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

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

(11) **1-0047562**

(51)[2021.01] **H04L 9/08**; H04L 9/32; G06F 21/32 (13) **B**

(21) 1-2022-03202
(22) 18/09/2020
(86) PCT/JP2020/035536 18/09/2020
(87) WO2021/106334 03/06/2021
(30) 2019-216479 29/11/2019 JP
(45) 25/06/2025 447
(43) 25/08/2022 413A
(73) HITACHI, LTD. (JP)
6-6, Marunouchi 1-chome, Chiyoda-ku, Tokyo 1008280, Japan
(72) TAKAHASHI Kenta (JP).
(74) Công ty TNHH một thành viên Sở hữu trí tuệ VCCI (VCCI-IP CO.,LTD)

(54) THIẾT BỊ TẠO KHÓA, THIẾT BỊ SỬ DỤNG KHÓA VÀ PHƯƠNG PHÁP TẠO KHÓA

(21) 1-2022-03202

(57) Sáng chế đề cập đến thiết bị tạo khóa để hoàn thành việc xác thực có độ chính xác cao trong việc mã hóa sinh trắc học và việc ký sinh trắc học dựa vào các vectơ đặc điểm theo không gian O-clit nhiều chiều, trong đó thiết bị: chứa vectơ đặc điểm thứ nhất chỉ báo đặc điểm của thông tin sinh trắc học thứ nhất, và thông số để nhận dạng cách bố trí theo cách bố trí gói hình cầu với mật độ thấp hơn 1 và lớn hơn trị số định trước, hoặc cách bố trí bao phủ hình cầu với mật độ bằng hoặc lớn hơn 1 và nhỏ hơn trị số định trước, nhận dạng cách bố trí theo cách bố trí gói hình cầu hoặc cách bố trí bao phủ hình cầu dựa vào thông số; lựa chọn điểm thứ nhất được bao gồm theo cách bố trí được nhận dạng; tạo ra khóa thứ nhất bằng việc chuyển đổi thứ nhất được định trước trên điểm thứ nhất; và tạo ra, dựa vào vectơ đặc điểm thứ nhất và điểm thứ nhất, khuôn mẫu được kết hợp với thông tin sinh trắc học thứ nhất.

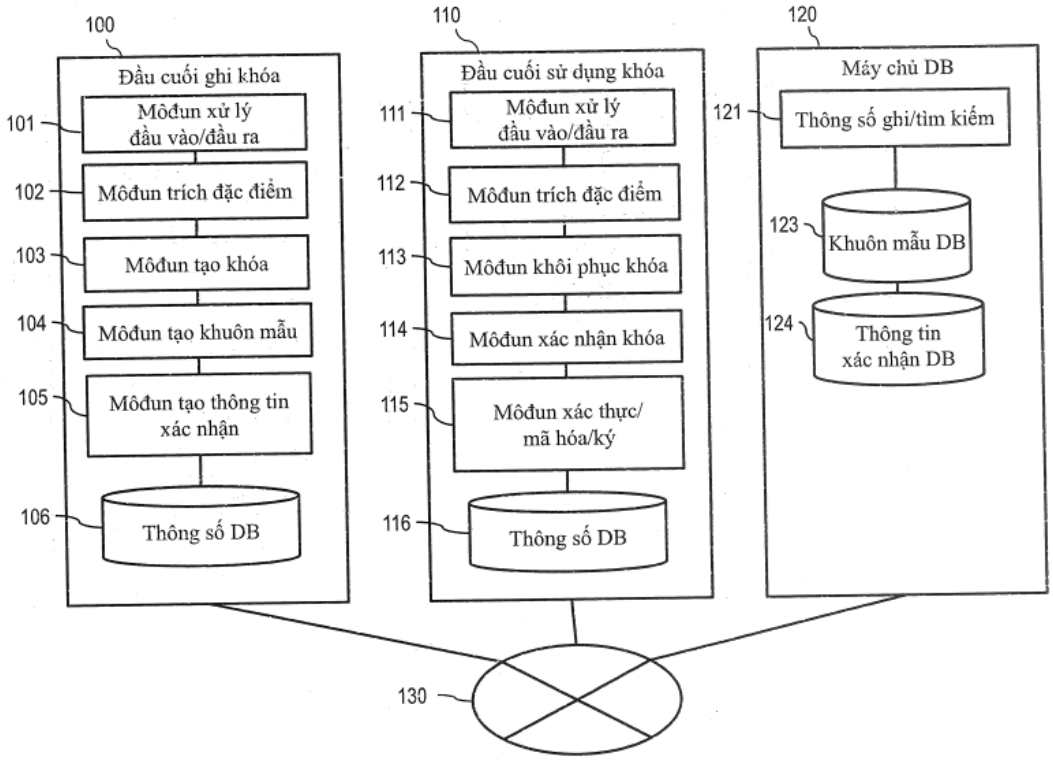

FIG. 1

Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập đến thiết bị tạo khóa, thiết bị sử dụng khóa, và phương pháp tạo khóa.

Tình trạng kỹ thuật của sáng chế

Các công nghệ xác thực sinh trắc học để xác thực cá nhân dựa vào các dấu tay, nét đặc trưng, khuôn mặt, con ngươi, hoặc các loại thông tin sinh trắc học khác được sử dụng rộng rãi. Với các công nghệ xác thực sinh trắc học thuộc lĩnh vực kỹ thuật liên quan, dữ liệu đặc điểm (khuôn mẫu) được trích từ thông tin sinh trắc học của người dùng được ghi trong hệ thống trong việc ghi người dùng, dữ liệu đặc điểm được trích lại từ thông tin sinh trắc học của người dùng được so sánh với khuôn mẫu trong việc xác thực người dùng, và việc xác thực được xác định là thành công khi khoảng cách giữa hai thông tin là đủ gần, theo cách khác, là lỗi.

Tuy nhiên, thông tin sinh trắc học thông thường là thông tin không thể thay thế được và, một khi bị rò rỉ, sẽ gây ra vấn đề nghiêm trọng. Để đề cập đến vấn đề này, khuôn mẫu bảo vệ các công nghệ xác thực sinh trắc học để thực hiện việc xác thực với thông tin sinh trắc học được giữ bí mật được nghiên cứu và phát triển. Các công nghệ này bao gồm công nghệ được gọi là sự mã hóa sinh trắc học trong đó dữ liệu khóa được tạo ra từ thông tin sinh trắc học để thực hiện việc xác thực mật mã, việc mã hóa, việc tạo chữ ký, và các loại xử lý khác.

Trong việc mã hóa sinh trắc học, dữ liệu đặc điểm X của thông tin sinh trắc học được chuyển đổi và khóa bí mật K được nhúng cũng như trong việc ghi, nhờ đó tạo khuôn mẫu T được bảo vệ. Tiếp theo, khóa bí mật K được khôi phục từ dữ liệu đặc điểm X′ của thông tin sinh trắc học được thu nhận mới và khuôn mẫu T được bảo vệ. Khi việc khôi

phục thành công, việc xác thực mật mã, việc mã hóa và việc giải mã, việc tạo chữ ký điện tử, và các loại xử lý khác có thể được thực hiện nhờ sử dụng khóa bí mật được khôi phục K. Trong việc mã hóa sinh trắc học, việc khôi phục hoặc việc suy luận của X từ T được yêu cầu là đủ khó (yêu cầu về sự an toàn). Ngoài ra, việc xử lý khôi phục khóa bí mật được yêu cầu là thành công khi, và chỉ khi, khoảng cách giữa X' và X là gần.

Các ví dụ về phương pháp thực hiện việc mã hóa sinh trắc học được mô tả trong Dodis, Y., Reyzin, L., Smith, A., "Các máy chiết mờ: Các tạo các khóa mạnh từ sinh trắc học và các dữ liệu nhiễu khác (Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data)" Trong: Cachin C., Camenisch J. L. (bài báo) Các tiến bộ trong mật mã học - EUROCRYPT 2004 (Cachin C., Camenisch J. L. (eds) Advances in Cryptology - EUROCRYPT 2004). Ghi chép bài giảng trong khoa học máy tính, tập 3027, Springer, Berlin, Heidelberg, Internet <URL: https://www.iacr.org/archive/eurocrypt2004/30270518/DRS-ec2004-final.pdf>. Các ví dụ bao gồm phương pháp khả dụng khi dữ liệu đặc điểm X và dữ liệu đặc điểm X′ được biểu diễn dưới dạng các chuỗi bit và độ tiếp cận giữa hai dữ liệu đặc điểm được định rõ bởi khoảng cách Hamming, và phương pháp khả thi khi dữ liệu đặc điểm X và dữ liệu đặc điểm X′ được biểu diễn như các tập hợp và độ tiếp cận giữa hai dữ liệu đặc điểm được định rõ bởi $|X-X'|+|X'-X|$.

Trong khi đó, trong các phương pháp nhận dạng mẫu hình mà là nền tảng của việc xác thực sinh trắc học, dữ liệu đặc điểm được biểu diễn dưới dạng vectơ theo không gian O-clit nhiều chiều, và độ tiếp cận được định rõ bởi khoảng cách O-clit hoặc khoảng cách O-clit chuẩn hóa (bao gồm khoảng cách cosin và tương quan chéo được chuẩn hóa). Ví dụ, phương pháp trích và các vectơ đặc điểm kiểm tra chéo từ hình ảnh khuôn mặt nhờ sử dụng việc học sâu và phương pháp trích và các vectơ đặc điểm kiểm tra chéo nhờ thực hiện việc phân tích thành phần chính, việc phân tích khác biệt, sự tương quan chỉ pha, hoặc tương tự trên các hình ảnh dấu tay, các hình ảnh vân tay, các hình ảnh nét đặc trưng, hoặc các hình

ảnh khác nhau có thể được coi như phương pháp trích các vectơ đặc điểm của không gian nhiều chiều từ thông tin sinh trắc học và kiểm tra chéo các vectơ đặc điểm bởi khoảng cách O-clit.

Tuy nhiên, các phương pháp như được mô tả trong "Các máy chiết mờ: Cách thức tạo các khóa mạnh từ sinh trắc học và các dữ liệu nhiễu khác (Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data)" là không thể áp dụng được cho khoảng cách O-clit. Phương pháp như được mô tả trong Yoneyama Yuta, Takahashi Kenta, Nishigaki Masakatsu, "Vấn đề vectơ gần nhất trên lưới hình tam giác và ứng dụng của nó đối với chữ ký mờ (Closest Vector Problem on Triangular Lattice and its Application to Fuzzy Signature)", các giao tác IEICE (A), quyển J98-A, số 6, trang 427-435, tháng 6 năm 2015, do đó nỗ lực để hoàn thành việc mã hóa sinh trắc học và ký sinh trắc học dựa gần như vào khoảng cách O-clit nhờ sử dụng lưới hình tam giác.

Bản chất kỹ thuật của sáng chế

Tuy nhiên, phương pháp như được mô tả trong "Vấn đề vectơ gần nhất trên lưới hình tam giác và ứng dụng của nó đối với chữ ký mờ" đã được chứng minh theo kinh nghiệm là có vấn đề về độ chính xác của việc xác thực giảm nhanh chóng (theo hàm mũ) với sự tăng theo thứ tự của số chiều. Khó hoàn thành độ chính xác thực tế của việc xác thực nhờ áp dụng phương pháp cho thông tin sinh trắc học thực tế.

Do đó, mục đích của ít nhất một khía cạnh của sáng chế này là đạt được việc xác thực có độ chính xác cao trong việc mã hóa sinh trắc học và việc ký sinh trắc học dựa vào các vectơ đặc điểm theo không gian O-clit nhiều chiều.

Để giải quyết các vấn đề, ít nhất một khía cạnh của sáng chế này áp dụng các cấu trúc dưới đây. Thiết bị tạo khóa để tạo ra khóa từ thông tin sinh trắc học, thiết bị tạo khóa bao gồm; bộ xử lý; và bộ nhớ, bộ nhớ chứa: vectơ đặc điểm thứ nhất chỉ báo đặc điểm của thông tin sinh trắc học thứ nhất; và thông số để nhận dạng cách bố trí theo cách bố trí gói

hình cầu với mật độ nhỏ hơn 1 và lớn hơn trị số định trước, hoặc cách bố trí bao phủ hình cầu với mật độ bằng hoặc lớn hơn 1 và nhỏ hơn trị số định trước, bộ xử lý được tạo kết cấu để: nhận dạng cách bố trí theo cách bố trí gói hình cầu hoặc cách bố trí bao phủ hình cầu dựa vào thông số; lựa chọn điểm thứ nhất được bao gồm trên cách bố trí được nhận dạng theo cách bố trí gói hình cầu hoặc cách bố trí bao phủ hình cầu; tạo ra khóa thứ nhất nhờ thực hiện việc chuyển đổi thứ nhất được định trước trên điểm thứ nhất; và tạo ra, dựa vào vectơ đặc điểm thứ nhất và điểm thứ nhất, khuôn mẫu được kết hợp với thông tin sinh trắc học thứ nhất.

