



(12) BẢN MÔ TẢ SÁNG CHẾ THUỘC BẰNG ĐỘC QUYỀN SÁNG CHẾ
(19) Cộng hòa xã hội chủ nghĩa Việt Nam (VN) (11) 
CỤC SỞ HỮU TRÍ TUỆ
1-0043407
(51)¹⁹ H04L 9/32; G06T 7/00; G06F 21/32; (13) B
G06F 21/64

(21) 1-2019-06820 (22) 18/04/2018
(86) PCT/JP2018/016055 18/04/2018 (87) WO 2018/225391 13/12/2018
(30) 2017-110552 05/06/2017 JP
(45) 25/02/2025 443 (43) 27/07/2020 388A
(73) HITACHI, LTD. (JP)
6-6, Marunouchi 1-chome, Chiyoda-ku, Tokyo 1008280, Japan
(72) SAKAZAKI, Hisao (JP); KAGA, Yosuke (JP); NEMOTO, Shigeyuki (JP).
(74) Công ty TNHH một thành viên Sở hữu trí tuệ VCCI (VCCI-IP CO.,LTD)

(54) THIẾT BỊ VÀ PHƯƠNG PHÁP XÁC MINH THÔNG TIN HÌNH ẢNH, HỆ
THỐNG XÁC THỰC VÀ PHƯƠNG PHÁP XÁC THỰC

(21) 1-2019-06820

(57) Sáng chế đề cập đến thiết bị và phương pháp xác minh thông tin hình ảnh, hệ thống xác thực và phương pháp xác thực. Tính xác thực của chứng nhận định danh số (hình ảnh) mà có thể được hiển thị trên màn hiển thị có thể được xác minh bằng cách trích các giá trị đặc trưng (chẳng hạn như “các vị trí của các điểm đặc trưng, chẳng hạn như đôi mắt, mũi, và các góc miệng, trên khuôn mặt” và “hình ảnh được cắt ra của chỉ phần mắt mà biểu thị đặc điểm khuôn mặt”) mà có dung lượng dữ liệu nhỏ và có khả năng định danh độc nhất ảnh chụp khuôn mặt, từ ảnh chụp khuôn mặt và nhúng các giá trị đặc trưng, làm dữ liệu xác minh tính xác thực, trong mã hai chiều.

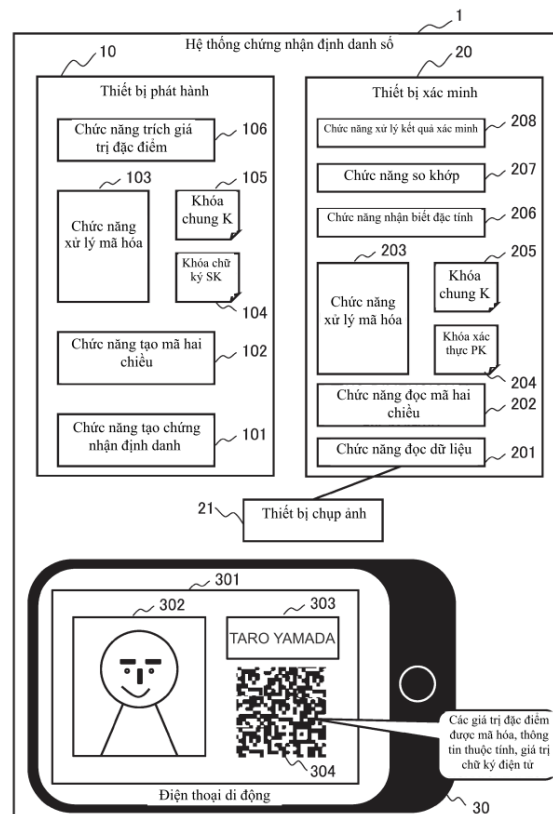


FIG.1

Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập đến việc xác minh thông tin hình ảnh và công nghệ xác thực dựa trên đó.

Tình trạng kỹ thuật của sáng chế

Chúng nhận định danh được tạo ra, đối với trường hợp thông thường, bằng cách in thông tin thuộc tính chẳng hạn như ảnh chụp khuôn mặt và tên trên phía mặt của thẻ IC, thẻ nhựa, hoặc tương tự và sau đó được ban hành; tuy nhiên, trong các năm gần đây khi thiết bị di động chẳng hạn như các điện thoại thông minh đã được phổ biến, có nhu cầu biểu diễn nhận dạng sử dụng thiết bị di động mà được mang theo mọi lúc, thay vì chứng nhận định danh loại thẻ.

Khi chứng nhận định danh là cần được thực hiện bởi thiết bị di động, dựa vào việc số hóa của thông tin thuộc tính chẳng hạn như ảnh chụp khuôn mặt và tên để chứng minh ID, ví dụ, có phương pháp có thể hiển thị dữ liệu được số hóa trên màn hiển thị của thiết bị di động và xác minh tính hợp lệ của chứng nhận định danh bằng cách kiểm tra trực quan nó và phương pháp có thể gửi dữ liệu tới thiết bị xác minh thông qua truyền thông và có thiết bị mà thực hiện việc xác minh để xác minh cơ học tính hợp lệ của dữ liệu chứng nhận định danh. Tuy nhiên, trong trường hợp sau, thiết bị di động lưu trữ các dữ liệu khác nhau ngoài dữ liệu chứng nhận định danh trong nhiều trường hợp và có thể gửi nhầm dữ liệu không cần thiết tới thiết bị mà thực hiện việc xác minh. Do đó, mong muốn là có cơ chế có khả năng chứng minh ID đơn giản bằng cách hiển thị và thể hiện hình ảnh của chứng nhận định danh trên màn hiển thị như trong trường hợp trước.

Tuy nhiên, trong trường hợp dữ liệu chứng nhận định danh được số hóa không giống chứng nhận định danh dạng thẻ thông thường được in trên phía mặt của thẻ, dễ dàng chuyển ảnh chụp khuôn mặt sang ảnh chụp khuôn mặt khác và

khó để phát hiện dấu vết chuyển ảnh chụp khuôn mặt ngay cả nếu dữ liệu hình ảnh được chuyển được hiển thị.

Do đó, đã có đề xuất công nghệ mà sử dụng ảnh chụp khuôn mặt và hình ảnh mã hai chiều, mà trong đó dữ liệu của ảnh chụp khuôn mặt được nhúng, làm chứng nhận định danh và đánh giá tính xác thực, khi chứng minh ID, bằng cách khôi phục lại ảnh chụp khuôn mặt từ mã hai chiều và so sánh nó với ảnh chụp khuôn mặt ban đầu (tài liệu sáng chế 1).

Danh mục tài liệu trích dẫn

Tài liệu sáng chế

Tài liệu sáng chế 1: Công bố đơn yêu cầu cấp patent Nhật Bản số 2005-141626

Tuy nhiên, do chính dữ liệu ảnh chụp khuôn mặt được nhúng trong mã hai chiều trong công nghệ thông thường, có vấn đề là việc tăng về kích thước của mã hai chiều. Thông thường, ngay cả dữ liệu ảnh chụp khuôn mặt có kích thước được sử dụng để chứng nhận định danh có dung lượng dữ liệu là vài kilobyte đến vài chục kilobyte. Ngay cả khi dữ liệu được nén, nếu dữ liệu ảnh chụp khuôn mặt được nhúng trong mã hai chiều và độ phân giải của nó được thiết đặt sao cho dữ liệu ảnh chụp khuôn mặt có thể được nhận biết bởi bộ đọc mã hai chiều, kích cỡ của mã hai chiều sẽ tăng tới, ví dụ, khoảng một nửa kích cỡ A4 phụ thuộc vào dung lượng dữ liệu của dữ liệu ảnh chụp khuôn mặt, mà dẫn đến vấn đề không có khả năng hiển thị mã hai chiều này trên màn hiển thị của điện thoại thông minh.

