



(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)



1-0035131

(51)⁸ H04L 29/08

(13) B

(21) 1-2018-04369

(22) 23/02/2017

(86) PCT/CN2017/074629 23/02/2017

(87) WO2017/152767 14/09/2017

(30) 201610130265.2 08/03/2016 CN

(45) 27/03/2023 420

(43) 25/12/2018 369A

(73) Advanced New Technologies Co., Ltd. (KY)

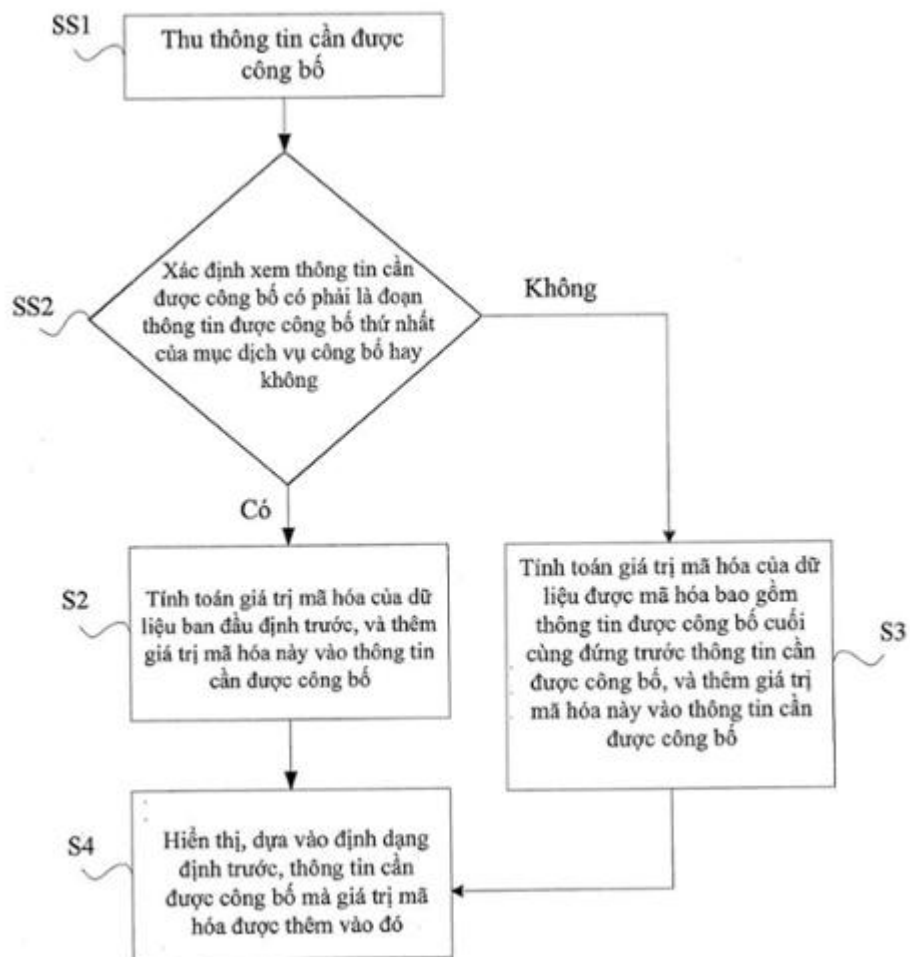
Cayman Corporate Centre, 27 Hospital Road, George Town, Grand Cayman KY1-9008, Cayman Islands

(72) YANG, Li (CN).

(74) Công ty TNHH Tầm nhìn và Liên danh (VISION & ASSOCIATES CO.LTD.)