Ít nhất một khía cạnh của sáng chế này có thể đạt được việc xác thực có độ chính xác cao trên việc mã hóa sinh trắc học và việc ký sinh trắc học dựa vào các vectơ đặc điểm theo không gian O-clit nhiều chiều.

Các vấn đề, các kết cấu, và các hiệu quả mà không được nêu trên sẽ được giải thích trong các phương án dưới đây.

Mô tả vắn tắt các hình vẽ

Sáng chế có thể được thấy rõ bởi phần mô tả mà tiếp theo kết hợp với các hình vẽ dưới đây, trong đó:

Fig.1 là sơ đồ khối minh họa kết cấu ví dụ về hệ thống xác thực sinh trắc học theo phương án thứ nhất;

Fig.2 là lưu đồ minh họa ví dụ về việc xử lý ghi khuôn mẫu và thông tin xác nhận theo phương án thứ nhất;

Fig.3 là lưu đồ minh họa ví dụ về việc xử lý xác thực theo phương án thứ nhất;

Fig.4 là lưu đồ minh họa ví dụ chi tiết về việc xử lý tạo khóa và việc xử lý tạo khuôn mẫu theo phương án thứ nhất;

Fig.5 là lưu đồ minh họa ví dụ chi tiết về việc xử lý khôi phục khóa theo phương

án thứ nhất; và

Fig.6 là sơ đồ khối minh họa kết cấu phần cứng ví dụ của các máy tính mà thiết bị đầu cuối ghi khóa, thiết bị đầu cuối sử dụng khóa, và máy chủ DB được tạo kết cấu một cách tách biệt theo phương án thứ nhất.

Mô tả chi tiết sáng chế

Dưới đây, phương án của sáng chế được giải thích dựa vào các hình vẽ. Phương án là ví dụ để đạt được sáng chế và không giới hạn phạm vi công nghệ của sáng chế. Trong các hình vẽ, kết cấu giống nhau có số chỉ dẫn giống nhau.

Phương án thứ nhất

Hệ thống xác thực sinh trắc học theo phương án thứ nhất của sáng chế này tạo ra, từ thông tin sinh trắc học của người dùng, khuôn mẫu và thông tin xác nhận để xác nhận khóa, ghi khuôn mẫu và thông tin xác nhận, khôi phục khóa nhờ sử dụng khuôn mẫu và thông tin sinh trắc học được thu nhận mới của người dùng, và sử dụng khóa để thực hiện việc xác thực người dùng, việc mã hóa và việc giải mã dữ liệu, việc tạo ra chữ ký điện tử, và tương tự.

Fig.1 là sơ đồ khối để minh họa kết cấu ví dụ về hệ thống xác thực sinh trắc học. Hệ thống xác thực sinh trắc học bao gồm, ví dụ, một, hoặc lớn hơn một, thiết bị đầu cuối ghi khóa 100, một, hoặc lớn hơn một, thiết bị đầu cuối sử dụng khóa 110, và máy chủ cơ sở dữ liệu (database, viết tắt là DB) 120, mà được ghép nối với nhau bởi mạng 130, mà là Internet hoặc tương tự.

Hai trong số hoặc tất cả ba thiết bị đầu cuối ghi khóa 100, thiết bị đầu cuối sử dụng khóa 110, và máy chủ DB 120 có thể được thực hiện trong cùng một thiết bị. Khi ba thiết bị đầu cuối này đều được thực hiện trong cùng một thiết bị, mạng 130 có thể được bỏ qua.

Thiết bị đầu cuối ghi khóa 100 tạo ra khuôn mẫu và thông tin xác nhận từ thông tin sinh trắc học của người dùng, và ghi khuôn mẫu và thông tin xác nhận. Thiết bị đầu

cuối ghi khóa 100 bao gồm, ví dụ, môđun xử lý đầu vào/đầu ra 101 mà xử lý đầu vào từ người dùng và từ các thiết bị khác cũng như đầu ra từ thiết bị khác, môđun trích đặc điểm 102 mà trích đặc điểm dữ liệu ghi từ thông tin sinh trắc học ghi được thu nhận về khuôn mặt, nét đặc trưng, và tương tự từ người dùng với bộ cảm biến, môđun tạo khóa 103 mà tạo ra khóa, môđun tạo khuôn mẫu 104 mà tạo ra khuôn mẫu từ đặc điểm dữ liệu ghi, và môđun tạo thông tin xác nhận 105 mà tạo ra thông tin xác nhận được sử dụng để xác thực độ chính xác của khóa được tạo ra bởi thiết bị đầu cuối sử dụng khóa 110 (nghĩa là, khóa được tạo ra bởi thiết bị đầu cuối ghi khóa 100 và khóa được tạo ra bởi thiết bị đầu cuối sử dụng khóa 110 khớp hay không). Thiết bị đầu cuối ghi khóa 100 cũng bao gồm môđun lưu trữ thông số 106 để giữ, trong số các thông số khác, các thông số chỉ rõ cách bố trí gói hình cầu và cách bố trí bao phủ hình cầu được mô tả sau đây.

Thiết bị đầu cuối sử dụng khóa 110 thu nhận mới thông tin sinh trắc học của người dùng, và khôi phục khóa từ thông tin sinh trắc học được thu nhận và khuôn mẫu để thực hiện người dùng việc xác thực, việc mã hóa và việc giải mã dữ liệu, việc tạo ra chữ ký điện tử, và tương tự.

Thiết bị đầu cuối sử dụng khóa 110 bao gồm môđun xử lý đầu vào/đầu ra 111 mà xử lý đầu vào từ người dùng và thiết bị khác cũng như đầu ra từ thiết bị khác, môđun trích đặc điểm 112 mà trích dữ liệu đặc điểm từ thông tin sinh trắc học được thu nhận với bộ cảm biến từ người dùng, môđun khôi phục khóa 113 mà khôi phục khóa từ dữ liệu đặc điểm và khuôn mẫu, môđun xác nhận khóa 114 mà xác thực độ chính xác của khóa, và môđun xác thực/mã hóa/ký 115 mà thực hiện việc xác thực, việc mã hóa, việc giải mã, việc tạo ra chữ ký điện tử, và các loại xử lý mật mã nhờ sử dụng khóa. Thiết bị đầu cuối sử dụng khóa 110 cũng bao gồm môđun lưu trữ thông số 116 mà giữ, trong số các thông số khác, các thông số chỉ rõ cách bố trí gói hình cầu và cách bố trí bao phủ hình cầu được mô tả sau đây.

Máy chủ DB 120 ghi và quản lý các khuôn mẫu và các đoạn thông tin xác nhận.

Máy chủ DB 120 bao gồm môđun ghi/tìm kiếm 121 mà ghi và tìm kiếm khuôn mẫu và đoạn thông tin xác nhận. Máy chủ DB 120 cũng bao gồm khuôn mẫu DB 123 trong đó các khuôn mẫu được giữ và thông tin xác nhận DB 124 trong đó các đoạn thông tin xác nhận được giữ. Khuôn mẫu DB 123 có thể giữ các ID người dùng kết hợp với các khuôn mẫu tương ứng. Thông tin xác nhận DB 124 có thể giữ các ID người dùng kết hợp với các đoạn thông tin xác nhận tương ứng.

Khuôn mẫu DB 123 và thông tin xác nhận DB 124 có thể được quản lý trên các máy chủ khác nhau hoặc các thiết bị đầu cuối khác nhau theo cách được phân phối. Việc quản lý phân phối nâng cao độ an toàn khỏi rủi ro rò rỉ nhiều hơn. Ít nhất một loại dữ liệu trong các khuôn mẫu và các đoạn thông tin xác nhận có thể được lưu trữ và được quản lý trên thiết bị đầu cuối sử dụng khóa 110. Ít nhất một loại dữ liệu trong các khuôn mẫu và các đoạn thông tin xác nhận có thể được lưu trữ và được quản lý trên thẻ IC, bộ nhớ USB, thiết bị đầu cuối cầm tay, tờ giấy mà mã hai chiều của dữ liệu được in lên, hoặc phương tiện cầm tay khác, hoặc trên điện thoại thông minh hoặc các thiết bị đầu cuối được quản lý cá nhân khác.

Fig.6 là sơ đồ khối để minh họa kết cấu phần cứng ví dụ của các máy tính mà thiết bị đầu cuối ghi khóa 100, thiết bị đầu cuối sử dụng khóa 110, và máy chủ DB 120 được tạo kết cấu một cách tách biệt. Các máy tính mà mỗi trong số đó bao gồm bộ phận xử lý trung tâm (control processing unit, viết tắt là CPU) 600, bộ nhớ 601, thiết bị lưu trữ phụ 602, thiết bị đầu vào 603, thiết bị đầu ra 604, thiết bị truyền thông 605, và bộ cảm biến 606, mà được ghép nối với nhau bởi bus hoặc đường truyền thông nội bộ tương tự. Tuy nhiên, máy tính mà máy chủ DB 120 được tạo kết cấu không được yêu cầu bao gồm bộ cảm biến 606.

CPU 600 bao gồm bộ xử lý, và thực hiện chương trình được lưu trữ trong bộ nhớ 601. Bộ nhớ 601 bao gồm ROM, mà là thiết bị bộ nhớ bất khả biến, và RAM, mà là thiết bị bộ nhớ khả biến. ROM lưu trữ, ví dụ, chương trình bất biến (ví dụ, BIOS). RAM là bộ nhớ truy cập ngẫu nhiên động (dynamic random access memory, viết tắt là DRAM) hoặc

thiết bị bộ nhớ khả biến tốc độ cao khác, và lưu trữ tạm thời chương trình được thực hiện bởi bộ xử lý và dữ liệu được sử dụng ở thời điểm thực hiện chương trình.

Thiết bị lưu trữ phụ 602 là, ví dụ, thiết bị lưu trữ từ tính (magnetic storage device, viết tắt là HDD), bộ nhớ tia chớp (flash memory, viết tắt là SSD), hoặc thiết bị lưu trữ bất khả biến dung lượng lớn khác, và lưu trữ chương trình được thực hiện bởi CPU 600 và dữ liệu được sử dụng ở thời điểm thực hiển chương trình. Nói cách khác, chương trình được đọc từ thiết bị lưu trữ phụ 602, và được tải vào bộ nhớ 601 để được thực hiện bởi CPU 600.

Mỗi trong số các máy tính có thể bao gồm giao diện đầu vào và giao diện đầu ra. Giao diện đầu vào là giao diện mà thiết bị đầu vào 603, như bàn phím và chuột, được ghép nối, và thu đầu vào từ bộ phận thao tác. Giao diện đầu ra là giao diện mà thiết bị đầu ra 604, như thiết bị hiển thị và máy in, được ghép nối, và đưa ra kết quả của việc thực hiện chương trình theo định dạng có thể nhận dạng theo bề ngoài tới bộ phận thao tác. Thiết bị truyền thông 605 là thiết bị giao diện mạng mà điều khiển truyền thông đến và từ thiết bị khác nhờ theo sau giao thức đưa ra. Bộ cảm biến 606 bộ cảm biến mà thu nhận thông tin sinh trắc học để nhận dạng người dùng (ví dụ, thiết bị chụp ảnh hoặc tai nghe). Bộ cảm biến 606 có thể được ghép nối với giao diện đầu vào thay vì được bao gồm trong mỗi trong số các máy tính.

Chương trình được thực hiện bởi CPU 600 được bố trí cho mỗi trong số các máy tính từ thiết bị lưu trữ không chuyển tiếp của thiết bị khác qua trung gian là phương tiện có thể tháo được (như CD-ROM hoặc bộ nhớ tia chớp) hoặc qua mạng 130, và được lưu trữ trong thiết bị lưu trữ phụ bất khả biến 602 là phương tiện lưu trữ không chuyển tiếp. Do đó, mỗi trong số các máy tính tốt hơn là bao gồm giao diện mà đọc dữ liệu từ phương tiện có thể tháo được.