Trái lại, nếu cố gắng nhúng dữ liệu ảnh chụp khuôn mặt trong mã hai chiều ở kích thước đủ nhỏ để được hiển thị trên điện thoại thông minh, thì cần thiết phải làm giảm dung lượng dữ liệu của dữ liệu ảnh chụp khuôn mặt. Vì vậy, việc này làm cho ảnh chụp khuôn mặt trở thành hình ảnh thô và dẫn đến vấn đề là khó kiểm tra tính hợp lệ của ảnh chụp khuôn mặt bằng cách sử dụng hình ảnh thô đó.

Bản chất kỹ thuật của sáng chế

Nhằm giải quyết vấn đề nêu trên, công nghệ được sử dụng cho việc xác thực sinh trắc được áp dụng để trích các giá trị đặc trưng có khả năng định danh độc nhất ảnh chụp khuôn mặt (chẳng hạn như “các vị trí của các điểm đặc trưng, chẳng hạn như đôi mắt, mũi, và các góc miệng, trên khuôn mặt” và “hình ảnh được cắt ra của chỉ phần mắt mà biểu thị đặc điểm khuôn mặt”), từ dữ liệu ảnh chụp khuôn mặt và được nhúng các giá trị đặc trưng trong mã hai chiều.

Sau đó, khi ảnh chụp khuôn mặt và mã hai chiều được hiển thị làm cùng nền trên màn hiển thị của điện thoại thông minh để xác minh hình ảnh tương ứng (mà có thể được sử dụng như chứng nhận định danh), thiết bị chụp hình ảnh chẳng hạn như camera số, camera WEB, hoặc máy quét được sử dụng để đọc hình ảnh mà được hiển thị trên màn hiển thị, chữ ký điện tử từ mã hai chiều trong hình ảnh được hiển thị được xác minh, và xem mã hai chiều có phải là xác thực hay không được đánh giá.

Hơn thế nữa, sáng chế khác xác thực đối tượng camera dựa vào hình ảnh khuôn mặt được chụp bởi camera bên ngoài hoặc tương tự và ảnh chụp khuôn mặt mà đã được xác minh là xác thực.

Hiệu quả của sáng chế

Dấu hiệu của sáng chế là ở chỗ tính hợp lệ của hình ảnh (mà có thể được sử dụng như chứng nhận định danh) có thể được xác minh sử dụng dung lượng dữ liệu nhỏ hơn so với trường hợp trong đó dữ liệu ảnh chụp khuôn mặt được nhúng trong mã hai chiều.

Mô tả vắn tắt các hình vẽ

Fig.1 là hình vẽ minh họa ví dụ cấu hình hệ thống của phương án 1 của sáng chế;

Fig.2 là hình vẽ minh họa ví dụ cấu hình phần cứng của thiết bị ban hành, thiết bị xác minh, và điện thoại thông minh theo các phương án 1 và 2 của sáng chế;

Fig.3 là sơ đồ trình tự minh họa trình tự xử lý để ban hành chứng nhận định danh số theo các phương án 1 và 2 của sáng chế;

Fig.4 là sơ đồ trình tự minh họa trình tự xử lý để xác minh chứng nhận định danh số theo phương án 1 của sáng chế;

Fig.5 là hình vẽ hiển thị các kết quả xác minh của thiết bị xác minh theo phương án 1 của sáng chế;

Fig.6 là hình vẽ minh họa ví dụ cấu hình hệ thống của phương án 2 của sáng chế (sự khác biệt với Fig.1);

Fig.7 là sơ đồ trình tự minh họa trình tự xử lý để xác minh chứng nhận định danh số theo phương án 2 của sáng chế và trình tự xử lý để xác thực người nắm quyền của chứng nhận định danh số; và

Fig.8 là hình vẽ minh họa các kết quả xác thực của thiết bị xác minh theo phương án 2 (sự khác biệt với Fig.5).

Mô tả chi tiết sáng chế

[Phương án 1]

Cấu hình hệ thống

Phương án 1 của sáng chế sẽ được giải thích chi tiết dưới đây dựa vào các hình vẽ.

Fig.1 là hình vẽ minh họa ví dụ cấu hình tổng quát của hệ thống chứng nhận định danh số 1 theo phương án 1 này. Hình vẽ này cũng minh họa ví dụ cấu hình chức năng của mỗi máy tính mà tạo cấu hình hệ thống chứng nhận định danh số 1 cùng với cấu hình tổng quát. Hệ thống chứng nhận định danh số 1 được minh họa trên Fig.1 là hệ thống được thiết kế sao cho thiết bị ban hành 10 ban hành chứng nhận định danh số (dữ liệu hình ảnh) 301 cho điện thoại thông minh 30 và thiết bị xác minh 20 đọc hình ảnh của chứng nhận định danh số 301 được hiển thị trên màn hiển thị của điện thoại thông minh 30 và đánh giá tính xác thực của chứng nhận định danh số 301 được thể hiện, dựa vào hình ảnh đó.

Như được minh họa trên Fig.1, thiết bị ban hành 10 quản lý khóa chữ ký SK104 để tạo ra chữ ký điện tử và khóa chung K105 được sử dụng chung với thiết bị xác minh 20 và có thể được tạo cấu hình gồm: chức năng trích giá trị đặc trưng 106 mà trích các giá trị đặc trưng từ dữ liệu của ảnh chụp khuôn mặt, chức năng xử lý mã hóa 103 mà thực hiện mã hóa dữ liệu và quy trình xử lý tạo ra chữ ký điện tử; chức năng tạo mã hai chiều 102 mà tạo ra mã hai chiều; và chức năng thực hiện chứng nhận định danh 101 mà tạo nên chứng nhận định danh số (dữ liệu hình ảnh) 301 từ dữ liệu ảnh chụp khuôn mặt 302, thông tin thuộc tính 303 chẳng hạn như tên, và mã hai chiều 304. Hơn thế nữa, thiết bị xác minh 20 được liên kết với thiết bị chụp hình ảnh 21 và thiết bị xác minh 20 quản lý khóa xác minh PK204 để xác minh chữ ký điện tử và khóa chung K205 được sử dụng chung với thiết bị ban hành 10 và có thể được tạo cấu hình gồm: chức năng đọc dữ liệu 201 mà đọc hình ảnh của chứng nhận định danh số 301 được hiển thị trên màn hiển thị của điện thoại thông minh 30; chức năng đọc mã hai chiều 202 mà lấy ra phần mã hai chiều 304 từ hình ảnh được đọc và giải mã mã hai chiều; chức năng xử lý mã hóa 203 mà thực hiện xử lý để giải mã dữ liệu và xác minh chữ ký điện tử; chức năng nhận biết đặc tính 206 mà nhận biết các đặc tính của thông tin thuộc tính 303 chẳng hạn như tên từ hình ảnh của chứng nhận định danh số được đọc 301; chức năng so khớp 207 mà so sánh các giá trị đặc trưng được nhúng trong mã hai chiều với ảnh chụp khuôn mặt 302 được bao gồm trong hình ảnh của chứng nhận định danh số được đọc 301 và thực hiện việc xác minh; và chức năng xử lý kết quả xác minh 208 mà hiển thị các màn hình theo kết quả xác minh và ban hành lệnh để mở hoặc đóng cổng để quản lý vào và ra. Hơn thế nữa, điện thoại thông minh 30 cài đặt và lưu trữ chứng nhận định danh số (dữ liệu hình ảnh) 301 được thu nhận bởi, ví dụ, sự phân bố thông qua mạng hoặc phương tiện và hiển thị chứng nhận định danh số 301 trên màn hiển thị nếu cần.