(54) PHƯƠNG PHÁP VÀ THIẾT BỊ XỬ LÝ THÔNG TIN ĐƯỢC CÔNG BỐ

(57) Sáng chế đề cập đến phương pháp và thiết bị xử lý thông tin được công bố, và hệ thống công bố thông tin. Phương pháp này bao gồm các bước sau: thu thông tin cần được công bố, và xác định xem thông tin cần được công bố có phải là đoạn thông tin được công bố thứ nhất tương ứng với mục đích vụ công bố hay không; nếu kết quả xác định là có, thì tính toán giá trị mã hóa của thông tin ban đầu định trước bằng cách sử dụng thuật toán mã hóa định trước, và thêm giá trị mã hóa của thông tin ban đầu định trước vào thông tin cần được công bố; hoặc nếu không thì, tính toán, bằng cách sử dụng thuật toán mã hóa định trước, giá trị mã hóa của dữ liệu được mã hóa bao gồm thông tin được công bố cuối cùng đứng trước thông tin cần được công bố, và thêm giá trị mã hóa của dữ liệu được mã hóa vào thông tin cần được công bố; và hiển thị, dựa vào định dạng định trước, thông tin cần được công bố mà giá trị mã hóa được thêm vào đó. Bằng cách sử dụng các phương án thực hiện về phương pháp hoặc thiết bị theo sáng chế, sự khó khăn trong việc can thiệp vào thông tin được công bố có thể được tăng lên, tính nguyên gốc và tính toàn vẹn của thông tin được công bố được bảo đảm, và độ đáng tin của thông tin được công bố được cải thiện nhiều.



Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập đến lĩnh vực các công nghệ xử lý thông tin dữ liệu, và cụ thể là, phương pháp và thiết bị xử lý thông tin được công bố, và hệ thống công bố thông tin.

Tình trạng kỹ thuật của sáng chế

Với sự phát triển nhanh chóng của các công nghệ Internet, số lượng công ty và tổ chức lựa chọn hiển thị thông tin cho các người dùng trên các nền tảng Internet ngày càng tăng trưởng. Ví dụ, nhà bán lẻ trực tuyến có thể công bố thông tin khuyến mại và thông tin bán hàng trên Internet; người tiêu dùng có thể công bố bình luận về hàng hóa và dạng như vậy lên Internet; tổ chức ngân hàng có thể công bố thông tin bán sản phẩm tài chính, thông tin giảm giá mua hàng bằng thẻ ngân hàng và dạng như vậy cho các người dùng trên Internet; và tổ chức phúc lợi công cộng có thể bộc lộ thông tin quyên góp cho các người dùng trên Internet. Bằng cách sử dụng Internet để công bố thông tin cho các người dùng, hiệu quả hoạt động của các công ty và tổ chức có thể được cải thiện, và các người dùng có thể được biết nhiều thông tin hơn. Tuy nhiên, nhà quản lý thông tin được công bố có thể là nhà công bố thông tin. Cụ thể là, nhà công bố thông tin có thể xóa hoặc sửa đổi thông tin được công bố hoặc điều chỉnh trình tự của thông tin được công bố bằng cách sử dụng máy chủ phía sau. Tính nguyên gốc và tính toàn vẹn của thông tin được công bố bởi nhà công bố thông tin rất quan trọng đối với các người dùng, và độ đáng tin được cải thiện của thông tin được công bố làm cho các người dùng tin tưởng hơn vào các nhà công bố thông tin.

Trong công nghệ hiện có, thông tin được công bố thu được bởi các người dùng là độc lập lẫn nhau và hầu như không được kết hợp với nhau. Trong trường hợp này, nhà công bố thông tin có thể dễ dàng can thiệp vào thông tin được công bố. Ví dụ, nếu các người dùng đưa ra các bình luận về các dịch vụ sau khi bán chất lượng thấp được đề xuất bởi nhà bán lẻ trực tuyến nhất định đối với hàng hóa được bán bởi nhà bán lẻ trực tuyến, vì bình luận này có thể ảnh hưởng đến việc bán hàng hóa, nên nhà bán lẻ trực tuyến có thể xóa bình luận khỏi cơ sở dữ liệu phía sau thông qua một số kênh. Do đó, các người dùng khác sẽ không biết về bình luận hoặc nhận định rằng bình luận bị can thiệp vào bởi nhà công bố thông tin. Theo một ví dụ khác, nếu công ty công bố

thông báo trên Internet ở thời điểm muộn hơn so với thời điểm mà thông báo phải được công bố, nghĩa là, công ty sửa đổi thời gian công bố của thông báo trong cơ sở dữ liệu phía sau, nên rất khó để các người dùng cung cấp bằng chứng.