Mỗi trong số thiết bị được bao gồm trong hệ thống xác thực sinh trắc học theo phương án thứ nhất là hệ thống máy tính về vật lý được tạo nên trên một máy tính hoặc được tạo nên trên nhiều máy tính mà được tạo kết cấu một cách logic hoặc vật lý, và có thể

được điều khiển trên các mạch riêng lẻ trên cùng máy tính, hoặc có thể hoạt động trên máy ảo được xây dựng trên nhiều tài nguyên máy tính vật lý.

Môđun trích đặc điểm 102, môđun tạo khóa 103, môđun tạo khuôn mẫu 104, và môđun tạo thông tin xác nhận 105 của thiết bị đầu cuối ghi khóa 100 được thực hiện bởi các chương trình được thực hiện bởi CPU 600 của máy tính mà thiết bị đầu cuối ghi khóa 100 được tạo kết cấu. Tương tự, môđun trích đặc điểm 112, môđun khôi phục khóa 113, môđun xác nhận khóa 114, và môđun xác thực/mã hóa/ký 115 của thiết bị đầu cuối sử dụng khóa 110 được thực hiện bởi các chương trình được thực hiện bởi CPU 600 của máy tính mà thiết bị đầu cuối sử dụng khóa 110 được tạo kết cấu. Môđun ghi/tìm kiếm 121 của máy chủ DB 120 được thực hiện một cách tương tự bởi các chương trình thực hiện bởi CPU 600 của máy tính mà máy chủ DB 120 được tạo kết cấu.

Ví dụ, CPU 600 của máy tính mà thiết bị đầu cuối ghi khóa 100 được tạo kết cấu các chức năng như môđun xử lý đầu vào/đầu ra 101 nhờ hoạt động phù hợp với chương trình xử lý đầu vào/đầu ra được tải lên bộ nhớ 601, và các chức năng như môđun trích đặc điểm 102 bởi các hoạt động phù hợp với chương trình trích đặc điểm chương trình được tải lên bộ nhớ 601. Tương tự áp dụng cho mối quan hệ giữa môđun chức năng khác được bao gồm trong thiết bị đầu cuối ghi khóa 100 và chương trình, và mối quan hệ giữa môđun chức năng được bao gồm trong thiết bị khác mà là thành phần của hệ thống xác thực và chương trình.

Môđun lưu trữ thông số 106 của thiết bị đầu cuối ghi khóa 100 được tạo kết cấu từ, ví dụ, một phần của vùng lưu trữ được bao gồm trong bộ nhớ 601, hoặc thiết bị lưu trữ phụ 602, mà là thành phần của máy tính mà thiết bị đầu cuối ghi khóa 100 được tạo kết cấu. Tương tự, môđun lưu trữ thông số 116 của thiết bị đầu cuối sử dụng khóa 110 được tạo kết cấu từ một phần của vùng lưu trữ được bao gồm trong bộ nhớ 601, hoặc thiết bị lưu trữ phụ 602, mà là thành phần máy tính mà thiết bị đầu cuối sử dụng khóa 110 được tạo kết cấu. Khuôn mẫu DB 123 và thông tin xác nhận DB 124 của máy chủ DB 120 được tạo

kết cấu tương tự từ một phần của vùng lưu trữ được bao gồm trong bộ nhớ 601, hoặc thiết bị lưu trữ phụ 602, mà là thành phần máy tính mà máy chủ DB 120 được tạo kết cấu.

Theo phương án thứ nhất, thông tin được sử dụng bởi mỗi thiết bị được bao gồm trong hệ thống xác thực không phụ thuộc vào cấu trúc dữ liệu và có thể có cấu trúc dữ liệu bất kỳ. Ví dụ, cấu trúc dữ liệu được lựa chọn một cách phù hợp từ bảng, danh sách, cơ sở dữ liệu, và hàng có thể được sử dụng để lưu trữ thông tin.

Fig.2 là lưu đồ minh họa ví dụ về việc xử lý ghi khuôn mẫu và thông tin xác nhận. Đầu tiên, môđun xử lý đầu vào/đầu ra 101 của thiết bị đầu cuối ghi khóa 100 bắt đầu việc xử lý ghi phản ứng với hoạt động được thực hiện bởi người dùng hoặc bộ phận thao tác (bước S200).

Môđun xử lý đầu vào/đầu ra 101 thu nhân thông tin sinh trắc học ghi của người dùng được thu nhận bởi bộ cảm biến 606 của thiết bị đầu cuối ghi khóa 100 (bước S201). Môđun xử lý đầu vào/đầu ra 101 có thể gán ID người dùng để nhận dạng người dùng trong việc xử lý thu nhận thông tin sinh trắc học ghi. Thuật ngữ "thông tin sinh trắc học" như được sử dụng ở đây có nghĩa là thông tin mà người dùng có thể được nhận dạng và được thu nhận từ các đặc điểm vật lý hoặc các đặc điểm hành vi của người dùng. Đây có thể là lỗi giữa các đoạn thông tin sinh trắc học được thu nhận về cùng người dùng ở các thời điểm khác nhau (thông tin sinh trắc học có thể thay đổi phụ thuộc vào tình huống, ví dụ, góc chụp ảnh hoặc tiếng ồn của bộ cảm biến 606, hoặc điều kiện của người dùng), và do đó có thể nói rằng thông tin sinh trắc học là thông tin mờ.

Các ví dụ về thông tin sinh trắc học bao gồm hình ảnh tĩnh hoặc hình ảnh động được thu nhận nhờ chụp ảnh một phần cơ thể, như khuôn mặt, bàn tay, ngón tay, mắt, các nét đặc trưng, mống mắt, hoặc võng mạc với ánh sáng có bước sóng bất kỳ được xác định trước, như ánh sáng nhìn thấy được, ánh sáng hồng ngoại, ánh sáng hồng ngoại gần, hoặc tia X, tín hiệu âm thanh của lời nói của người dùng, và các đoạn thông tin tín hiệu được thu nhận nhờ đo các phần khác nhau của cơ thể của người dùng. Dữ liệu được thu nhận

nhờ đo chữ ký viết tay, cử chỉ, và hành động là một ví dụ khác của thông tin sinh trắc học. Điều tương tự áp dụng cho thông tin sinh trắc học khôi phục khóa trong việc xử lý sử dụng khóa được mô tả sau đây.

Môđun trích đặc điểm 102 trích đặc điểm dữ liệu ghi từ thông tin sinh trắc học ghi được thu nhận ở bước S201 (bước S202). Định dạng mà đặc điểm dữ liệu ghi được biểu diễn dưới dạng, ví dụ, hình ảnh, vectơ, tín hiệu, hoặc một hoặc nhiều hơn các trị số bằng số. Điều tương tự áp dụng cho dữ liệu đặc điểm khôi phục khóa trong việc xử lý sử dụng khóa được mô tả sau đây.

Môđun tạo khóa 103 tạo ra khóa sk từ đặc điểm dữ liệu ghi được trích ở bước S202 (bước S203). Khóa sk có thể là chuỗi bit có độ dài được xác định trước, số nguyên với số lượng chữ số được xác định trước, hoặc vectơ hoặc ma trận với số lượng chiều được xác định trước. Các chi tiết về bước xử lý ở bước S203 được mô tả sau đây.

Môđun tạo khuôn mẫu 104 tạo ra khuôn mẫu T từ đặc điểm dữ liệu ghi được tạo ra ở bước S202 (bước S204). Các chi tiết về bước xử lý của bước S204 được mô tả sau đây. Bước xử lý ở bước S204 có thể được thực hiện trước bước xử lý ở bước S203, hoặc có thể được thực hiện sau bước xử lý của bước S205.

Môđun tạo thông tin xác nhận 105 tạo ra thông tin xác nhận vk từ khóa sk được tạo ra ở bước S203 (bước S205). Ví dụ chi tiết về bước xử lý của bước S205 được mô tả dưới đây.

Như ví dụ thứ nhất về phương pháp tạo thông tin xác nhận vk từ khóa sk, môđun tạo thông tin xác nhận 105 tính biểu thức 1 nhờ sử dụng hàm một chiều Hash () được xác định trước.

vk=Hash(sk) ... (Biểu thức 1)

SHA256, SHA3, hoặc hàm hash mã hóa bất kỳ khác là ví dụ của Hash(). Hàm hash tuyến tính cũng là ví dụ của Hash().

Như ví dụ thứ hai về phương pháp tạo thông tin xác nhận vk từ khóa sk, môđun tạo thông tin xác nhận 105 tính biểu thức 2 nhờ sử dụng nhóm vòng G = <g> ("g" là hàm sinh của G) và ánh xạ φ từ tập hợp mà khóa sk thuộc về đến tập hợp tất cả các số nguyên.

vk=g^φ(sk) ... (Biểu thức 2)

Các cặp (sk, vk) được tạo nên theo cách này có thể được sử dụng như các cặp khóa bí mật và khóa công khai trong nhiều thuật toán mã hóa khóa công khai/chữ ký điện tử, như thuật toán mã hóa ElGamal/chữ ký, thuật toán chữ ký số (digital signature algorithm, viết tắt là DSA), và thuật toán chữ ký Schnorr, hoặc các thuật toán mã hóa ElGamal cong eliptic/chữ ký, DSA cong eliptic, và thuật toán chữ ký Schnorr cong eliptic.

Như ví dụ thứ ba về phương pháp tạo thông tin xác nhận vk từ khóa sk, môđun tạo thông tin xác nhận 105 tính biểu thức 3 nhờ sử dụng khóa bí mật được xác định trước cho việc tạo thông tin xác nhận ngoài khóa sk, hoặc thông số (p) tạo thông tin xác nhận.

vk=Enc(sk, p) ... (Biểu thức 3)

AES, RSA, hoặc hàm mã hóa bất kỳ khác, và hàm hash có khóa đều là ví dụ của Enc().

Khóa bí mật tạo thông tin xác nhận hoặc thông số (p) tạo thông tin xác nhận có thể được thiết đặt cho mỗi người dùng hoặc cho mỗi đoạn của thông tin sinh trắc học được ghi bởi môđun tạo thông tin xác nhận 105, hoặc có được thiết đặt cho mỗi thiết bị đầu cuối sử dụng khóa 110 hoặc cho mỗi hệ thống xác thực sinh trắc học bởi môđun tạo thông tin xác nhận 105, hoặc có thể được thiết đặt trước. Tập hợp thông số (p) được lưu trữ trong môđun lưu trữ thông số 106.

Cuối cùng, môđun xử lý đầu vào/đầu ra 101 ghi khuôn mẫu T trong khuôn mẫu DB 123 của máy chủ DB 120, và ghi thông tin xác nhận vk trong thông tin xác nhận DB 124 của máy chủ DB 120 (bước S206). Khi bước S200 bao gồm bước gán ID người dùng, môđun xử lý đầu vào/đầu ra 101 ghi khuôn mẫu T kết hợp với ID người dùng trong khuôn

mẫu DB 123, và ghi thông tin xác nhận vk kết hợp với ID người dùng trong thông tin xác nhận DB 124 của máy chủ DB 120.

Fig.3 là lưu đồ minh họa ví dụ về việc xử lý xác thực. Đầu tiên, môđun xử lý đầu vào/đầu ra 111 của thiết bị đầu cuối sử dụng khóa 110 khởi động việc xử lý xác thực phản ứng với hoạt động được thực hiện bởi người dùng hoặc bộ phận thao tác (bước S300). Môđun xử lý đầu vào/đầu ra 111 thu nhận thông tin sinh trắc học xác thực được thu nhận về người dùng bởi bộ cảm biến 606 của thiết bị đầu cuối sử dụng khóa 110 (bước S301). Trong trường hợp về việc xác thực 1:1, môđun xử lý đầu vào/đầu ra 111 cũng thu đầu vào của ID người dùng từ người dùng ở bước S301. Phần mô tả dưới đây xử lý trường hợp trong đó việc xác thực 1:1 được thực hiện.

Môđun trích đặc điểm 112 trích dữ liệu đặc điểm xác thực từ thông tin sinh trắc học xác thực được thu nhận ở bước S301 (bước S302). Dữ liệu đặc điểm xác thực được trích bằng phương pháp giống như phương pháp trích ở bước S202.