Thiết bị ban hành 10, thiết bị xác minh 20, và điện thoại thông minh 30 mà có các chức năng được đề cập ở trên có thể được thực hiện bởi thiết bị xử lý thông tin chung 40 như được minh họa trên Fig.2. Ví dụ, chức năng trích giá trị đặc trưng 106, chức năng xử lý mã hóa 103, chức năng tạo mã hai chiều 102, và

chức năng tạo chứng nhận định danh 101 của thiết bị ban hành 10 và chức năng đọc dữ liệu 201, chức năng đọc mã hai chiều 202, chức năng xử lý mã hóa 203, chức năng nhận biết đặc tính 206, chức năng so khớp 207, và chức năng xử lý kết quả xác minh 208 của thiết bị xác minh 20 có thể được thực hiện như các chương trình máy tính được thực hiện bởi CPU 405 chẳng hạn như CPU (bộ xử lý trung tâm). Các chương trình máy tính này có thể được sử dụng bằng cách, ví dụ, lưu trữ nó từ trước trong thiết bị lưu trữ 404 chẳng hạn như đĩa cứng và duy trì nó ở đó hoặc nhận phân phối của nó từ mạng và mở rộng nó trong bộ nhớ 403.

Hơn thế nữa, các lệnh từ người dùng mà sử dụng hệ thống chứng nhận định danh số 1 này được đưa vào thông qua thiết bị đầu vào 401 chẳng hạn như bàn phím, chuột, và panen chạm mà chấp nhận các mục nhập; và xử lý các kết quả thu được làm kết quả của các lệnh được xuất ra từ thiết bị đầu ra 402 chẳng hạn như thiết bị hiển thị tinh thể lỏng và màn hình EL hữu cơ (quang điện).

Các thiết bị này dùng cho thiết bị ban hành 10, thiết bị xác minh 20, và điện thoại thông minh 30 có thể được tạo cấu hình trong thiết bị xử lý thông tin 40 được kết nối thông qua đường truyền thông bên trong chẳng hạn như bus (sau đây được gọi là bus) 406.

Hơn thế nữa, thiết bị chụp hình ảnh 21 được liên kết với thiết bị xác minh 20 được thực hiện bởi thiết bị chẳng hạn như camera số, camera WEB, hoặc máy quét.

Các ví dụ trình tự xử lý

Các trình tự xử lý theo phương án 1 này sẽ được giải thích dưới đây dựa vào các hình vẽ. Các loại thao tác khác nhau được giải thích dưới đây được thực hiện bởi các chương trình mà được đọc cho bộ nhớ hoặc tương tự và được thực hiện tương ứng bởi các thiết bị/bộ phận tương ứng mà cấu hình hệ thống chứng nhận định danh số 1.

Fig.3 là sơ đồ trình tự minh họa trình tự xử lý để ban hành chứng nhận định danh số 301 theo phương án này.

Dữ liệu ảnh chụp khuôn mặt 302 của người cần trở thành người nắm quyền của chứng nhận định danh số 301 được nhập vào thiết bị ban hành 10; và thiết bị ban hành 10 thực hiện chức năng trích giá trị đặc trưng 106 và nhờ đó trích các giá trị đặc trưng (chẳng hạn như “các vị trí của các điểm đặc trưng, chẳng hạn như đôi mắt, mũi, và các góc miệng, trên khuôn mặt” và “hình ảnh được cắt ra của chỉ phần mắt mà biểu thị đặc điểm khuôn mặt”) mà có dung lượng dữ liệu tương đối nhỏ và có khả năng định danh độc nhất ảnh chụp khuôn mặt, từ dữ liệu ảnh chụp khuôn mặt 302 (bước S101). Sau đó, thiết bị ban hành 10 thực hiện chức năng xử lý mã hóa 103 và nhờ đó mã hóa các giá trị đặc trưng với khóa chung K105 cần được sử dụng chung với thiết bị xác minh 20 (bước S102). Hơn thế nữa, thông tin thuộc tính 303 chẳng hạn như tên của người mà nên là người nắm quyền của chứng nhận định danh số 301 được nhập vào thiết bị ban hành 10 và thiết bị ban hành 10 kết nối thông tin thuộc tính 303 với các giá trị đặc trưng được mã hóa (bước S103). Tiếp theo, thiết bị ban hành 10 tính toán giá trị chữ ký điện tử đối với dữ liệu của các giá trị đặc trưng được mã hóa và thông tin thuộc tính 303, mà được kết nối với nhau, bằng cách sử dụng khóa chữ ký SK104 của thiết bị ban hành 10 và gán giá trị chữ ký điện tử cho dữ liệu của các giá trị đặc trưng được mã hóa và thông tin thuộc tính 303 mà được kết nối với nhau (bước S104). Sau đó, chức năng tạo mã hai chiều 102 được thực hiện và mã hai chiều 304 nhờ đó được tạo ra bằng cách sử dụng các giá trị đặc trưng được mã hóa, thông tin thuộc tính 303, và dữ liệu chữ ký điện tử mà được kết nối với nhau, làm các đầu vào. Mô tả cụ thể, dữ liệu được kết nối nêu trên được mã hóa thành mã hai chiều (bước S105). Sau đó, thiết bị ban hành 10: thực hiện chức năng tạo chứng nhận định danh 101 và nhờ đó định vị và tạo nên dữ liệu ảnh chụp khuôn mặt 302, thông tin thuộc tính 303, và mã hai chiều 304 sao cho chúng có thể được hiển thị cùng lúc trên màn hiển thị của điện thoại thông minh (bước S106); và xuất chúng ra ngoài làm chứng nhận định danh số (dữ liệu hình ảnh) 301 (bước S107).

Điện thoại thông minh 30 thu nhận chứng nhận định danh số (dữ liệu hình ảnh) 301 bằng, ví dụ, việc phân phối thông qua mạng hoặc phương tiện (bước

S108) và lưu trữ chứng nhận định danh số (dữ liệu hình ảnh) 301 trong thiết bị lưu trữ 404 cho điện thoại thông minh 30 (bước S109).

Fig.4 là sơ đồ trình tự minh họa trình tự xử lý để xác minh chứng nhận định danh số theo phương án 1.

Điện thoại thông minh 30 hiển thị chứng nhận định danh số (dữ liệu hình ảnh) 301, mà được lưu trữ ở bước S109, trên màn hiển thị của điện thoại thông minh 30 và thể hiện nó cho thiết bị chụp hình ảnh 21 (bước S200).

Thiết bị chụp hình ảnh 21 chụp hình ảnh được hiển thị trên màn hiển thị của điện thoại thông minh 30 (bước S201); và thiết bị xác minh 20 thu nhận hình ảnh nền được chụp bởi thiết bị chụp hình ảnh 21 từ thiết bị chụp hình ảnh 21 (bước S202). Sau đó, thiết bị xác minh 20 đọc mã hai chiều từ hình ảnh nền được thu nhận bởi chức năng đọc mã hai chiều 202 ở bước S202 và giải mã mã hai chiều (bước S203). Dữ liệu được giải mã được cấu thành từ các giá trị đặc trưng được mã hóa, thông tin thuộc tính, và giá trị chữ ký điện tử và chữ ký điện tử được xác minh dựa vào các mẫu dữ liệu này bằng cách sử dụng chức năng xử lý mã hóa 203 (bước S204). Nếu việc xác minh chữ ký không thành công, nó được hiển thị, như quy trình xử lý lỗi, trên màn hiển thị của thiết bị xác minh 20 như được minh họa trên hình vẽ ở phía trên bên trái của Fig.5 rằng phần mã hai chiều 304 trong chứng nhận định danh số 301 là sai và việc xác minh chữ ký do đó đã thất bại (bước S205).

Nếu việc xác minh chữ ký thành công, các đặc tính liên quan tới thông tin thuộc tính 303 từ hình ảnh nền được thu nhận ở bước S202 được nhận biết bằng cách sử dụng chức năng nhận biết đặc tính 206 và được so sánh với thông tin thuộc tính được giải mã ở bước S203 để thực hiện việc xác minh (bước S206). Nếu các mẫu thông tin này không khớp với nhau, nó được hiển thị, như quy trình xử lý lỗi, trên màn hiển thị của thiết bị xác minh 20 như được minh họa trên hình vẽ ở phía trên bên phải của Fig.5 rằng phần thông tin thuộc tính 303 trong chứng nhận định danh số 301 là sai và thông tin thuộc tính đã bị giả mạo, và sau đó thông tin thuộc tính chính xác được hiển thị (bước S207).