Trong công nghệ hiện có, do thiếu sự giám sát của người dùng, nên nhà công bố thông tin có thể sửa đổi hoặc xóa thông tin được công bố, và do đó, tính nguyên gốc và tính toàn vẹn của thông tin được công bố bởi nhà công bố thông tin không thể được bảo đảm, và độ đáng tin của thông tin được công bố bị giảm xuống. Do đó, trong công nghệ hiện có, cần có phương pháp xử lý thông tin được công bố để cải thiện độ đáng tin của thông tin công bố.

Bản chất kỹ thuật của sáng chế

Các phương án thực hiện của sáng chế nhằm đề xuất phương pháp và thiết bị công bố thông tin, và hệ thống công bố thông tin, để tăng sự khó khăn trong việc can thiệp vào thông tin được công bố, duy trì tính nguyên gốc và tính toàn vẹn của bản ghi thông tin được công bố, và cải thiện độ đáng tin của thông tin được công bố.

Phương pháp và thiết bị công bố thông tin, và hệ thống công bố thông tin được đề xuất theo các phương án thực hiện của sáng chế được thực hiện như được mô tả dưới đây.

Sáng chế đề xuất phương pháp xử lý thông tin được công bố, và phương pháp này bao gồm các bước sau: thu thông tin cần được công bố, và xác định xem thông tin cần được công bố có phải là đoạn thông tin được công bố thứ nhất tương ứng với mục dịch vụ công bố hay không; nếu kết quả xác định là có, thì tính toán giá trị mã hóa của thông tin ban đầu định trước bằng cách sử dụng thuật toán mã hóa định trước, và thêm giá trị mã hóa của thông tin ban đầu định trước vào thông tin cần được công bố; hoặc nếu không thì, tính toán, bằng cách sử dụng thuật toán mã hóa định trước, giá trị mã hóa của dữ liệu được mã hóa bao gồm thông tin được công bố cuối cùng đứng trước thông tin cần được công bố, và thêm giá trị mã hóa của dữ liệu được mã hóa vào thông tin cần được công bố; và hiển thị, dựa vào định dạng định trước, thông tin cần được công bố mà giá trị mã hóa được thêm vào đó.

Sáng chế đề xuất phương pháp xử lý thông tin được công bố, và phương pháp này bao gồm các bước sau: đọc, từ thông tin được công bố, giá trị mã hóa thứ nhất mà

là của dữ liệu được mã hóa bao gồm thông tin được công bố cuối cùng đứng trước thông tin được công bố và được tính toán bằng cách sử dụng thuật toán mã hóa định trước; hoặc khi thông tin được công bố là đoạn thông tin được công bố thứ nhất của mục đích vụ công bố, thì đọc, từ thông tin được công bố, giá trị mã hóa thứ nhất mà là của thông tin ban đầu định trước và được tính toán bằng cách sử dụng thuật toán mã hóa định trước; tính toán, dựa vào thuật toán mã hóa định trước đã bộc lộ và thông tin được công bố cuối cùng mà đứng trước thông tin được công bố và bao gồm giá trị mã hóa, giá trị mã hóa thứ hai của thông tin được công bố cuối cùng mà bao gồm giá trị mã hóa; xác định xem giá trị mã hóa thứ nhất có giống với giá trị mã hóa thứ hai hay không; và nếu kết quả xác định là không, thì xác định rằng ít nhất một đoạn thông tin được công bố trước thông tin được công bố được sửa đổi.