Môđun xử lý đầu vào/đầu ra 111 yêu cầu máy chủ DB 120 tìm kiếm khuôn mẫu DB 123 cho khuôn mẫu T mà được kết hợp với ID người dùng được thu nhận ở bước S301, và đọc khuôn mẫu T được kết hợp trong khuôn mẫu DB 123, môđun ghi/tìm kiếm 121 của máy chủ DB 120 đọc khuôn mẫu T và truyền khuôn mẫu T được đọc đến thiết bị đầu cuối sử dụng khóa 110, và môđun khôi phục khóa 113 khôi phục khóa sk′ từ khuôn mẫu T được nhận và từ dữ liệu đặc điểm xác thực (bước S303). Các chi tiết về bước xử lý của bước S303 được mô tả sau đây.

Môđun xử lý đầu vào/đầu ra 111 yêu cầu máy chủ DB 120 tìm kiếm thông tin xác nhận DB 124 cho đoạn thông tin xác nhận vk mà được kết hợp với ID người dùng được thu nhận ở bước S301, và đọc đoạn thông tin xác nhận vk được kết hợp trong thông tin xác nhận DB 124, môđun ghi/tìm kiếm 121 của máy chủ DB 120 đọc đoạn thông tin xác nhận vk được kết hợp và truyền đoạn thông tin xác nhận vk được đọc đến thiết bị đầu cuối sử dụng khóa 110, và môđun xác nhận khóa 114 xác thực độ chính xác của khóa sk′ (nghĩa là,

sk′=sk được thiết lập hay không) nhờ sử dụng đoạn được nhận của thông tin xác nhận vk (bước S304).

Ví dụ chi tiết về bước xử lý của bước S304 được mô tả dưới đây. Ở bước xử lý của bước S304, môđun xác nhận khóa 114 tạo ra vk′ từ sk′ bằng phương pháp giống như ở bước xử lý của bước S205 nêu trên, và xác định vk′ và vk khớp nhau hay không bằng cách so sánh. Cụ thể, khi phương pháp của ví dụ thứ nhất được sử dụng ở bước S205, môđun xác nhận khóa 114 tính vk′=Hash(sk′).

Khi phương pháp của ví dụ thứ hai được sử dụng ở bước S205, môđun xác nhận khóa 114 tính vk′=g^φ(sk′). Khi phương pháp của ví dụ thứ ba được sử dụng ở bước S205, môđun xác nhận khóa 114 tính vk′=Enc(sk′, p) (tuy nhiên, trị số giống như trị số ở bước S205 được sử dụng cho khóa bí mật tạo thông tin xác nhận hoặc thông số (p) tạo thông tin xác nhận).

Phương pháp bất kỳ của ví dụ thứ nhất, phương pháp của ví dụ thứ hai, và phương pháp của ví dụ thứ ba được sử dụng ở bước S205, thông tin về phương pháp được sử dụng được chia sẻ trước giữa thiết bị đầu cuối ghi khóa 100 và thiết bị đầu cuối sử dụng khóa 110. Khi phương pháp của ví dụ thứ ba được sử dụng ở bước S205, khóa bí mật tạo thông tin xác nhận hoặc thông số (p) tạo thông tin xác nhận được chia sẻ trước giữa thiết bị đầu cuối ghi khóa 100 và thiết bị đầu cuối sử dụng khóa 110.

Khi việc xác nhận bởi môđun xác nhận khóa 114 ở bước S304 là thành công (nghĩa là, khi sk′ được xác định là bằng sk), môđun xác thực/mã hóa/ký 115 thực hiện, ví dụ, việc xử lý xác thực, việc xử lý mã hóa, và/hoặc việc xử lý ký được yêu cầu bởi người dùng hoặc bộ phận thao tác, nhờ sử dụng khóa sk′ (=sk) (bước S305).

Khi việc xử lý xác thực được thực hiện, môđun xác thực/mã hóa/ký 115 tạo ra, cho, ví dụ, mã thách thức được xác định trước, chữ ký điện tử hoặc mã xác thực tin nhắn (message authentication code, viết tắt là MAC) với sk′ dưới dạng khóa bí mật. Khi việc xử

lý mã hóa được thực hiện, môđun xác thực/mã hóa/ký 115 mã hóa, ví dụ, dữ liệu tin nhắn được xác định trước với sk′ dưới dạng khóa mã hóa, và giải mã dữ liệu được mã hóa được xác định trước với sk′ dưới dạng khóa giải mã. Khi việc ký điện tử được thực hiện, môđun xác thực/mã hóa/ký 115 tạo ra, cho, ví dụ, dữ liệu được xác định trước, chữ ký điện tử với sk′ như khóa ký.

Fig.4 là lưu đồ minh họa ví dụ chi tiết về việc xử lý tạo khóa ở bước S203 và việc xử lý tạo khuôn mẫu ở bước S204. Các bước từ bước S400 đến bước S404 là các bước xử lý được bao gồm ở bước S203, và bước S405 là bước xử lý được bao gồm ở bước S204.

Môđun tạo khóa 103 của thiết bị đầu cuối ghi khóa 100 đọc thông số bố trí gói hình cầu hoặc thông số bố trí bao phủ hình cầu trong môđun lưu trữ thông số 106 (bước S400). Thuật ngữ "thông số bố trí gói hình cầu" nghĩa là thông số định rõ cách bố trí gói hình cầu cụ thể, và thuật ngữ "thông số bố trí bao phủ hình cầu" nghĩa là thông số định rõ cách bố trí bao phủ hình cầu cụ thể.

Cách bố trí gói hình cầu là cách bố trí trong đó, đối với mỗi điểm S_i của tập hợp đếm được L = {S_i | i=0, 1, 2 ...} theo không gian O-clit n chiều, siêu cầu n chiều có bán kính được xác định trước "r" (ví dụ, r=1) được tạo nên mà ở điểm S_i tạo nên tập hợp các siêu cầu n chiều, theo cách tránh khỏi việc chồng lấn giữa siêu cầu được tạo nên ở một điểm S_i và siêu cầu được tạo nên ở điểm S_i khác.

Cách bố trí bao phủ hình cầu là cách bố trí trong đó, đối với mỗi điểm S_i của tập hợp đếm được L = {S_i | i=0, 1, 2 ...} theo không gian O-clit n chiều, siêu cầu n chiều có bán kính được xác định trước "r" được tạo nên ở điểm S_i tạo nên tập hợp các siêu cầu n chiều, và tập hợp các siêu cầu n chiều phủ toàn bộ không gian n chiều mà không có khe hở. Số lượng chiều n ở đây là giống như số lượng chiều n của vectơ đặc điểm được mô tả sau đây, ví dụ, khoảng vài chục đến vài chục nghìn. Trong phần mô tả dưới đây, cách bố trí gói hình cầu hoặc cách bố trí bao phủ hình cầu có thể được đề cập một cách đơn giản như "cách bố trí."

Khi cách bố trí L = {S_i} có cấu trúc về mặt toán học là lưới, L được gọi là cách bố trí lưới. Cách bố trí lưới có thể được định rõ với ma trận cơ bản B của không gian mà lưới thuộc về, và ma trận cơ bản B do đó có thể được sử dụng như thông số bố trí gói hình cầu hoặc thông số bố trí bao phủ hình cầu.

Theo cách bố trí, phần thể tích của các hình cầu (trong trường hợp về cách bố trí bao phủ hình cầu, thể tích của các phần chồng lấn của các hình cầu được cộng theo phép nhân) tới không gian được gọi là "mật độ." Mật độ theo cách bố trí gói hình cầu là trị số lớn hơn 0 và bằng hoặc nhỏ hơn 1, và mật độ theo cách bố trí bao phủ hình cầu là trị số bằng hoặc lớn hơn 1. Cách bố trí gói hình cầu với mật độ lớn nhất được gọi là "cách bố trí gói hình cầu đặc nhất," và cách bố trí bao phủ hình cầu với mật độ thấp nhất (thưa nhất) được gọi là "cách bố trí bao phủ hình cầu thưa nhất."

Cách bố trí gói hình cầu đặc nhất và cách bố trí bao phủ hình cầu thưa nhất theo không gian n chiều thay đổi phụ thuộc vào số lượng chiều n. Các phương pháp cụ thể của việc tạo kết cấu cách bố trí gói hình cầu đặc nhất và cách bố trí bao phủ hình cầu thưa nhất được biết đến bởi một số trị số của số lượng chiều n. Ví dụ, khi số lượng chiều n là 24, cách bố trí được gọi là lưới Leech được biết đến là cách bố trí gói hình cầu đặc nhất.

Các phương pháp khác nhau về cách thức tạo kết cấu cách bố trí gói hình cầu đặc, mặc dù không phải cách bố trí đặc nhất, và cách thức tạo kết cấu cách bố trí bao phủ hình cầu thưa, mặc dù không phải cách bố trí thưa nhất, được biết đến bởi các không gian của thứ tự cao hơn của các chiều. Ví dụ, cách bố trí được gọi là lưới Barnes-Wall (lưới BW) được biết đến như phương pháp tạo kết cấu cách bố trí gói hình cầu đặc.

Phương án thứ nhất sử dụng cách bố trí gói hình cầu với mật độ nhỏ hơn 1 và lớn hơn trị số định trước (trị số định trước có thể thay đổi phụ thuộc vào số lượng chiều của không gian), hoặc cách bố trí bao phủ hình cầu với mật độ bằng hoặc lớn hơn 1 và nhỏ hơn trị số định trước (trị số định trước có thể thay đổi phụ thuộc vào số lượng chiều của không gian). Các cách bố trí này do đó được tạo kết cấu trước và các thông số định rõ các cách

bố trí được tạo kết cấu được lưu trữ trong môđun lưu trữ thông số 106 và môđun lưu trữ thông số 116. Do đặc điểm này, việc mã hóa sinh trắc học và việc ký sinh trắc học nhờ sử dụng vectơ đặc điểm theo không gian O-clit nhiều chiều là khó với lĩnh vực kỹ thuật liên quan được hoàn thành với độ chính xác cao. Lý do cho điều này được mô tả sau đây.

Trong " Vấn đề vectơ gần nhất trên lưới hình tam giác và ứng dụng của nó đối với chữ ký mờ," được bộc lộ rằng phương pháp của việc ký sinh trắc học nhờ sử dụng lưới hình tam giác. Tuy nhiên, lưới hình tam giác không đặc như cách bố trí gói hình cầu và không thưa như cách bố trí bao phủ hình cầu theo không gian nhiều chiều (n là hàng chục hoặc lớn hơn). Ứng dụng của lưới hình tam giác vào thông tin sinh trắc học thực tế do đó gây ra sự giảm đáng kể về độ chính xác và do đó là không thực tế.

Cách bố trí L = {S_i | i=0, 1, 2 ...} và cách bố trí t·L = {t·S_i | i=0, 1, 2 ...}, mà là phiên bản tỷ lệ của cách bố trí L được thu nhận bằng cách nhân với "t" ("t" là số thực dương), có cùng mật độ bất kể trị số của "t."

Theo phương án thứ nhất, "t" cũng đóng vai trò "trị số ngưỡng xác thực" trong các hệ thống xác thực sinh trắc học thông thường, và các khả năng được chấp nhận là cao hơn đối với người dùng xác thực cũng như người khác ở trị số lớn hơn của "t," với trị số nhỏ hơn của "t" tăng các khả năng từ chối đối với người khác cũng như người dùng xác thực. Mỗi thông số bố trí gói hình cầu hoặc mỗi thông số bố trí bao phủ hình cầu có thể bao gồm thông tin của "t." Khi trị số ngưỡng xác thực "t" được thay đổi từ người dùng sang người dùng khác (ví dụ, người dùng định rõ trị số của "t" khi thông tin sinh trắc học được thu nhận trong việc xử lý ghi khuôn mẫu), "t" có thể được bao gồm trong khuôn mẫu T.