Nếu các mẫu của thông tin thuộc tính nêu trên khớp với nhau, chức năng xử lý mã hóa 203 được thực hiện và các giá trị đặc trưng được mã hóa được giải mã ở bước S203 nhờ đó được giải mã với khóa chung K205 (bước S208); và các giá trị đặc trưng được giải mã được so sánh với phần ảnh chụp khuôn mặt của hình ảnh nền được thu nhận ở bước S202 để thực hiện việc xác minh bằng cách sử dụng chức năng so khớp 207 và xem các giá trị đặc trưng có phải là dữ liệu được trích từ ảnh chụp khuôn mặt đó hay không được xác minh (bước S209). Chức năng so khớp 207 thể hiện mối tương quan giữa ảnh chụp khuôn mặt và các giá trị đặc trưng như giá trị số học; và nếu tỷ lệ khớp giữa ảnh chụp khuôn mặt và các giá trị đặc trưng là bằng hoặc nhỏ hơn giá trị ngưỡng, nó được hiển thị, như quy trình xử lý lỗi, trên màn hiển thị của thiết bị xác minh 20 như được minh họa trên hình vẽ ở phần phía dưới bên trái của Fig.5 rằng phần ảnh chụp khuôn mặt 302 trong chứng nhận định danh số 301 là sai và ảnh chụp khuôn mặt đã bị giả mạo (bước S210).

Nếu tỷ lệ khớp giữa ảnh chụp khuôn mặt và các giá trị đặc trưng là bằng hoặc lớn hơn giá trị ngưỡng, nó được hiển thị, như quy trình xử lý kết quả tính xác thực, trên màn hiển thị của thiết bị xác minh 20 như được minh họa trên hình vẽ ở phần phía dưới bên phải của Fig.5 rằng chứng nhận định danh số 301 là xác thực (bước S210).

[Phương án 2]

Phương án 2 của sáng chế sẽ được giải thích chi tiết dựa vào các hình vẽ. Phương án 2 được thực hiện bổ sung cho phương án 1.

Fig.6 là hình vẽ minh họa ví dụ cấu hình tổng thể của hệ thống chứng nhận định danh số 2 theo phương án 2 này (sự khác biệt với Fig.1). Trong phương án 2, thiết bị xác minh 20 là hệ thống mà cũng được liên kết với thiết bị chụp hình ảnh chân dung 22 và cũng xác minh xem người có chứng nhận định danh số 301 có phải là người nắm quyền hay không, thông qua chức năng xác thực khuôn mặt 209 được sử dụng cho việc xác thực sinh trắc dựa vào ảnh chụp khuôn mặt 302 và các video và các hình ảnh được chụp bởi thiết bị chụp hình ảnh chân dung 22.

Thiết bị chụp hình ảnh chân dung 22 mà được liên kết với thiết bị xác minh được thực hiện bởi thiết bị chẳng hạn như camera số hoặc camera WEB.

Cần lưu ý rằng trong phương án 2, chứng nhận định danh số 301 được ban hành theo cách giống như trong phương án 1.

Fig.7 là sơ đồ trình tự minh họa trình tự xử lý để xác minh chứng nhận định danh số theo phương án 2 này và trình tự xử lý để xác thực người nắm quyền của chứng nhận định danh số. Các bước từ S200 đến bước S210 là cùng quy trình xử lý như quy trình xử lý của phương án 1.

Thiết bị chụp hình ảnh chân dung 22 chụp hình ảnh người mà có chứng nhận định danh số 301 (bước S301); và thiết bị xác minh 20 thu nhận hình ảnh chân dung được chụp ở bước S301 từ thiết bị chụp hình ảnh chân dung 22 (bước S302). Sau đó, thiết bị xác minh 20 thực hiện việc so sánh và việc xác minh bằng cách sử dụng dữ liệu ảnh chụp khuôn mặt, mà đã được xác định là xác thực ở bước S209, và dữ liệu hình ảnh chân dung được thu nhận ở bước S301, và nhờ đó xác minh xem người mà có chứng nhận định danh số 301 có phải là người nắm quyền hay không (bước S303). Chức năng xác thực khuôn mặt 209 thể hiện mối tương quan giữa ảnh chụp khuôn mặt và hình ảnh chân dung như giá trị số học; và nếu tỷ lệ khớp giữa ảnh chụp khuôn mặt và hình ảnh chân dung là bằng hoặc nhỏ hơn giá trị ngưỡng, nó được hiển thị, như quy trình xử lý lỗi, trên màn hiển thị của thiết bị xác minh 20 như được minh họa trên hình vẽ ở phần phía trên của Fig.8 rằng ảnh chụp khuôn mặt 302 của chứng nhận định danh số 301 không khớp với khuôn mặt của người mà có chứng nhận định danh số 301 (bước S304).

Nếu tỷ lệ khớp giữa ảnh chụp khuôn mặt và hình ảnh chân dung là bằng hoặc lớn hơn giá trị ngưỡng, nó được hiển thị, như quy trình xử lý kết quả tính xác thực, trên màn hiển thị của thiết bị xác minh 20 như được minh họa trên hình vẽ ở phần phía dưới của Fig.8 rằng chứng nhận định danh số 301 là xác thực và khớp với khuôn mặt của người mà có chứng nhận định danh số 301 (bước S305).

Danh mục các số chỉ dẫn

- 1: hệ thống chứng nhận định danh số

- 2: hệ thống chứng nhận định danh số
- 10: thiết bị ban hành
- 20: thiết bị xác minh
- 21: thiết bị chụp hình ảnh
- 22: thiết bị chụp hình ảnh chân dung
- 30: điện thoại thông minh
- 40: thiết bị xử lý thông tin
- 101: chức năng thực hiện chứng nhận định danh
- 102: chức năng tạo mã hai chiều
- 103: chức năng xử lý mã hóa
- 104: khóa chữ ký SK
- 105: khóa chung K
- 106: chức năng trích giá trị đặc trưng
- 201: chức năng đọc dữ liệu
- 202: chức năng đọc mã hai chiều
- 203: chức năng xử lý mã hóa
- 204: khóa xác minh PK
- 205: khóa chung K
- 206: chức năng nhận biết đặc tính
- 207: chức năng so khớp
- 208: chức năng xử lý kết quả xác minh
- 209: chức năng xác thực khuôn mặt
- 301: chứng nhận định danh số
- 302: ảnh chụp khuôn mặt
- 303: thông tin thuộc tính
- 304: mã hai chiều
- 401: thiết bị đầu vào

- 402: thiết bị đầu ra
- 403: bộ nhớ
- 404: thiết bị lưu trữ
- 405: CPU (bộ xử lý trung tâm)
- 406: bus

YÊU CẦU BẢO HỘ

1. Thiết bị xác minh thông tin hình ảnh bao gồm:

bộ trích mà đọc hình ảnh và trích hình ảnh định danh, hình ảnh khuôn mặt, và hình ảnh thông tin thuộc tính liên quan đến hình ảnh khuôn mặt từ hình ảnh;

bộ phận xác minh hình ảnh định danh mà xác minh hình ảnh định danh dựa vào chữ ký điện tử được bao gồm trong hình ảnh định danh; và

bộ phận xác minh hình ảnh mà so sánh hình ảnh thông tin thuộc tính được trích với thông tin thuộc tính được bao gồm trong hình ảnh định danh được xác minh, và, nếu hình ảnh thông tin thuộc tính khớp với thông tin thuộc tính, so sánh thông tin giá trị đặc trưng thứ nhất được trích từ hình ảnh khuôn mặt với thông tin giá trị đặc trưng thứ hai được bao gồm trong hình ảnh định danh được xác minh và xác minh tính xác thực của hình ảnh,

trong đó hình ảnh định danh là hình ảnh định danh được tạo ra bằng cách đưa vào chữ ký điện tử, thông tin giá trị đặc trưng thứ hai, và thông tin thuộc tính.