Sáng chế đề xuất thiết bị xử lý thông tin được công bố, và thiết bị này bao gồm các bộ phận sau: bộ phận tiếp nhận thông tin cần được công bố, được tạo cấu hình để thu thông tin cần được công bố, và xác định xem thông tin cần được công bố có phải là đoạn thông tin được công bố thứ nhất tương ứng với mục đích vụ công bố hay không; bộ phận tính toán giá trị mã hóa dữ liệu định trước, được tạo cấu hình để tính toán giá trị mã hóa của thông tin ban đầu định trước bằng cách sử dụng thuật toán mã hóa định trước, và thêm giá trị mã hóa của thông tin ban đầu định trước vào thông tin cần được công bố nếu kết quả xác định của bộ phận tiếp nhận thông tin cần được công bố là có; bộ phận tính toán giá trị mã hóa, được tạo cấu hình để tính toán, bằng cách sử dụng thuật toán mã hóa định trước, giá trị mã hóa của dữ liệu được mã hóa bao gồm thông tin được công bố cuối cùng đứng trước thông tin cần được công bố, và thêm giá trị mã hóa của dữ liệu được mã hóa vào thông tin cần được công bố nếu kết quả xác định của bộ phận tiếp nhận thông tin cần được công bố là không; và bộ phận hiển thị thông tin cần được công bố, được tạo cấu hình để hiển thị, dựa vào định dạng định trước, thông tin cần được công bố mà giá trị mã hóa được thêm vào đó.

Sáng chế đề xuất thiết bị xử lý thông tin được công bố, và thiết bị này bao gồm các bộ phận sau: bộ phận tiếp nhận giá trị mã hóa thứ nhất, được tạo cấu hình để đọc, từ thông tin được công bố, giá trị mã hóa thứ nhất mà là của dữ liệu được mã hóa bao gồm thông tin được công bố cuối cùng đứng trước thông tin được công bố và được tính toán bằng cách sử dụng thuật toán mã hóa định trước; hoặc khi thông tin được

công bố là đoạn thông tin được công bố thứ nhất của mục dịch vụ công bố, thì đọc, từ thông tin được công bố, giá trị mã hóa thứ nhất mà là của thông tin ban đầu định trước và được tính toán bằng cách sử dụng thuật toán mã hóa định trước; bộ phận tính toán giá trị mã hóa thứ hai, được tạo cấu hình để tính toán, dựa vào thuật toán mã hóa định trước đã bộc lộ và thông tin được công bố cuối cùng mà đứng trước thông tin được công bố và bao gồm giá trị mã hóa, giá trị mã hóa thứ hai của thông tin được công bố cuối cùng mà bao gồm giá trị mã hóa; bộ phận xác định giá trị mã hóa, được tạo cấu hình để xác định xem giá trị mã hóa thứ nhất có giống với giá trị mã hóa thứ hai hay không; và bộ phận xác định sửa đổi, được tạo cấu hình để xác định rằng ít nhất một đoạn thông tin được công bố trước thông tin được công bố được xóa hoặc sửa đổi nếu kết quả xác định của bộ phận xác định giá trị mã hóa là không.

Hệ thống công bố thông tin, hệ thống này bao gồm giao diện I/O và bộ xử lý, trong đó giao diện I/O được tạo cấu hình để thu thông tin cần được công bố, và gửi thông tin đã xử lý cần được công bố đến bộ phận xử lý hiển thị được chỉ định; và bộ xử lý được tạo cấu hình để xác định xem thông tin cần được công bố có phải là đoạn thông tin được công bố thứ nhất tương ứng với mục dịch vụ công bố hay không; nếu kết quả xác định là có, thì tính toán giá trị mã hóa của thông tin ban đầu định trước bằng cách sử dụng thuật toán mã hóa định trước, và thêm giá trị mã hóa của thông tin ban đầu định trước vào thông tin cần được công bố; hoặc nếu không thì, tính toán, bằng cách sử dụng thuật toán mã hóa định trước, giá trị mã hóa của dữ liệu được mã hóa bao gồm thông tin được công bố cuối cùng đứng trước thông tin cần được công bố, và thêm giá trị mã hóa của dữ liệu được mã hóa vào thông tin cần được công bố; và tạo ra thông tin đã xử lý cần được công bố.