Tiếp theo, môđun tạo khóa 103 biến đổi và chuẩn hóa đặc điểm dữ liệu ghi để tạo ra vectơ đặc điểm ghi X = (X_1 ... X_n) (bước S401). Vectơ X là vectơ theo không gian O-clit n chiều, và khoảng cách "d" (X, X′) từ vectơ đặc điểm khôi phục khóa X′ = (X′_1 ... X′_n) được mô tả sau đây được định rõ bởi khoảng cách O-clit được biểu diễn như bởi biểu thức 4.

d(X, X′)=((X_1−X′)^2+...+(X_n−X′_n)^2)^(1/2) ... (Biểu thức 4)

Như ví dụ về phương pháp tạo vectơ đặc điểm theo không gian O-clit n chiều, phương pháp trong đó các phương pháp học sâu, phân tích thành phần chính, phân tích khác biệt, và các phương pháp học máy khác được sử dụng để tạo ra vectơ đặc điểm từ thông tin sinh trắc học hoặc từ dữ liệu đặc điểm, hoặc để nghiên cứu máy trích vectơ đặc điểm được biến đến. Nói chung, số lượng chiều n của vectơ đặc điểm được yêu cầu là hàng chục đến hàng chục nghìn để hoàn thành độ chính xác thực tế của việc xác thực, và lưu ý rằng việc xử lý không gian O-clit nhiều chiều theo đó là điều kiện cần thiết.

Môđun tạo khóa 103 lựa chọn điểm S từ cách bố trí L = {S_i | i=0, 1, 2 ...} được định rõ bởi thông số bố trí gói hình cầu hoặc thông số bố trí bao phủ hình cầu (bước S402). Như phương pháp cụ thể của việc lựa chọn điểm S, môđun tạo khóa 103 có thể sử dụng, ví dụ, một trong các phương pháp dưới đây.

(a) Môđun tạo khóa 103 lựa chọn S ngẫu nhiên phù hợp với sự phân phối được xác định trước được định rõ trong L. Sự phân phối này có thể là, ví dụ, sự phân phối thường riêng biệt với L như sự hỗ trợ, hoặc sự phân phối đều trong tập hợp con hữu hạn được xác định trước của L.

(b) Môđun tạo khóa 103 lựa chọn điểm gần nhất với vectơ đặc điểm ghi X (dưới đây được gọi là "điểm lân cận gần nhất của X") trong L.

(c) Khi L là cách bố trí lưới, môđun tạo khóa 103 tính vectơ Y = B^(−1)X bằng cách nhân X với ma trận nghịch đảo của ma trận cơ bản B của cách bố trí lưới. Môđun tạo khóa 103 tính, dưới dạng Z, vectơ nguyên nhờ làm tròn xuống hoặc lên mỗi thành phần của Y đến số nguyên gần nhất. Môđun tạo khóa 103 chọn, dưới dạng S, vectơ S = BZ, mà được thu nhận nhờ nhân ma trận cơ bản B với vectơ nguyên Z.

Khi môđun tạo khóa 103 sử dụng phương pháp (b) hoặc phương pháp (c), trị số tuyệt đối của mỗi thành phần của vectơ vi phân D, mà được mô tả dưới đây và được tính

bởi biểu thức 8, là nhỏ hơn khi phương pháp (a) được sử dụng. Kích thước dữ liệu của khuôn mẫu T do đó nhỏ hơn khi môđun tạo khóa 103 sử dụng phương pháp (b) hoặc (c) khi phương pháp (a) được sử dụng, với kết quả mà việc ghi hiệu quả được hoàn thành.

Môđun tạo khóa 103 tiếp theo tạo ra trị số được gọi là salt (bước S403). Môđun tạo khóa 103 có thể tạo ra, ví dụ, chuỗi ký tự hoặc chuỗi bit mà có độ dài được xác định trước, hoặc trị số bằng số ngẫu nhiên trong khoảng được xác định trước, như salt. Môđun tạo khóa 103 cũng có thể sử dụng, như salt, ID người dùng, trị số đếm, hoặc trị số khác mà thay đổi từ người dùng đến người dùng khác hoặc từ một đoạn của thông tin sinh trắc học được ghi đến đoạn khác của thông tin sinh trắc học được ghi. Salt được mong muốn có độ dài (s bit) mà tấn công lực mạnh là khó, ví dụ, khoảng 128 bit (s=128) hoặc lớn hơn.

Môđun tạo khóa 103 không được yêu cầu thực hiện bước xử lý của bước S403 và, trong trường hợp này, salt không được yêu cầu được sử dụng trong việc xử lý tiếp theo. Trong trường hợp này, salt trong việc xử lý tiếp theo được đọc như chuỗi ký tự hoặc chuỗi bit mà có độ dài là 0.

Môđun tạo khóa 103 sau đó tạo ra khóa sk từ điểm S và salt (bước S404). Cụ thể, môđun tạo khóa 103 tính sk bằng biểu thức 5 nhờ sử dụng hàm một chiều Hash (), ví dụ, SHA256 hoặc SHA3.

sk=Hash(S||salt) ... (Biểu thức 5)

Trong biểu thức, || chỉ báo sự ghép dữ liệu. Môđun tạo khóa 103 có thể sử dụng hàm hash tuyến tính để tính sk. Môđun tạo khóa 103 cũng có thể tính sk bằng biểu thức 6, mà sử dụng AES hoặc hàm mã hóa khác hoặc hàm hash có khóa Enc() và thông số (p) được xác định trước.

sk=enc(s||salt, p) ... (Biểu thức 6)

Môđun tạo khóa 103 cũng có thể tính sk bằng biểu thức 7, mà sử dụng hàm tuyến tính "f" và ánh xạ phù hợp "g."

sk=f(S)+g(salt) ... (Biểu thức 7)

Điều này kết thúc phần mô tả ví dụ chi tiết về việc xử lý tạo khóa ở bước S203.

Ví dụ chi tiết về bước tạo khuôn mẫu (bước S204) được mô tả tiếp theo. Môđun tạo khuôn mẫu 104 tính vectơ vi phân D, mà được thu nhận bằng cách trừ vectơ đặc điểm ghi X cho điểm S, nhờ sử dụng biểu thức 8 để tạo ra khuôn mẫu T = (D, salt) trong đó D và salt được ghép cặp (bước S405).

D=X−S ... (Biểu thức 8)

Môđun tạo khuôn mẫu 104 có thể tính D dưới dạng S+X hoặc dưới dạng S−X.

Fig.5 là lưu đồ minh họa ví dụ chi tiết về việc xử lý khôi phục khóa ở bước S303. Môđun khôi phục khóa 113 của thiết bị đầu cuối sử dụng khóa 110 đọc thông số bố trí gói hình cầu hoặc thông số bố trí bao phủ hình cầu (thông số cho cách bố trí được sử dụng bởi thiết bị đầu cuối ghi khóa 100 trong việc tạo khóa và việc tạo khuôn mẫu) trong môđun lưu trữ thông số 116 (bước S500). Thông tin chỉ báo mà cách bố trí gói hình cầu và cách bố trí bao phủ hình cầu được sử dụng bởi thiết bị đầu cuối ghi khóa 100 trong việc tạo khóa và việc tạo khuôn mẫu đọc chia sẻ trước với thiết bị đầu cuối sử dụng khóa 110.

Môđun khôi phục khóa 113 biến đổi và chuẩn hóa dữ liệu đặc điểm xác thực để tạo ra vectơ đặc điểm xác thực X′ = (X′_1 ... X′_n) (bước S501). Môđun khôi phục khóa 113 tính điểm R từ việc xác thực vectơ đặc điểm X′ và từ khuôn mẫu T = (D, salt) (bước S502). Cụ thể, môđun khôi phục khóa 113 tính điểm R nhờ tính, ví dụ, biểu thức 9.

R=X′−D ... (Biểu thức 9)

Từ biểu thức 8 và biểu thức 9, biểu thức 10 được thiết lập.

R=X′−(X−S)=S+(X′−X) ... (Biểu thức 10)

Môđun khôi phục khóa 113 tìm kiếm cách bố trí L cho điểm lân cận gần nhất S′ của điểm R (bước S503). Từ biểu thức 10, điểm lân cận gần nhất S′ của điểm R được mong

chờ sẽ khớp với S khi X′−X là vectơ đủ ngắn, nghĩa là, khi việc xác thực vectơ đặc điểm X′ là đủ gần với vectơ đặc điểm ghi X. Khi X′ không gần với X, mặt khác, S′ và S được mong chờ sẽ khác nhau. Mong chờ rằng S′=S sẽ được thiết lập khi thông tin sinh trắc học xác thực là thông tin của người được ghi, và không được thiết lập trong trường hợp của người khác.

Môđun khôi phục khóa 113 tạo ra khóa sk′ từ điểm S′ và từ salt được bao gồm trong khuôn mẫu T = (D, salt) (bước S504). Phương pháp cụ thể của việc tạo khóa sk′ là giống như phương pháp tạo khóa sk ở bước S404. Được mong chờ rằng sk=sk′ sẽ được thỏa mãn khi S′=S được thiết lập, và sk=sk′ không được thỏa mãn khi S′=S không được thiết lập. Do đó, khóa chỉnh sửa có thể được lưu trữ lại chỉ khi thông tin sinh trắc học xác thực được đưa vào bởi người dùng chính xác.

Trong trường hợp về việc xác thực1:N, môđun xử lý đầu vào/đầu ra 111 không thu nhận ID người dùng ở bước S301, và, ví dụ, thu nhận mọi khuôn mẫu T từ khuôn mẫu DB 123 của máy chủ DB 120 ở bước S303. Môđun xử lý đầu vào/đầu ra 111 còn thu nhận, ở bước S304, mọi đoạn thông tin xác nhận từ thông tin xác nhận DB 124 của máy chủ DB 120. Ví dụ, quy trình của bước S303 được thực hiện đối với mỗi và mọi khuôn mẫu T một cách tách biệt, và bước xử lý của bước S304 được thực hiện đối với mỗi và mọi đoạn thông tin xác nhận một cách tách biệt.

Như được nêu trên, hệ thống xác thực theo phương án thứ nhất khác biệt nhờ sử dụng cách bố trí gói hình cầu mật độ cao hoặc cách bố trí bao phủ hình cầu mật độ thấp, và do đó có hiệu quả trong đó độ chính xác của việc xác thực cao hơn trong các phương pháp mã hóa sinh trắc học và các phương pháp việc lý sinh trắc học của lĩnh vực kỹ thuật liên quan được hoàn thành. Lý do cho điều này được mô tả dưới đây.

Điều kiện để được thỏa mãn bởi vectơ đặc điểm xác thực X′ để được chấp nhận là đặc điểm của người được ghi được định rõ từ lúc bắt đầu là bằng hoặc nhỏ hơn trị số ngưỡng được xác định trước "r" xét về khoảng cách O-clit d (X, X′) từ vectơ đặc điểm ghi

X. Nói cách khác, tập hợp các trị số có thể chấp nhận được của X′ (diện tích có thể chấp nhận được) là siêu cầu có bán kính "r" và định tâm ở X theo không gian n chiều.

Trong khi đó, trong việc xử lý tạo khóa trong việc mã hóa sinh trắc học và việc ký sinh trắc học theo phương án thứ nhất, khóa chỉnh sửa sk được lưu trữ lại và người được xác thực được chấp nhận là người được ghi khi và chỉ khi điểm lân cận gần nhất của điểm $R = S+(X'-X)$ của biểu thức 10 theo cách bố trí $L = \{S_i \mid i=0, 1, 2 ...\}$ theo không gian n chiều là S. Khi diện tích trong đó S điểm lân cận gần nhất (ô Voronoi của S) theo không gian n chiều được cho là V(S), điều kiền cần và đủ để X′ được chấp nhận có thể được biểu diễn như bởi biểu thức 11.

$$S+X'-X\in V(S)\Leftrightarrow X'\in X-S+V(S) \quad \text{... (Biểu thức 11)}$$

Trong biểu thức 11, X−S+V(S) ở bên phải của biểu thức là diện tích đạt được bởi trục song song của V(S) bởi X−S. Khi V(S) được giả sử là siêu cầu định tâm ở S và có bán kính "r," bên phải là siêu cầu định tâm ở X và có bán kính "r." Điều này khớp với diện tích có thể chấp nhận được nêu trên dựa vào khoảng cách O-clit và cũng khớp với độ chính xác của việc xác thực, và không có sự giảm về độ chính xác do đó được gây ra. Tuy nhiên, xét về mỗi điểm S theo cách bố trí L, ô Voronoi của điểm S thông thường không khớp với siêu cầu và độ chính xác giảm. Nói chung, độ lớn của sự giảm về độ chính xác là lớn hơn khi diện tích trong đó siêu cầu và ô Voronoi không khớp là lớn hơn.