2. Thiết bị xác minh thông tin hình ảnh theo điểm 1,

trong đó thông tin giá trị đặc trưng thứ nhất và thông tin giá trị đặc trưng thứ hai là thông tin liên quan đến vị trí điểm đặc trưng trên khuôn mặt.

3. Thiết bị xác minh thông tin hình ảnh theo điểm 1 hoặc 2, thiết bị này còn bao gồm bộ phận hiển thị mà hiển thị kết quả xác minh, trong đó bộ phận hiển thị:

hiển thị việc xác minh không thành công chữ ký điện tử nếu việc xác minh hình ảnh định danh bởi bộ phận xác minh hình ảnh định danh không thành công;

hiển thị rằng thông tin thuộc tính đã bị giả mạo, và hiển thị thông tin thuộc tính chính xác nếu hình ảnh thông tin thuộc tính không khớp với thông tin thuộc tính là kết quả của sự so sánh giữa hình ảnh thông tin thuộc tính và thông tin thuộc tính bởi bộ phận xác minh hình ảnh; và

hiển thị rằng hình ảnh khuôn mặt đã bị giả mạo nếu thông tin giá trị đặc trưng thứ nhất không khớp với thông tin giá trị đặc trưng thứ hai là kết quả của sự

so sánh giữa thông tin giá trị đặc trưng thứ nhất và thông tin giá trị đặc trưng thứ hai bởi bộ phận xác minh hình ảnh.

4. Hệ thống xác thực bao gồm thiết bị xác minh thông tin hình ảnh theo điểm bất kỳ trong số các điểm từ 1 đến 3 và thiết bị chụp hình ảnh,

trong đó thiết bị xác minh thông tin hình ảnh còn bao gồm bộ phận xác thực mà so sánh hình ảnh được chụp bởi thiết bị chụp hình ảnh với hình ảnh khuôn mặt, mà được trích từ hình ảnh được xác minh bởi bộ phận xác minh hình ảnh, và xác thực đối tượng mà hình ảnh đã được chụp bởi thiết bị chụp hình ảnh.

5. Hệ thống xác thực theo điểm 4, hệ thống này còn bao gồm bộ phận xử lý kết quả xác minh mà ban hành lệnh đóng/mở cho cổng theo kết quả xác thực của đối tượng.

6. Hệ thống xác thực theo điểm 5, trong đó hình ảnh định danh được tạo ra bằng cách mã hóa thông tin giá trị đặc trưng thứ hai với khóa chung.

7. Phương pháp xác minh thông tin hình ảnh bao gồm:

bước đọc hình ảnh để đọc hình ảnh;

bước trích để trích hình ảnh định danh, hình ảnh khuôn mặt, và hình ảnh thông tin thuộc tính liên quan đến hình ảnh khuôn mặt từ hình ảnh;

bước xác minh hình ảnh định danh để xác minh hình ảnh định danh dựa vào chữ ký điện tử được bao gồm trong hình ảnh định danh; và

bước xác minh hình ảnh, mà được thực hiện nếu hình ảnh thông tin thuộc tính được trích được so sánh với thông tin thuộc tính được bao gồm trong hình ảnh định danh được xác minh và hình ảnh thông tin thuộc tính khớp với thông tin thuộc tính, để so sánh thông tin giá trị đặc trưng thứ nhất được trích từ hình ảnh khuôn mặt với thông tin giá trị đặc trưng thứ hai được bao gồm trong hình ảnh định danh được xác minh và xác minh tính xác thực của hình ảnh,

trong đó hình ảnh định danh là hình ảnh định danh được tạo ra bằng cách đưa vào chữ ký điện tử, thông tin giá trị đặc trưng thứ hai, và thông tin thuộc tính.

8. Phương pháp xác thực bao gồm:

bước đọc hình ảnh để đọc hình ảnh;

bước trích để trích hình ảnh định danh, hình ảnh khuôn mặt, và hình ảnh thông tin thuộc tính liên quan đến hình ảnh khuôn mặt từ hình ảnh;

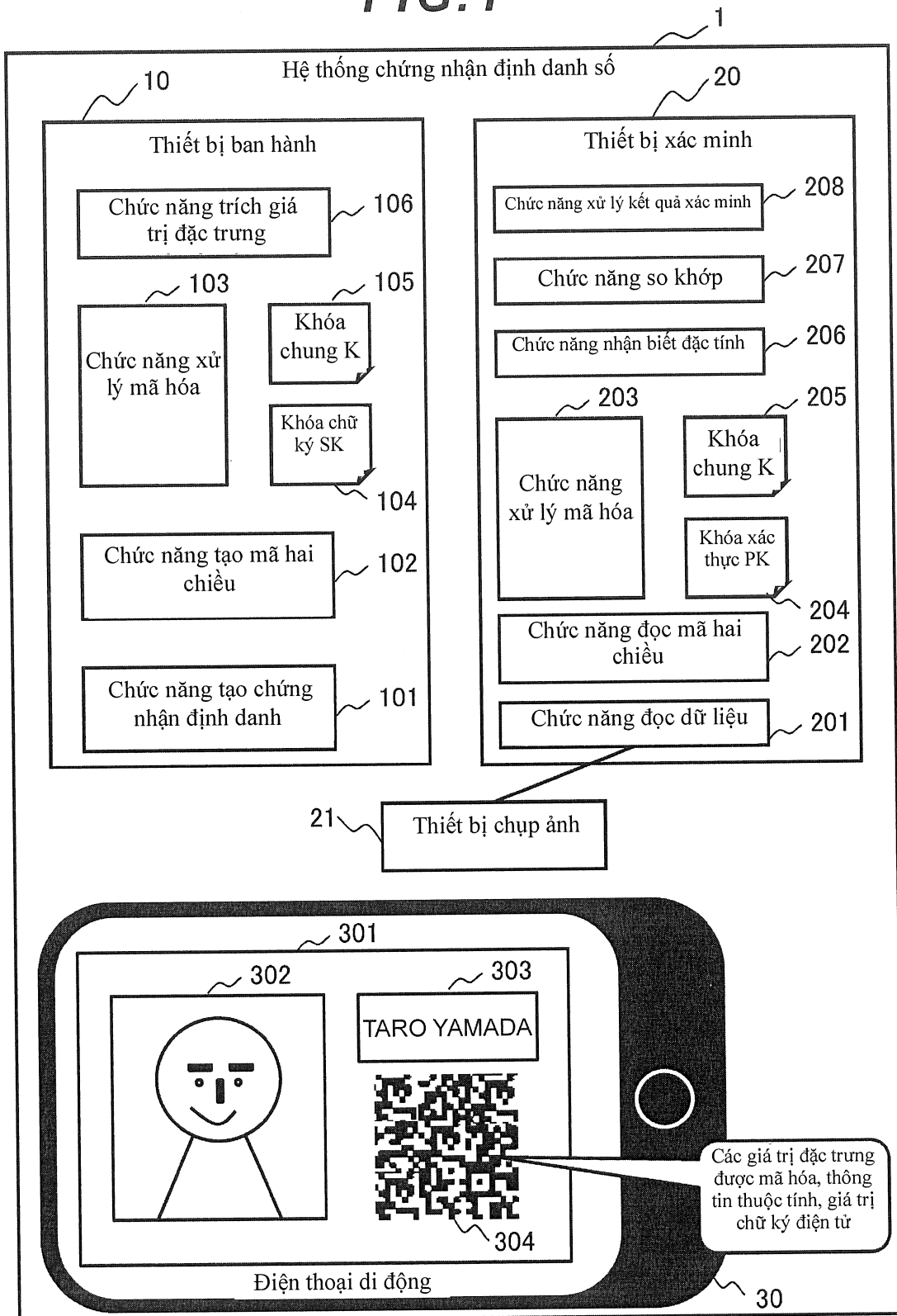
bước xác minh hình ảnh định danh để xác minh hình ảnh định danh dựa vào chữ ký điện tử được bao gồm trong hình ảnh định danh;

bước xác minh hình ảnh, mà được thực hiện nếu hình ảnh thông tin thuộc tính được trích được so sánh với thông tin thuộc tính được bao gồm trong hình ảnh định danh được xác minh và hình ảnh thông tin thuộc tính khớp với thông tin thuộc tính, để so sánh thông tin giá trị đặc trưng thứ nhất được trích từ hình ảnh khuôn mặt với thông tin giá trị đặc trưng thứ hai được bao gồm trong hình ảnh định danh được xác minh và xác minh tính xác thực của hình ảnh; và