Theo phương pháp và thiết bị xử lý thông tin được công bố, và hệ thống công bố thông tin được đề xuất theo sáng chế này, mỗi quan hệ kết hợp có thể được thiết lập giữa thông tin được công bố độc lập lẫn nhau, và hệ thống mã hóa đã liên kết được tạo thành trong mục dịch vụ công bố mà bao gồm thông tin được công bố. Trong hệ thống mã hóa đã liên kết, bộ nội suy thông tin cần sửa đổi tất cả các bản ghi thông tin được công bố sau khi sửa đổi thông tin được công bố tương ứng, sao cho tất cả dữ liệu có vẻ hoàn hảo. Điều này yêu cầu các chi phí cao, và có thể được xác định một cách dễ dàng. Do đó, theo phương pháp và thiết bị theo các phương án thực hiện, sự khó khăn trong

việc can thiệp vào bản ghi thông tin được công bố có thể được tăng lên, tính nguyên gốc và tính toàn vẹn của bản ghi thông tin được công bố được bảo đảm, và độ đáng tin của thông tin được công bố được cải thiện nhiều. Ngoài ra, theo phương pháp và thiết bị xử lý thông tin được công bố được đề xuất theo sáng chế này, các người dùng có thể xác minh, bằng cách sử dụng thiết bị đầu cuối khách, xem giá trị mã hóa của thông tin được công bố có khớp với giá trị mã hóa đã bộc lộ hay không, và sau xác định xem bản ghi thông tin được công bố có bị can thiệp vào hay không. Do đó, theo phương pháp và thiết bị theo các phương án thực hiện, vai trò của các người dùng trong việc giám sát các bản ghi thông tin được công bố có thể được nâng cao hơn nữa, và độ đáng tin của thông tin được công bố được cải thiện nhiều, và nhà công bố thông tin được tin tưởng cao bởi các người dùng.

Mô tả vắn tắt các hình vẽ

Để mô tả các giải pháp kỹ thuật theo các phương án thực hiện của sáng chế hoặc trong công nghệ hiện có theo cách rõ ràng hơn, phần sau mô tả một cách ngắn gọn các hình vẽ kèm theo được yêu cầu để mô tả các phương án thực hiện hoặc công nghệ hiện có. Rõ ràng là, các hình vẽ kèm theo trong phần mô tả sau chỉ thể hiện một số phương án thực hiện được ghi lại theo sáng chế, và người có hiểu biết trung bình trong lĩnh vực kỹ thuật vẫn có thể suy ra các hình vẽ khác từ các hình vẽ kèm theo này mà không cần các nỗ lực sáng tạo.

Fig.1 là lưu đồ về phương pháp minh họa một phương án thực hiện về phương pháp xử lý thông tin được công bố, theo sáng chế;

Fig.2 là lưu đồ về phương pháp minh họa một phương án thực hiện về phương pháp tính toán giá trị mã hóa, theo sáng chế;

Fig.3 là lưu đồ về phương pháp minh họa một phương án thực hiện khác về phương pháp xử lý thông tin được công bố, theo sáng chế;

Fig.4 là sơ đồ cấu trúc sơ lược minh họa các môđun theo một phương án thực hiện về thiết bị xử lý thông tin được công bố, theo sáng chế;

Fig.5 là sơ đồ cấu trúc sơ lược minh họa các môđun theo một phương án thực hiện về bộ phận tính toán giá trị mã hóa, theo sáng chế;

Fig.6 là sơ đồ cấu trúc sơ lược minh họa các môđun theo một phương án thực

hiện khác về thiết bị xử lý thông tin được công bố, theo sáng chế; và

Fig.7 là sơ đồ cấu trúc sơ lược minh họa các môđun theo một phương án thực hiện khác về thiết bị xử lý thông tin được công bố, theo sáng chế.