Ô Voronoi của mỗi điểm theo cách bố trí gói hình cầu về các siêu cầu đều có bán kính "r" bao gồm, bởi định nghĩa, siêu cầu có bán kính "r." Khi mật độ của chúng là cao hơn, diện tích trong đó ô Voronoi và siêu cầu không khớp là nhỏ hơn và độ lớn của sự giảm về độ chính xác do đó nhỏ hơn. Tương tự, ô Voronoi của mỗi điểm theo cách bố trí bao phủ hình cầu về các siêu cầu đều có bán kính "r" được bao gồm trong siêu cầu có bán kính "r." Khi mật độ của chúng là thấp hơn, diện tích trong đó ô Voronoi và siêu cầu không khớp là nhỏ hơn và độ lớn của sự giảm về độ chính xác do đó nhỏ hơn.

Với các công nghệ mã hóa sinh trắc học và các công nghệ việc ký sinh trắc học của lĩnh vực kỹ thuật liên quan, ví dụ, phương pháp như được mô tả trong "Các máy chiết mờ: Các tạo các khóa mạnh từ sinh trắc học và các dữ liệu nhiễu khác " mà sử dụng lưới hình tam giác, khi số lượng chiều n là 4 hoặc lớn hơn, mật độ trở nên thấp hơn một cách nhanh chóng đối với cách bố trí gói hình cầu, và trở nên cao hơn hơn một cách nhanh chóng đối với cách bố trí bao phủ hình cầu. Độ lớn của sự giảm về độ chính xác do đó trở nên lớn hơn. Trong trường hợp về, ví dụ, lưới BW và lưới Leech, mặt khác, mật độ cũng là cao đối với cách bố trí gói hình cầu ở nhiều chiều hơn, và độ lớn của sự giảm về độ chính xác do đó là nhỏ.

Với lý do nêu trên, hệ thống xác thực theo phương án thứ nhất cho phép việc mã hóa sinh trắc học và việc ký sinh trắc học trong đó độ chính xác cao của việc xác thực (nghĩa là, tỷ lệ mà người dùng xác thực được chấp nhận và tỷ lệ mà người khác bị từ chối là cao) được hoàn thành.

Mặc dù hệ thống xác thực theo phương án thứ nhất thực hiện việc tạo khóa, khuôn mẫu, và thông tin xác nhận, việc khôi phục khóa, việc xác nhận khóa, và tương tự dựa vào thông tin sinh trắc học, thông tin mà việc thực hiện được dựa trên là không giới hạn ở thông tin sinh trắc học để nhận dạng người, và hệ thống xác thực có thể thực hiện việc tạo khóa, khuôn mẫu, và thông tin xác nhận, việc khôi phục khóa, việc xác nhận khóa, và tương tự dựa vào thông tin mờ để nhận dạng cá nhân (ví dụ, hàm không thể tạo bản sao dưới dạng vật lý (physically unclonable function, viết tắt là PUF)) để nhận dạng thiết bị bán dẫn).

Sáng chế này không giới hạn ở các phương án nêu trên nhưng bao gồm các sửa đổi khác nhau. Các phương án nêu trên được giải thích chi tiết nhằm làm dễ hiểu sáng chế này và không giới hạn ở các phương án bao gồm tất cả các kết cấu nêu trên. Một phần kết cấu theo một phương án có thể được thay thế bởi một phần kết cấu theo phương án khác; kết cấu theo một phương án có thể được hợp nhất với kết cấu theo phương án khác. Một phần kết cấu theo mỗi phương án có thể được bổ sung, được xóa, hoặc được thay thế bởi một

phần kết cấu của kết cấu khác.

Các kết cấu, các chức năng, các bộ xử lý nêu trên, đối với tất cả hoặc một phần của chúng, có thể được thực hiện bởi phần cứng: ví dụ, nhờ thiết kế mạch tích hợp. Các kết cấu và chức năng nêu trên có thể được thực hiện bởi phần mềm, nghĩa là bộ xử lý diễn dịch và thực hiện các chương trình cung cấp chức năng. Thông tin của các chương trình, các bảng, và các tệp để thực hiện các chức năng có thể được lưu trữ trong thiết bị lưu trữ như bộ nhớ, ổ đĩa cứng, hoặc ổ đĩa trạng thái rắn (Solid State Drive, viết tắt là SSD), hoặc phương tiện lưu trữ như thẻ IC, hoặc thẻ SD.

Các hình vẽ thể hiện các đường điều khiển và các đường thông tin như được xem là cần thiết cho các sự giải thích nhưng không thể hiện tất cả các đường điều khiển hoặc các đường thông tin trong các sản phẩm. Có thể xem gần như tất cả các thành phần thực tế được liên kết với nhau.

Yêu cầu quyền ưu tiên

Sáng chế yêu cầu quyền ưu tiên từ đơn xin cấp bằng độc quyền sáng chế Nhật Bản số JP 2019-216479 nộp ngày 29 tháng 11 năm 2019, nội dung của nó được kết hợp ở đây nhằm viện dẫn.

YÊU CẦU BẢO HỘ

1. Thiết bị tạo khóa để tạo ra khóa từ thông tin sinh trắc học, thiết bị tạo khóa bao gồm;

bộ xử lý; và

bộ nhớ,

bộ nhớ chứa:

vectơ đặc điểm thứ nhất chỉ báo đặc điểm thông tin sinh trắc học thứ nhất; và

thông số để nhận dạng cách bố trí theo cách bố trí gói hình cầu với mật độ nhỏ hơn 1 và lớn hơn trị số định trước, hoặc cách bố trí bao phủ hình cầu với mật độ bằng hoặc lớn hơn 1 và nhỏ hơn trị số định trước,

bộ xử lý được tạo kết cấu để:

nhận dạng cách bố trí theo cách bố trí gói hình cầu hoặc cách bố trí bao phủ hình cầu dựa vào thông số;

lựa chọn điểm thứ nhất được bao gồm theo cách bố trí được nhận dạng theo cách bố trí gói hình cầu hoặc cách bố trí bao phủ hình cầu;

tạo ra khóa thứ nhất nhờ thực hiện việc chuyển đổi thứ nhất định trước trên điểm thứ nhất; và

tạo ra, dựa vào vectơ đặc điểm thứ nhất và điểm thứ nhất, khuôn mẫu được kết hợp với thông tin sinh trắc học thứ nhất.

2. Thiết bị tạo khóa theo điểm 1,

Trong đó cách bố trí được nhận dạng trong thông số theo cách bố trí gói hình cầu và cách bố trí bao phủ hình cầu là cách bố trí lưới, và

trong đó bộ xử lý được tạo kết cấu để:

nhân vectơ đặc điểm thứ nhất với ma trận nghịch đảo của ma trận cơ bản của cách bố trí lưới để tính vectơ Y;

làm tròn xuống hoặc lên mỗi thành phần của vectơ Y đến số nguyên gần nhất để tính vectơ Z nguyên; và

lựa chọn, như điểm thứ nhất, vectơ được thu nhận nhờ nhân ma trận cơ bản với vectơ Z nguyên.

3. Thiết bị tạo khóa theo điểm 1, trong đó bộ xử lý được tạo kết cấu để lựa chọn điểm thứ nhất ngẫu nhiên tương ứng với sự phân phối được định trước, từ cách bố trí được nhận dạng theo cách bố trí gói hình cầu hoặc cách bố trí bao phủ hình cầu.

4. Thiết bị tạo khóa theo điểm 1, trong đó bộ xử lý được tạo kết cấu để lựa chọn, như điểm thứ nhất, điểm lân cận gần nhất của vectơ đặc điểm thứ nhất theo cách bố trí được nhận dạng theo cách bố trí gói hình cầu hoặc cách bố trí bao phủ hình cầu.

5. Thiết bị tạo khóa theo điểm 1, trong đó việc chuyển đổi thứ nhất được đinh trước bao gồm việc chuyển đổi bởi ít nhất một trong số hàm hash, hàm hash có khóa, hàm mã hóa, hoặc hàm hash tuyến tính.

6. Thiết bị tạo khóa theo điểm 1, trong đó bộ xử lý được tạo kết cấu để tạo ra, khi khóa thứ nhất được khôi phục, thông tin xác nhận để xác nhận tính hợp lệ của khóa thứ nhất được khôi phục, nhờ thực hiện việc chuyển đổi thứ hai được định trước trên khóa thứ nhất.

7. Thiết bị tạo khóa theo điểm 6, trong đó việc chuyển đổi thứ hai được định trước bao gồm việc chuyển đổi bởi ít nhất một trong số hàm hash, hàm hash có khóa, hàm mã hóa, hoặc hàm hash tuyến tính.

8. Thiết bị sử dụng khóa để sử dụng khóa được tạo ra thông tin sinh trắc học, thiết bị sử dụng khóa bao gồm:

bộ xử lý; và

bộ nhớ,

bộ nhớ chứa:

khuôn mẫu được tạo ra từ thông tin sinh trắc học thứ nhất;

thông tin xác nhận để xác nhận khóa thứ nhất được tạo ra từ thông tin sinh trắc học thứ nhất;

vectơ đặc điểm thứ hai chỉ báo đặc điểm của thông tin sinh trắc học thứ hai; và

thông số để nhận dạng cách bố trí theo cách bố trí gói hình cầu với mật độ nhỏ hơn 1 và lớn hơn trị số định trước, hoặc cách bố trí bao phủ hình cầu với mật độ bằng hoặc lớn hơn 1 và nhỏ hơn trị số định trước,

khuôn mẫu được tạo ra dựa vào điểm thứ nhất và đặc điểm thứ nhất, điểm thứ nhất được bao gồm cách bố trí được nhận dạng dựa vào thông số theo cách bố trí gói hình cầu hoặc cách bố trí bao phủ hình cầu, đặc điểm thứ nhất chỉ báo đặc điểm của thông tin sinh trắc học thứ nhất,

khóa thứ nhất được tạo ra nhờ thực hiện việc chuyển đổi thứ nhất được định trước trên điểm thứ nhất,

thông tin xác nhận được tạo ra nhờ thực hiện việc chuyển đổi thứ hai được định trước trên khóa thứ nhất,

bộ xử lý được tạo kết cấu để:

tính, từ vectơ đặc điểm thứ hai và khuôn mẫu, điểm thứ hai;

tính, như điểm thứ ba, điểm lân cận gần nhất của điểm thứ hai theo cách bố trí được nhận dạng theo cách bố trí gói hình cầu hoặc cách bố trí bao phủ hình cầu;

thực hiện việc chuyển đổi thứ nhất được định trước trên điểm thứ ba để tạo ra khóa thứ hai; và

so sánh, với thông tin xác nhận, trị số thu nhận được nhờ thực hiện việc chuyển đổi thứ hai được định trước trên khóa thứ hai, để xác định khóa thứ nhất và khóa thứ hai được tạo ra từ thông tin sinh trắc học của cơ thể sống giống nhau hay không.

9. Thiết bị sử dụng khóa theo điểm 8, trong đó, bộ xử lý được tạo kết cấu thực hiện, khi được xác định rằng khóa thứ nhất và khóa thứ hai được tạo ra từ thông tin sinh trắc học của cơ thể sống giống nhau từ việc so sánh trị số được thu nhận nhờ thực hiện việc chuyển đổi thứ hai được định trước trên khóa thứ hai thành thông tin xác nhận, ít nhất một trong số việc xử lý xác thực, việc xử lý mã hóa, hoặc việc xử lý chữ ký nhờ sử dụng khóa thứ hai.

10. Phương pháp tạo khóa bằng thiết bị tạo khóa để tạo ra khóa từ thông tin sinh trắc học, thiết bị tạo khóa chứa:

vectơ đặc điểm thứ nhất chỉ báo đặc điểm của thông tin sinh trắc học thứ nhất; và

thông số để nhận dạng cách bố trí theo cách bố trí gói hình cầu với mật độ nhỏ hơn 1 và lớn hơn trị số định trước, hoặc cách bố trí bao phủ hình cầu với mật độ bằng hoặc lớn hơn 1 và nhỏ hơn trị số định trước,

phương pháp tạo khóa bao gồm các bước:

nhận dạng, bằng thiết bị tạo khóa, cách bố trí theo cách bố trí gói hình cầu hoặc cách bố trí bao phủ hình cầu dựa vào thông số;

lựa chọn, bằng thiết bị tạo khóa, điểm thứ nhất được bao gồm theo cách bố trí được nhận dạng theo cách bố trí gói hình cầu hoặc cách bố trí bao phủ hình cầu;

tạo ra, bằng thiết bị tạo khóa, khóa thứ nhất nhờ thực hiện việc chuyển đổi thứ nhất được định trước trên điểm thứ nhất; và

tạo ra, bằng thiết bị tạo khóa, dựa vào vectơ đặc điểm thứ nhất và điểm thứ nhất, khuôn mẫu được kết hợp với thông tin sinh trắc học thứ nhất.