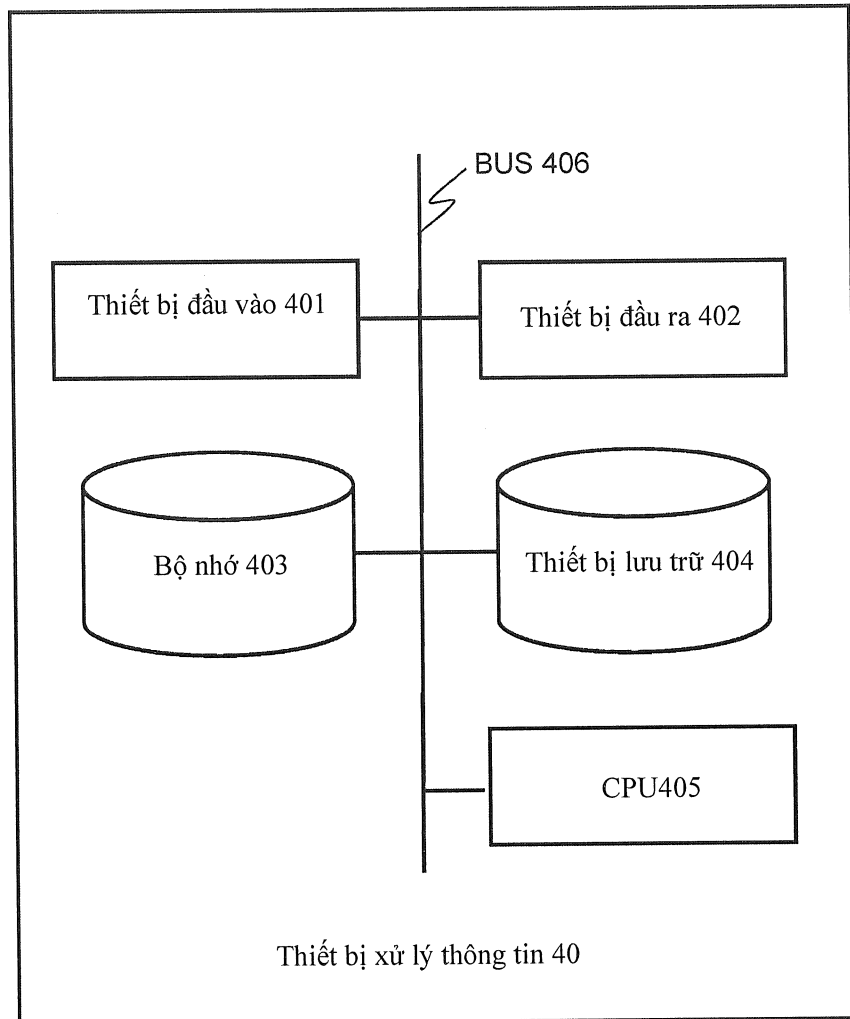
bước xác thực để so sánh hình ảnh được chụp bởi thiết bị chụp hình ảnh với hình ảnh khuôn mặt và xác thực đối tượng mà hình ảnh của đối tượng này đã được chụp bởi thiết bị chụp hình ảnh,

trong đó hình ảnh định danh là hình ảnh định danh được tạo ra bằng cách đưa vào chữ ký điện tử, thông tin giá trị đặc trưng thứ hai, và thông tin thuộc tính.

