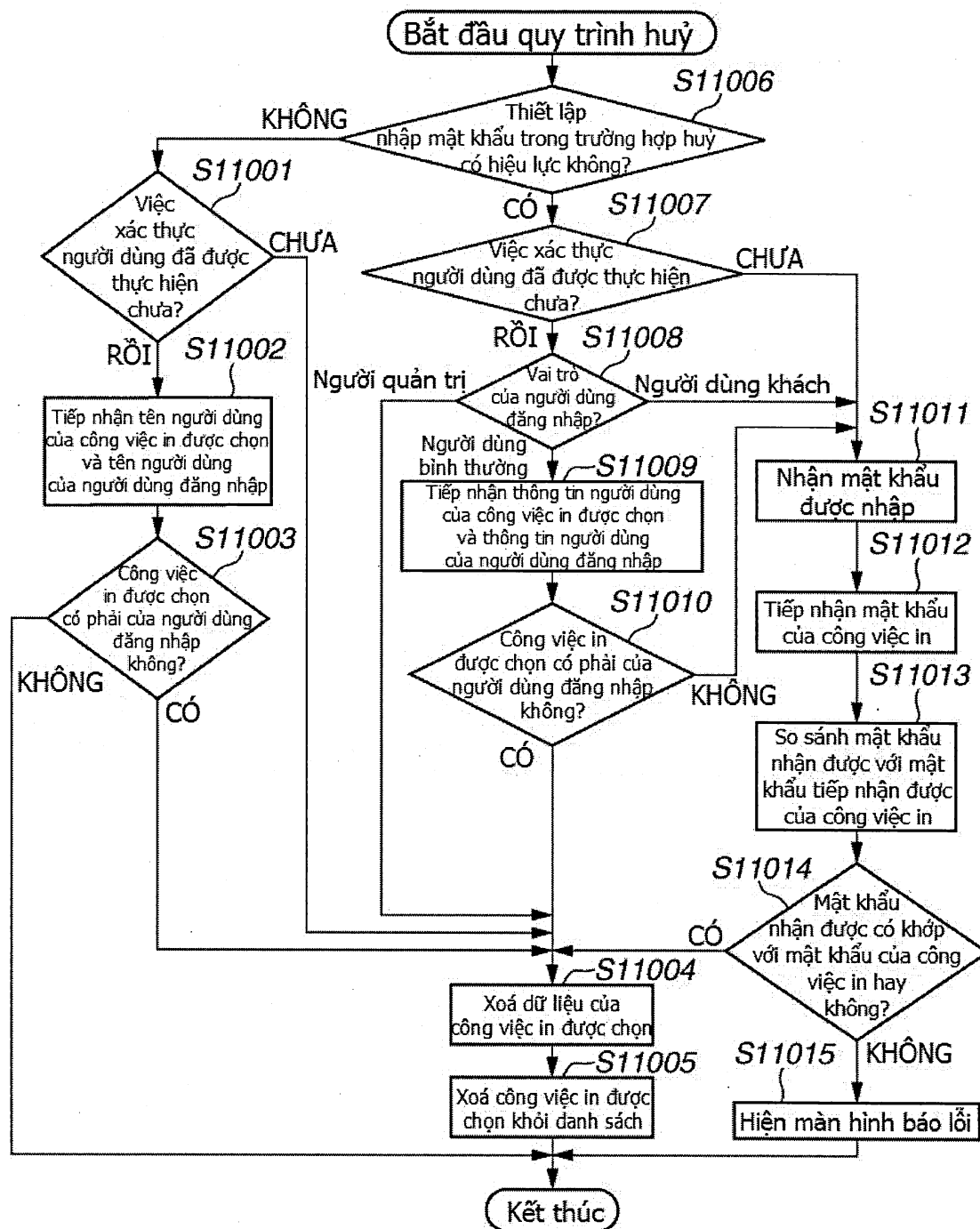


FIG.12

12001

THIẾT LẬP BỘ NHẬP MẬT KHẨU

TRONG TRƯỜNG HỢP IN

12002 ☒ VALID 12003 ☐ INVALID

TRONG TRƯỜNG HỢP HỦY BỎ

12006 ☒ VALID 12007 ☐ INVALID

OK CANCEL

12004 12005

FIG.13

1300

HÃY NHẬP TÊN NGƯỜI DÙNG VÀ MẬT KHẨU,
VÀ ÁN "ĐĂNG NHẬP" HOẶC "ĐĂNG NHẬP KHÁCH"

TÊN NGƯỜI DÙNG ▶ 1301

MẬT KHẨU ▶ 1302

■ ĐÍCH ĐĂNG NHẬP

THIẾT BỊ NÀY ▶

1303 ĐĂNG NHẬP

CHỨC NĂNG KHÁCH

SAO CHÉP

IN AN TOÀN

1/1

1304 ĐĂNG NHẬP KHÁCH