Mô tả chi tiết sáng chế

Để giúp người có hiểu biết trung bình trong lĩnh vực kỹ thuật hiểu rõ hơn về các giải pháp kỹ thuật theo sáng chế, phần sau mô tả một cách rõ ràng và đầy đủ các giải pháp kỹ thuật theo các phương án thực hiện của sáng chế dựa vào các hình vẽ kèm theo theo các phương án thực hiện của sáng chế. Rõ ràng là, các phương án thực hiện được mô tả chỉ là một số mà không phải là tất cả các phương án thực hiện của sáng chế. Tất cả các phương án thực hiện khác thu được bởi người có hiểu biết trung bình trong lĩnh vực kỹ thuật dựa vào các phương án thực hiện của sáng chế mà không có các nỗ lực sáng tạo sẽ nằm trong phạm vi bảo hộ của sáng chế.

Phần sau mô tả một cách chi tiết phương pháp xử lý thông tin được công bố theo sáng chế dựa vào các hình vẽ kèm theo. Fig.1 là lưu đồ về phương pháp sơ lược minh họa một phương án thực hiện về phương pháp xử lý thông tin được công bố, theo sáng chế. Mặc dù sáng chế đề xuất các bước hoạt động của phương pháp được thể hiện theo các phương án thực hiện sau hoặc các hình vẽ kèm theo, phương pháp này có thể bao gồm nhiều hoặc ít bước hoạt động hơn dựa vào nỗ lực thông thường hoặc không sáng tạo. Đối với các bước mà không có mối quan hệ nhân quả logic cần thiết, trình tự thực thi của các bước không bị giới hạn ở trình tự thực thi được đề xuất theo các phương án thực hiện của sáng chế. Trong quá trình xử lý thông tin được công bố thực tế hoặc khi phương pháp được thực hiện bởi thiết bị, thì phương pháp có thể được thực hiện dựa vào trình tự của phương pháp được thể hiện theo các phương án thực hiện hoặc các hình vẽ kèm theo, hoặc có thể được thực hiện song song (ví dụ, trong môi trường trong đó có các bộ xử lý song song hoặc sự xử lý đa luồng được thực hiện).

Một phương án thực hiện về phương pháp xử lý thông tin được công bố được đề xuất theo sáng chế được thể hiện trên Fig.1, và phương pháp này có thể bao gồm các bước sau.

S1: Thu thông tin cần được công bố, và xác định xem thông tin cần được công bố có phải là đoạn thông tin được công bố thứ nhất tương ứng với mục đích vụ công

bố hay không.

Theo phương án thực hiện này của sáng chế, mục đích vụ công bố có thể bao gồm dịch vụ công bố thông tin bởi công ty hoặc tổ chức cho các người dùng, và tính kịp thời, tính xác thực và tính toàn vẹn của dịch vụ thường ảnh hưởng đến các quyền lợi của các người dùng. Nói chung, các tổ chức công bố khác nhau có thể hình thành mục đích vụ công bố tương ứng dựa vào các yêu cầu của dịch vụ công bố thực tế. Ví dụ, mục đích vụ công bố để công bố thông tin trên nền tảng mua hàng trực tuyến có thể bao gồm bình luận của người tiêu dùng về hàng hóa, đoạn thông tin được công bố liên quan đến việc trích một số lợi nhuận của hàng hóa đã bán làm khoản quyền góp từ thiện và dạng như vậy. Nói chung, theo một phương án thực hiện được đề xuất theo sáng chế, mục đích vụ có thể bao gồm ít nhất một trong số các mục sau: quản lý bình luận của người dùng, thông tin thông báo kịp thời, thông tin quyền góp, dữ liệu cung ứng từ cộng đồng (crowdsourcing), bản ghi thông tin thanh toán, bản ghi dữ liệu đặt hàng và dạng như vậy.