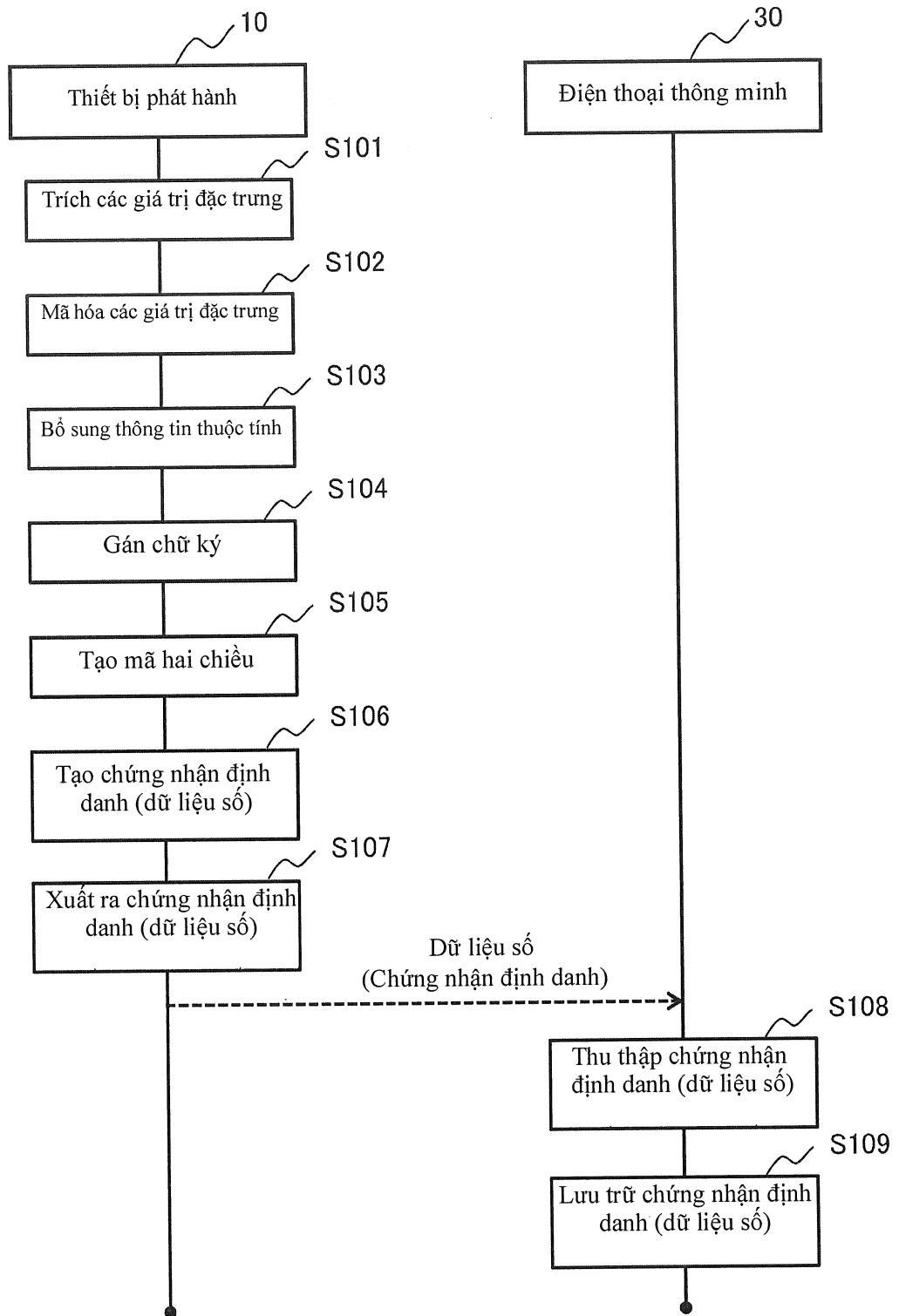
1/8

FIG. 1

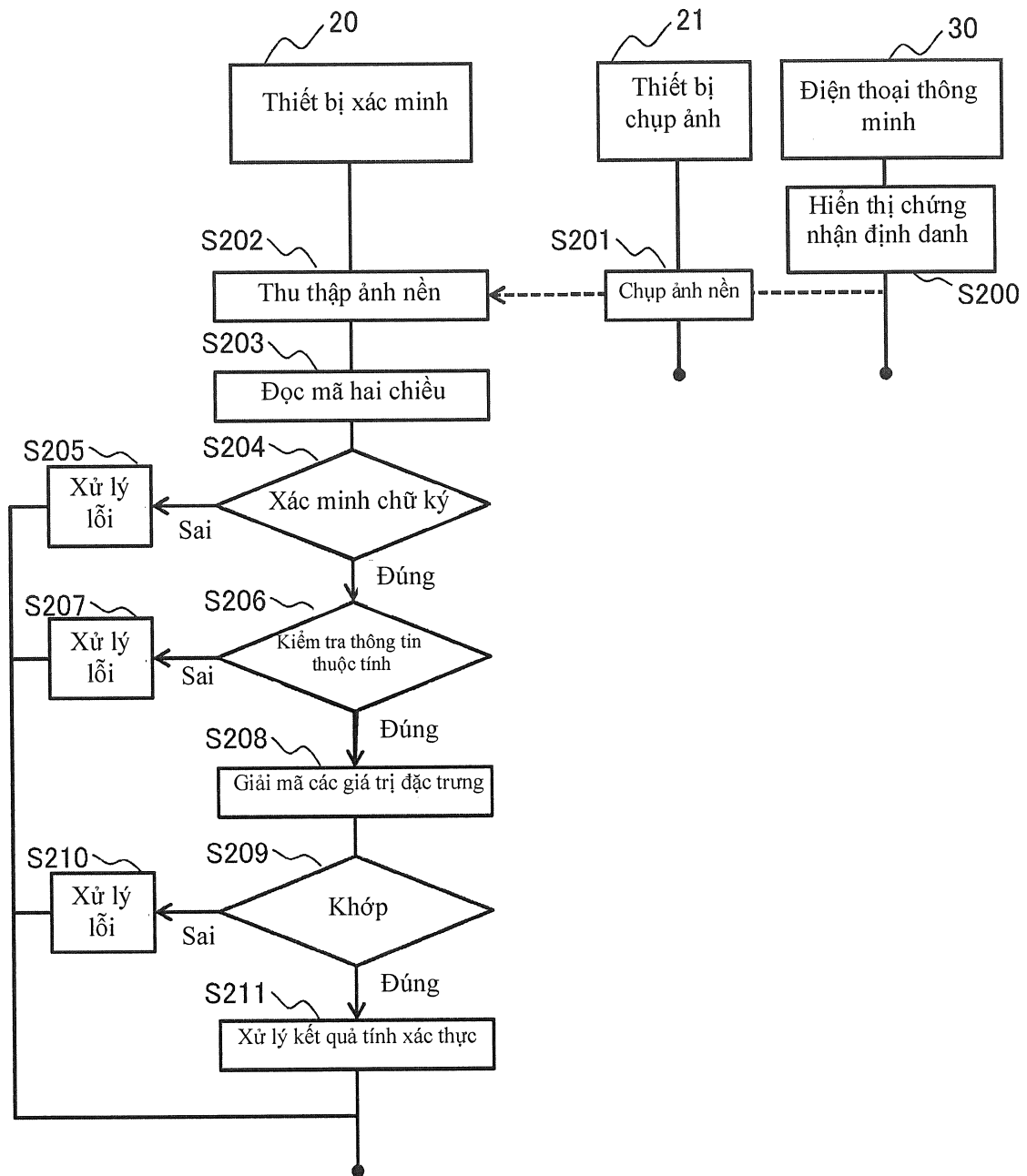
2/8

FIG.2

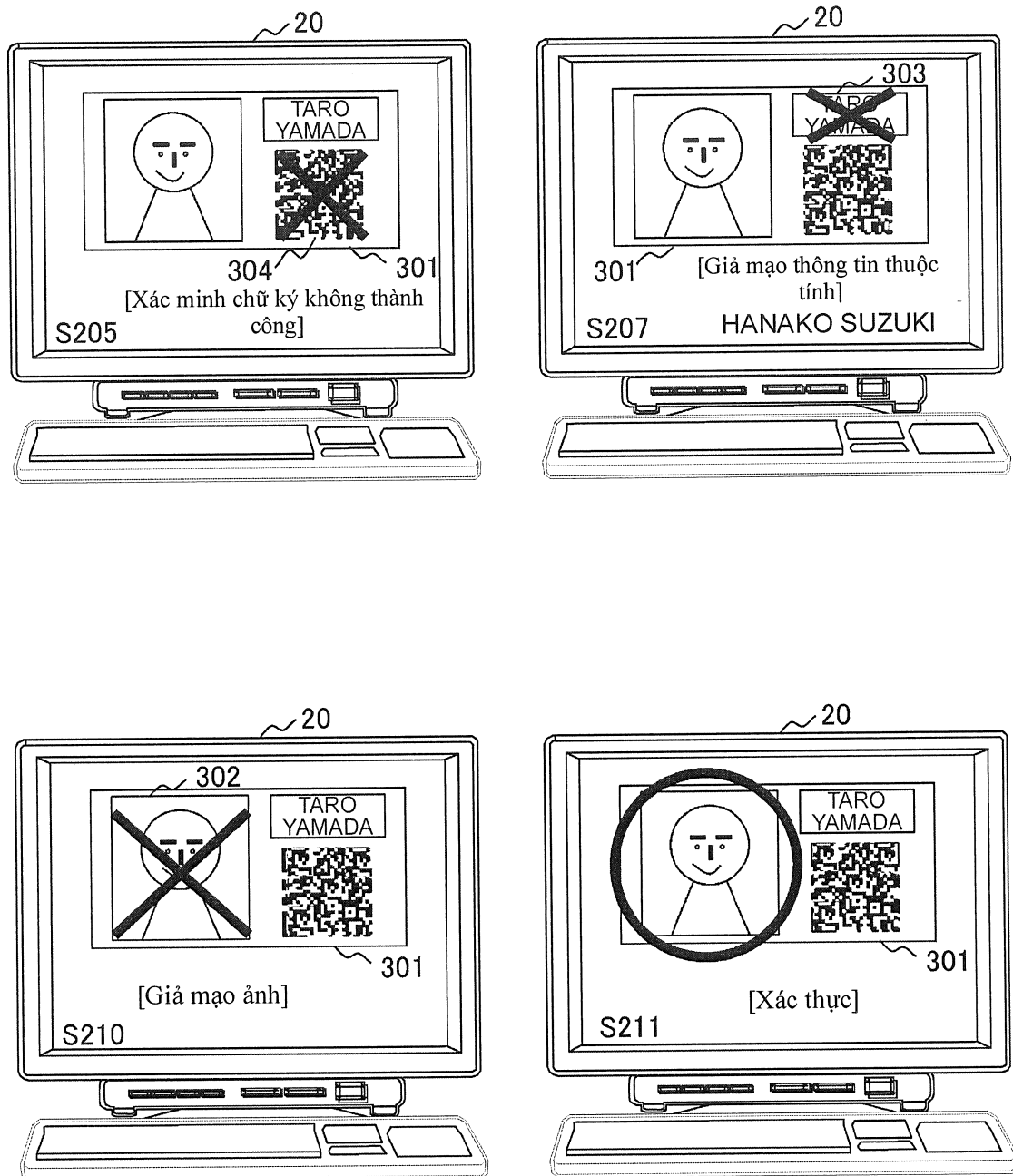
3/8