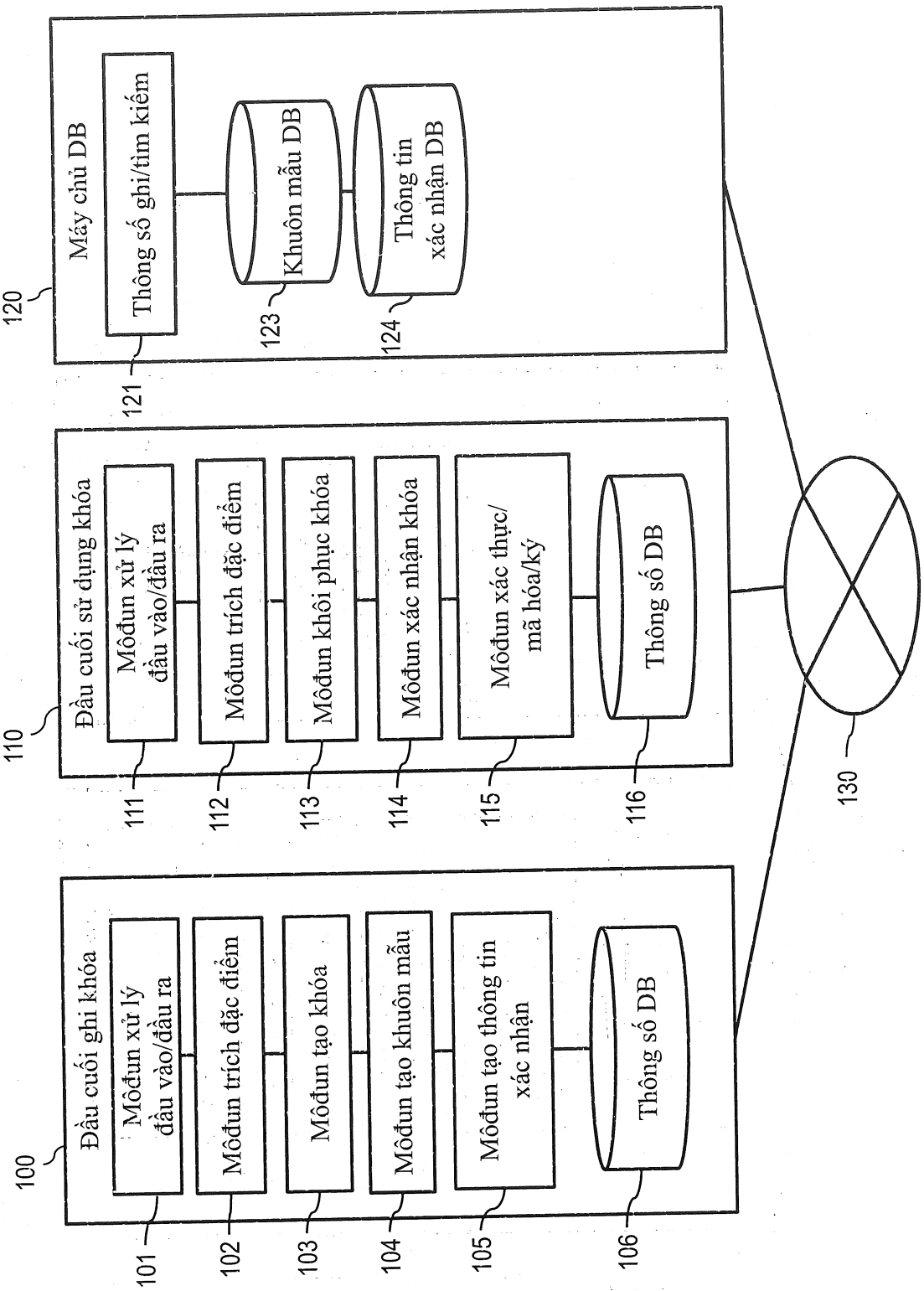
Đầu cuối ghi khóa
Môđun xử lý đầu vào/đầu ra
Môđun trích đặc điểm
Môđun tạo khóa
Môđun tạo khuôn mẫu
Môđun tạo thông tin xác nhận
Thông số DB
Đầu cuối sử dụng khóa
Môđun xử lý đầu vào/đầu ra
Môđun trích đặc điểm
Môđun khôi phục khóa
Môđun xác nhận khóa
Môđun xác thực/ mã hóa/ký
Thông số DB
Máy chủ DB
Thông số ghi/tìm kiếm
Khuôn mẫu DB
Thông tin xác nhận DB
100
101
102
103
104
105
106
110
111
112
113
114
115
116
120
121
123
124
130

FIG. 1

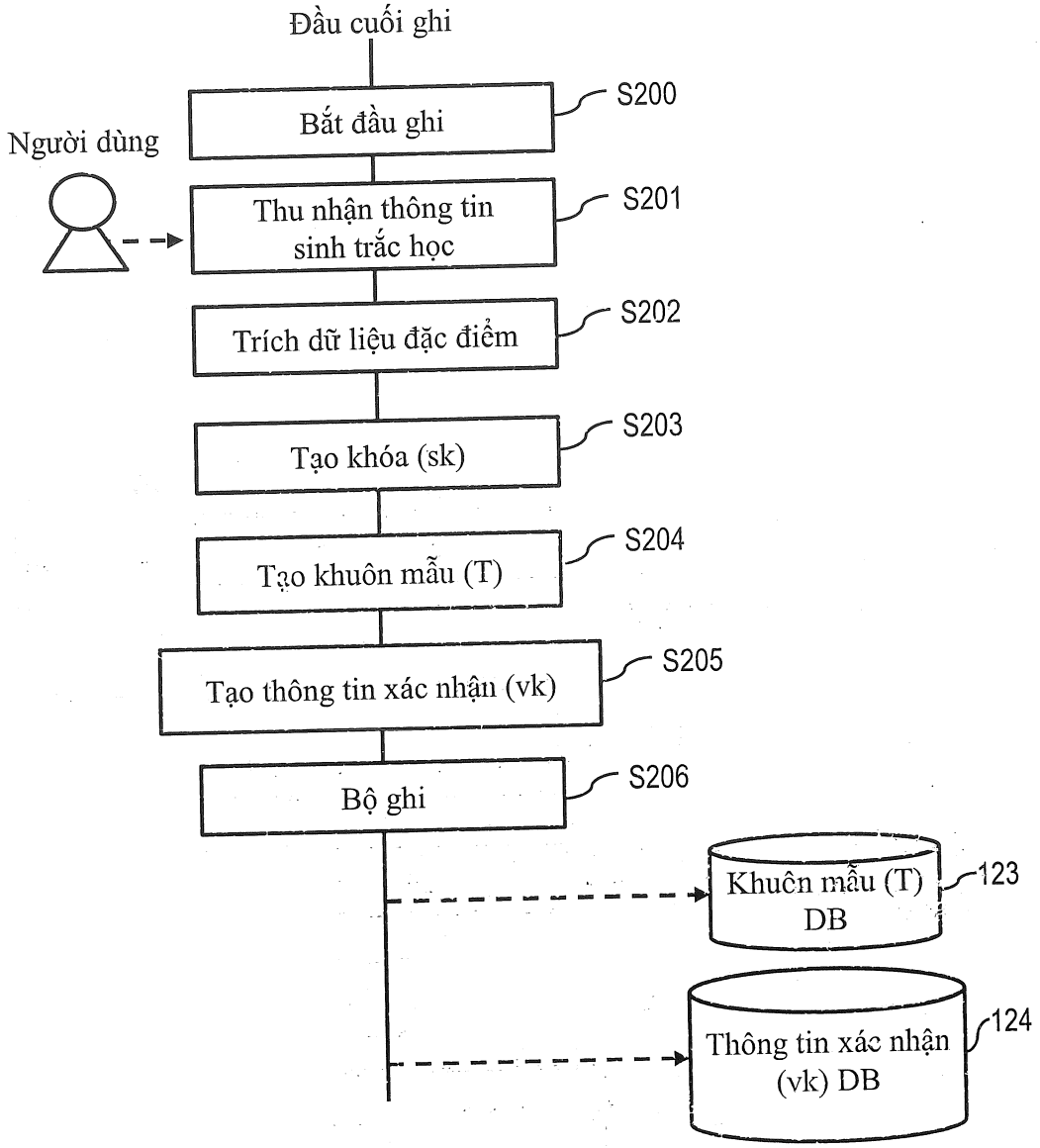
Đầu cuối ghi
Người dùng
Bắt đầu ghi
S200
Thu nhận thông tin sinh trắc học
S201
Trích dữ liệu đặc điểm
S202
Tạo khóa (sk)
S203
Tạo khuôn mẫu (T)
S204
Tạo thông tin xác nhận (vk)
S205
Bộ ghi
S206
Khuôn mẫu (T) DB
123
Thông tin xác nhận (vk) DB
124

FIG. 2

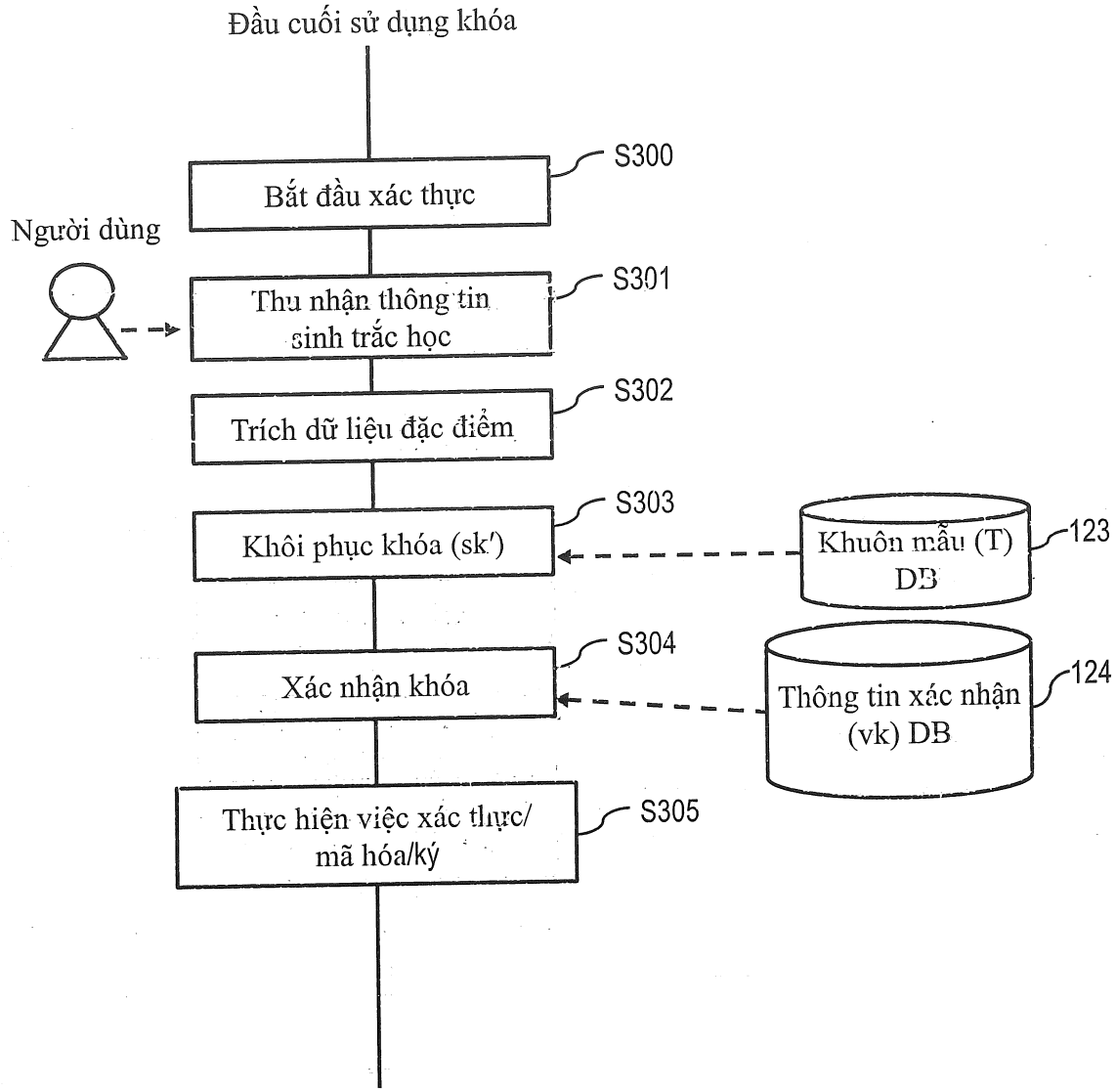
Đầu cuối sử dụng khóa
Người dùng
Bắt đầu xác thực
S300
Thu nhận thông tin sinh trắc học
S301
Trích dữ liệu đặc điểm
S302
Khôi phục khóa (sk')
S303
Khuôn mẫu (T) DB
123
Xác nhận khóa
S304
Thông tin xác nhận (vk) DB
124
Thực hiện việc xác thực/ mã hóa/ký
S305