Cụ thể, theo phương án thực hiện này, việc quản lý bình luận của người dùng có thể bao gồm bình luận của người dùng về hàng hóa hoặc dịch vụ. Tính xác thực và tính toàn vẹn của bình luận của người dùng là rất hữu ích khi các người dùng khác cố gắng đánh giá chất lượng của hàng hóa hoặc dịch vụ. Thông tin thông báo kịp thời có thể bao gồm thông tin có tính kịp thời mà được công bố bởi công ty hoặc tổ chức. Thời gian công bố thực tế của thông tin thông báo kịp thời giúp bảo vệ các quyền lợi của các người dùng. Thông tin quyền góp có thể bao gồm các bản ghi về các vật chất được quyền góp bởi các người dùng cho tổ chức phúc lợi công cộng hoặc hội từ thiện. Tính xác thực và tính toàn vẹn của các bản ghi quyền góp có thể cải thiện độ đáng tin của hoạt động phúc lợi công cộng. Dữ liệu cung ứng từ cộng đồng có thể bao gồm dữ liệu đầu tư mà là của các người dùng, người mà tham gia vào dự án cung ứng từ cộng đồng và được bộc lộ bởi người gây quỹ. Tính xác thực và tính toàn vẹn của dữ liệu cung ứng từ cộng đồng giúp bảo vệ nhiều đối với các quyền lợi của các người dùng. Bản ghi thông tin thanh toán có thể là bản ghi thanh toán được hiển thị bởi nền tảng thanh toán đối với người dùng. Tính toàn vẹn của bản ghi thông tin thanh toán giúp người dùng hiểu trạng thái chi tiêu cá nhân và dạng như vậy. Bản ghi dữ liệu đặt hàng có thể là bản ghi bán hàng của hàng hóa hoặc dịch vụ được hiển thị bởi nhà bán lẻ trực tuyến.

Quy trình thực hiện có thể bao gồm các bước sau:

SS1: Thu thông tin cần được công bố. Thông tin cần được công bố này có thể bao gồm thông tin mà cần được công bố bởi các người dùng về mục đích vụ. Nền tảng mua sắm lớn được sử dụng làm một ví dụ. Trên nền tảng mua sắm, cả nhà bán lẻ trực tuyến và người tiêu dùng đều là các người dùng. Nhà bán lẻ trực tuyến có thể công bố thông tin hàng hóa và thông báo khuyến mại trên nền tảng mua sắm, và các người dùng có thể công bố các bình luận về hàng hóa trên nền tảng mua sắm này. Trong phương pháp theo phương án thực hiện này, thông tin ban đầu định trước có thể được thiết lập dưới dạng điểm bắt đầu của mã hóa thông tin, để cung cấp sự hỗ trợ trong quy trình tính toán mã hóa thông tin.

Sau khi thông tin cần được công bố thu được, bước SS2 có thể được thực hiện: xác định xem thông tin cần được công bố có phải là đoạn thông tin được công bố thứ nhất tương ứng với mục đích vụ công bố hay không. Theo phương án thực hiện này, đoạn thông tin được công bố thứ nhất có thể là bình luận thứ nhất được công bố bởi các người dùng trong mục đích vụ công bố bình luận về hàng hóa. Trong kịch bản ứng dụng thực hiện khác, đoạn thông tin được công bố thứ nhất có thể là đoạn thông tin thông báo thứ nhất được công bố trong mục đích vụ công bố thông tin thông báo kịp thời. Đáng lưu ý rằng trong quy trình xác định xem thông tin cần được công bố có phải là đoạn thông tin được công bố thứ nhất tương ứng với mục đích vụ công bố hay không, xem thông tin cần được công bố có phải là đoạn thông tin được công bố thứ nhất của mục đích vụ công bố hay không có thể được xác định dựa vào thời gian công bố của thông tin cần được công bố. Cụ thể, khi xác định được rằng không có thông tin được công bố khác được công bố trong mục đích vụ công bố trước thời gian công bố của thông tin cần được công bố, thì có thể xác định được rằng thông tin cần được công bố là đoạn thông tin được công bố thứ nhất.