FIG. 3

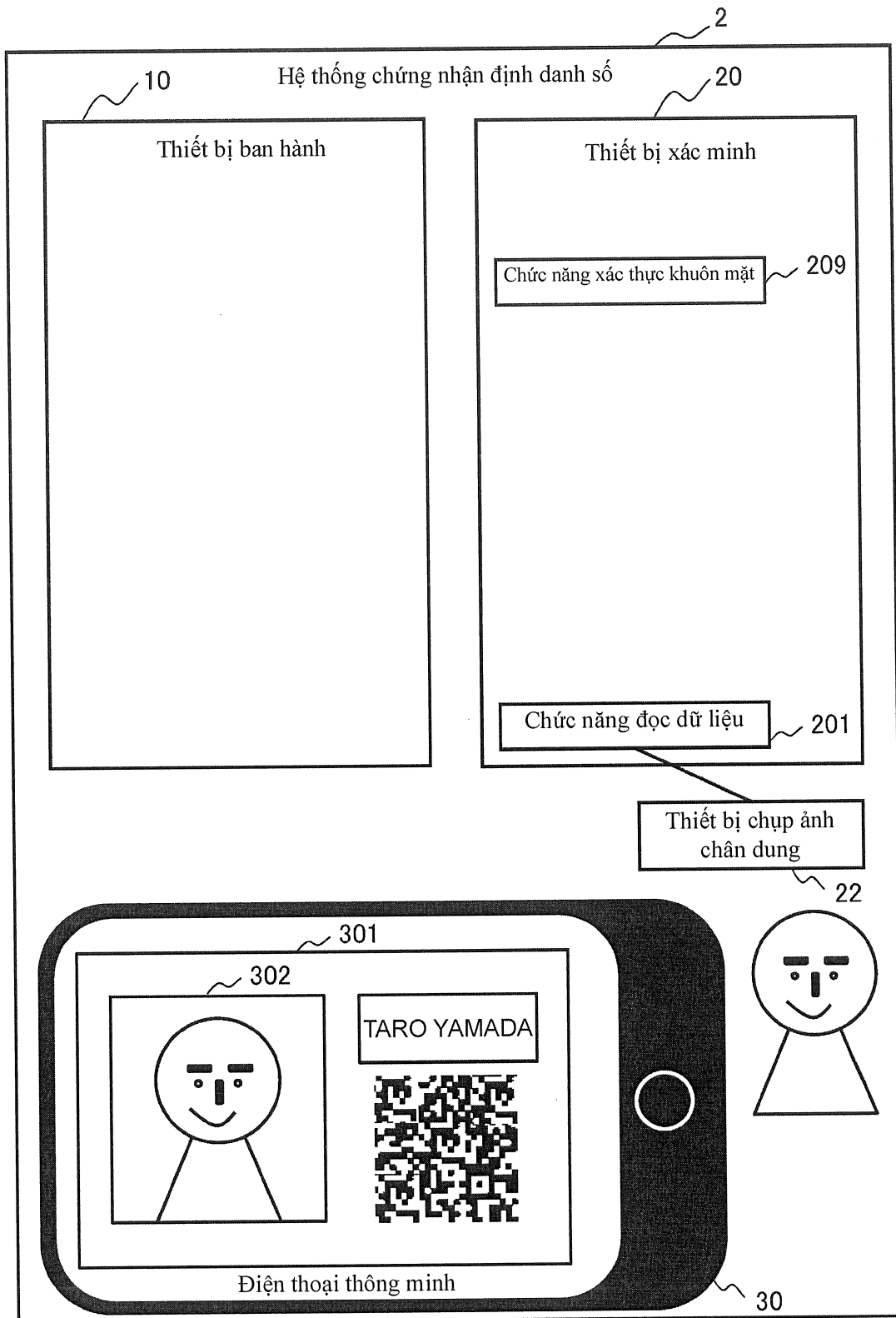
4/8

FIG.4

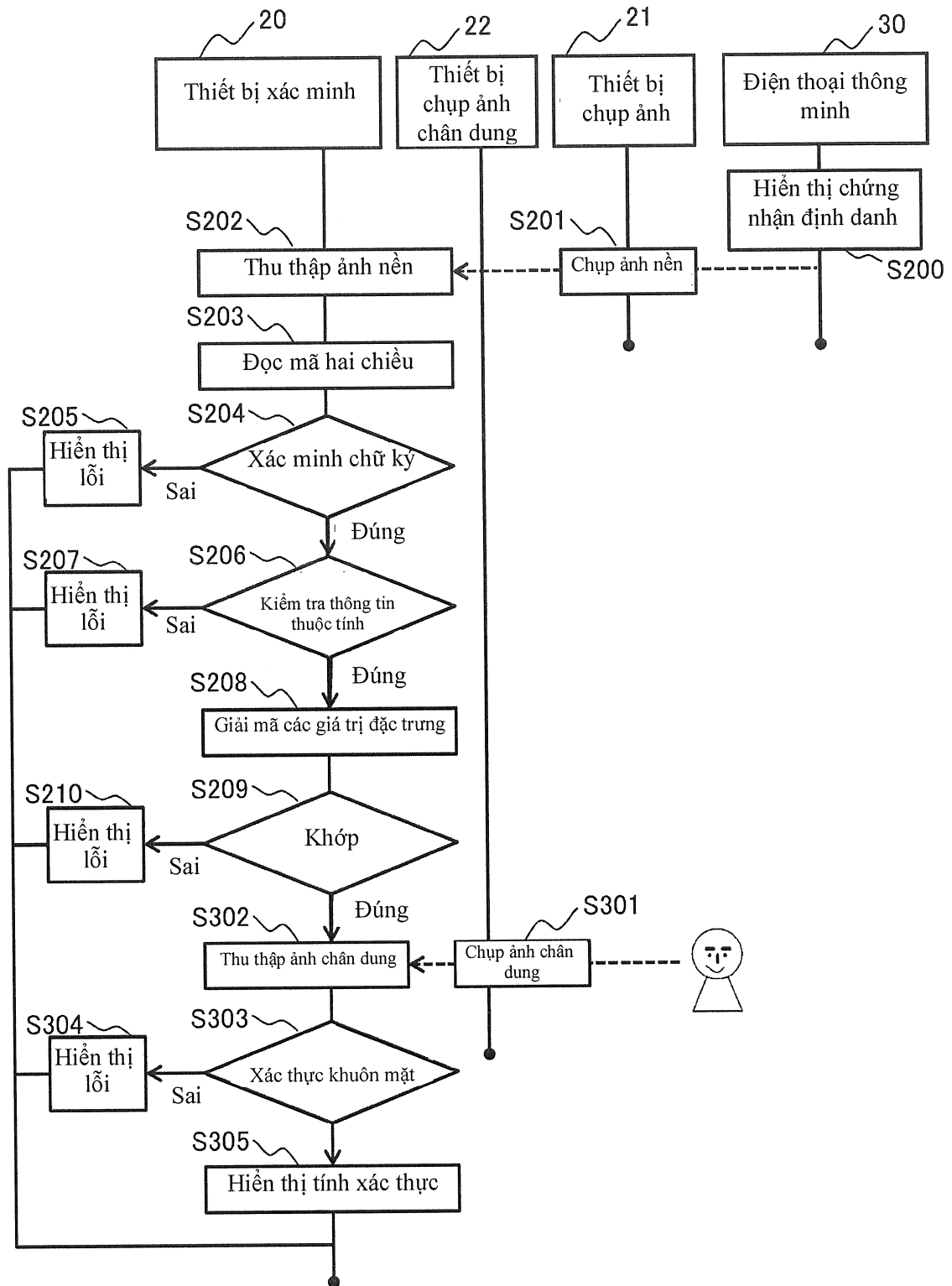
5/8

FIG. 5

6/8

FIG. 6

7/8

FIG. 7

8/8

FIG. 8