FIG. 3

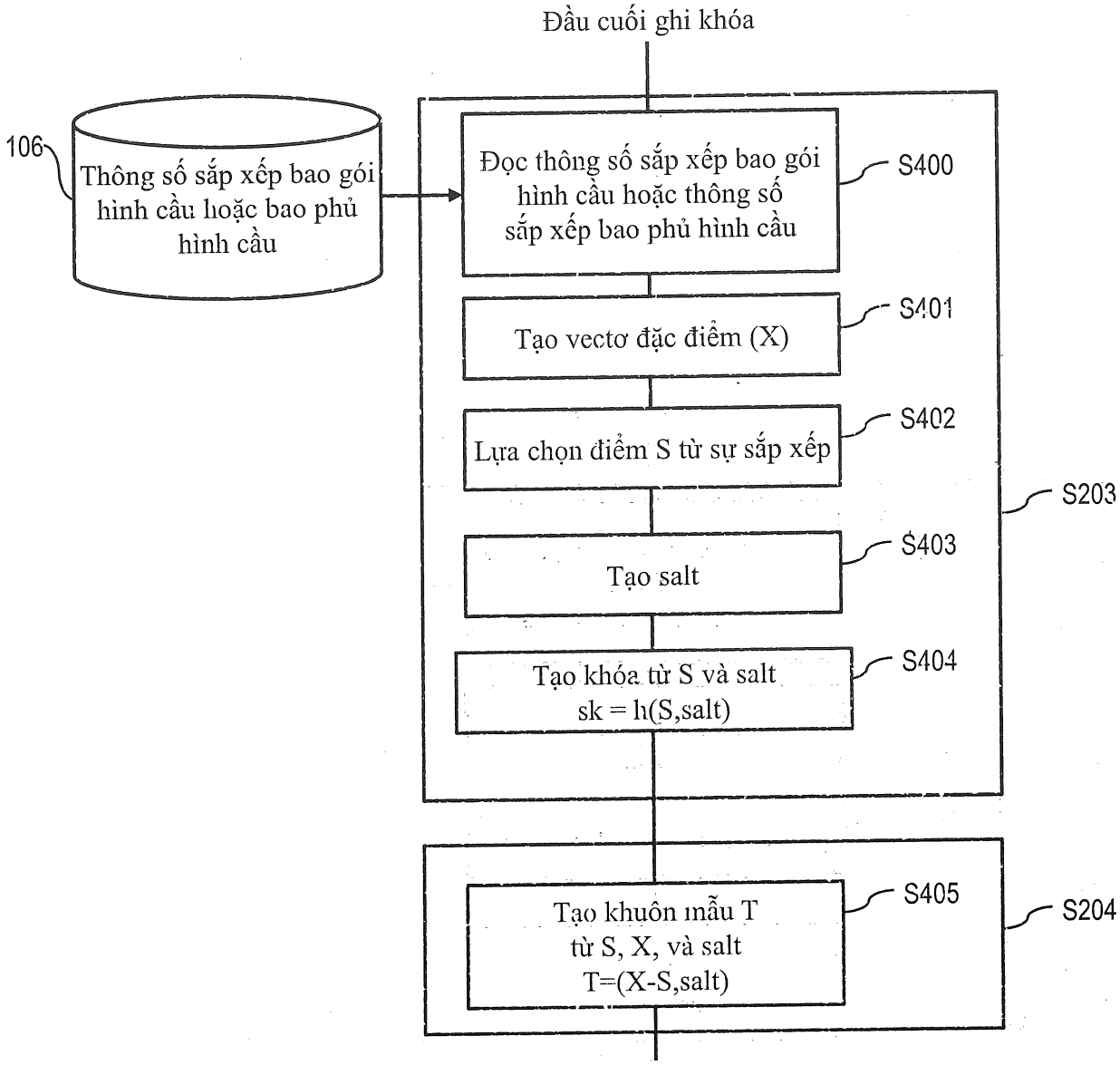
Đầu cuối ghi khóa
106
Thông số sắp xếp bao gói hình cầu hoặc bao phủ hình cầu
Đọc thông số sắp xếp bao gói hình cầu hoặc thông số sắp xếp bao phủ hình cầu
S400
Tạo vectơ đặc điểm (X)
S401
Lựa chọn điểm S từ sự sắp xếp
S402
Tạo salt
S403
Tạo khóa từ S và salt
sk = h(S,salt)
S404
S203
Tạo khuôn mẫu T từ S, X, và salt
T=(X-S,salt)
S405
S204

FIG. 4

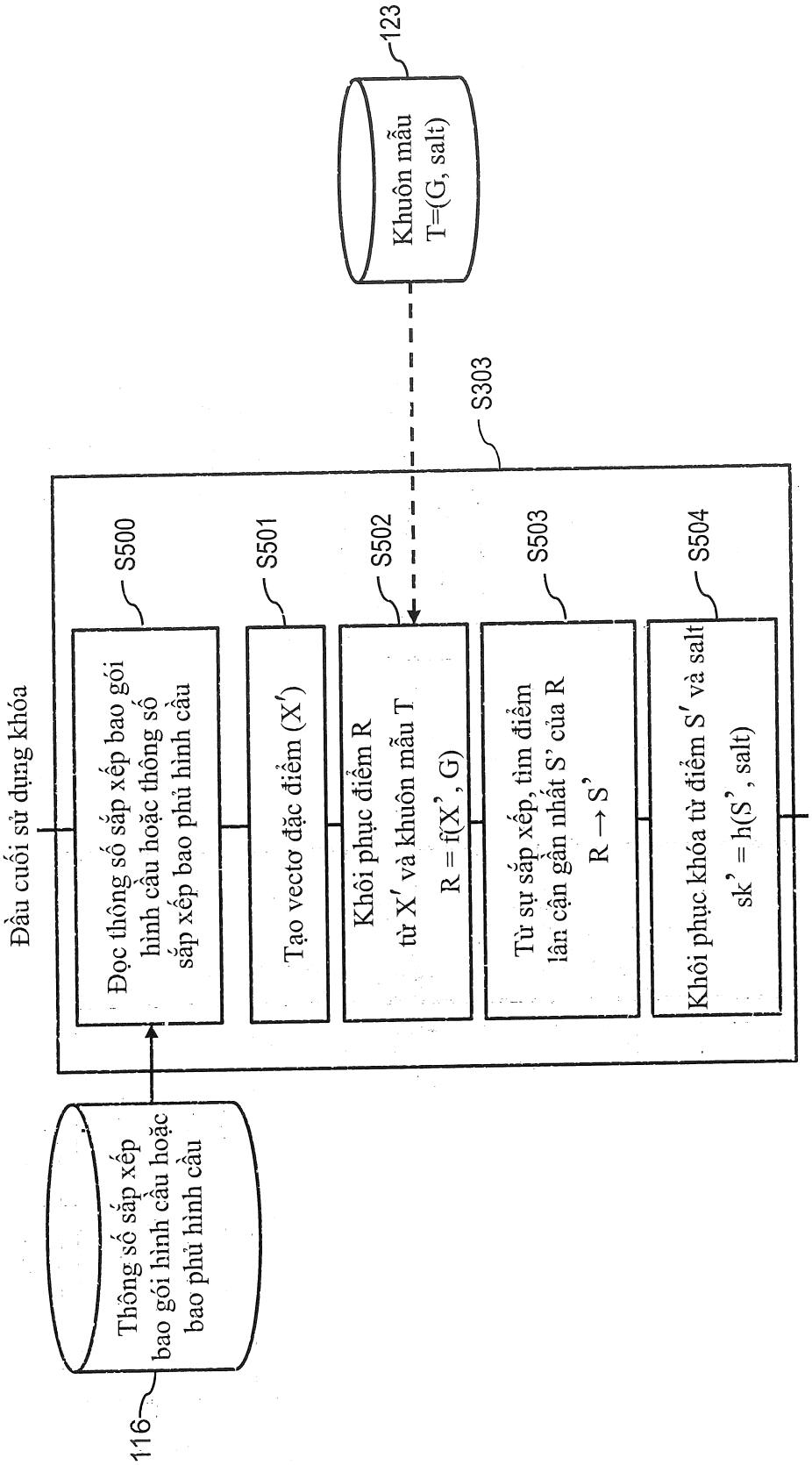
Đầu cuối sử dụng khóa
Thông số sắp xếp bao gói hình cầu hoặc bao phủ hình cầu
116
Đọc thông số sắp xếp bao gói hình cầu hoặc thông số sắp xếp bao phủ hình cầu
S500
Tạo vectơ đặc điểm (X')
S501
Khôi phục điểm R từ X' và khuôn mẫu T
R = f(X', G)
S502
Từ sự sắp xếp, tìm điểm lân cận gần nhất S' của R
R → S'
S503
Khôi phục khóa từ điểm S' và salt
sk' = h(S', salt)
S504
S303
Khuôn mẫu T=(G, salt)
123

FIG. 5

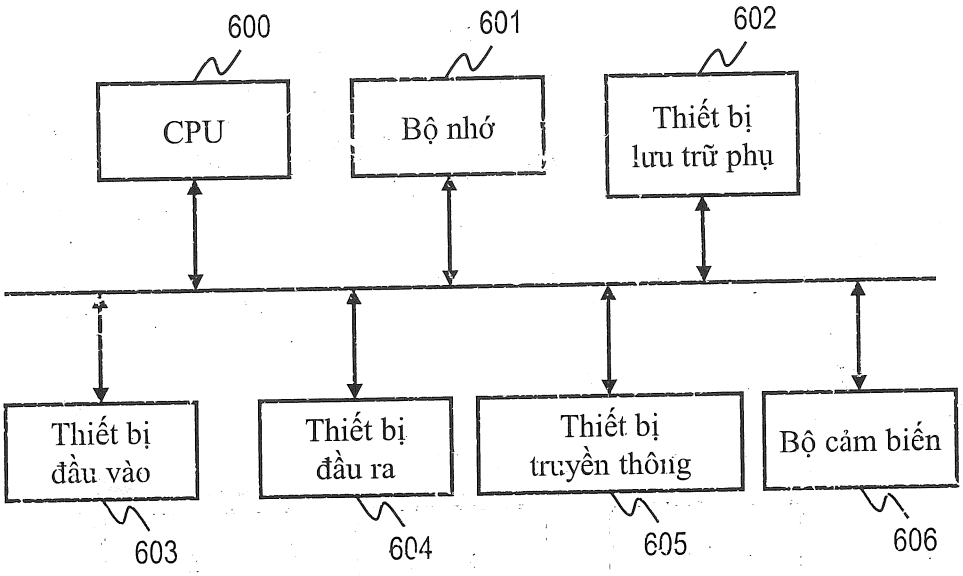
600
601
602
CPU
Bộ nhớ
Thiết bị
lưu trữ phụ
Thiết bị
đầu vào
Thiết bị
đầu ra
Thiết bị
truyền thông
Bộ cảm biến
603
604
605
606

FIG. 6