Theo phương án thực hiện này của sáng chế, thông tin cần được công bố có thể thu được, và sau đó xem thông tin cần được công bố có phải là đoạn thông tin được công bố thứ nhất tương ứng với mục đích vụ công bố hay không có thể được xác định.

S2: Nếu kết quả xác định là có, thì tính toán giá trị mã hóa của thông tin ban đầu định trước bằng cách sử dụng thuật toán mã hóa định trước, và thêm giá trị mã hóa của thông tin ban đầu định trước vào thông tin cần được công bố.

Nếu thông tin cần được công bố là đoạn thông tin được công bố thứ nhất tương ứng với mục đích vụ, thì giá trị mã hóa của thông tin ban đầu định trước có thể được tính toán. Theo phương án thực hiện này, thông tin ban đầu định trước có thể là chuỗi ký tự được tạo ra ngẫu nhiên trong cơ sở dữ liệu phía sau, hoặc có thể là chuỗi ký tự định trước. Thuật toán mã hóa định trước có thể là thuật toán băm (hash). Thuật toán băm này có thể ánh xạ giá trị nhị phân với độ dài tùy ý thành giá trị nhị phân tương đối ngắn với độ dài cố định. Giá trị mã hóa là giá trị băm thu được sau khi việc xử lý được thực hiện bằng cách sử dụng thuật toán băm. Giá trị băm là phương pháp biểu diễn giá trị ngắn gọn và duy nhất của phân đoạn của dữ liệu. Giá trị băm khác được tạo ra ngay cả khi một chữ cái trong thông tin cần được công bố được sửa đổi, để đảm bảo một cách hiệu quả rằng dữ liệu được mã hóa không bị can thiệp vào, và đảm bảo tính nguyên gốc và tính toàn vẹn của dữ liệu được mã hóa. Giá trị mã hóa duy nhất có thể thu được thông qua việc tính toán bằng cách sử dụng thuật toán băm, và độ bảo mật của dữ liệu được mã hóa được bảo đảm. Theo phương án thực hiện này, việc tính toán mã hóa có thể được thực hiện bằng cách sử dụng thuật toán băm theo các phương pháp sau làm thuật toán mã hóa định trước: Tóm lược thông điệp 2 (Message Digest 2, MD2), Tóm lược thông điệp 4 (Message Digest 4, MD4), Tóm lược thông điệp 5 (Message Digest 5, MD5), Thuật toán băm an toàn 1 (Secure Hash Algorithm 1, SHA1) và dạng như vậy. Hiển nhiên, thuật toán mã hóa định trước có thể là thuật toán mã hóa được chọn dựa vào yêu cầu mã hóa hoặc yêu cầu xử lý dữ liệu, hoặc thậm chí có thể là thuật toán mã hóa được xác định bởi người dùng.

Giá trị mã hóa thu được thông qua việc tính toán được thêm vào thông tin cần được công bố. Trong trường hợp này, thông tin cần được công bố được cập nhật, và giá trị mã hóa của thông tin ban đầu định trước được thêm vào dữ liệu gốc của thông tin cần được công bố.

Đáng lưu ý rằng thông tin ban đầu định trước và thuật toán mã hóa định trước được sử dụng để tính toán giá trị mã hóa có thể được bộc lộ cho các người dùng, sao cho các người dùng xác minh tính nguyên gốc và tính toàn vẹn của thông tin được công bố. Hiển nhiên, thông tin ban đầu định trước có thể được lược bỏ. Trong trường hợp này, thông tin ban đầu định trước được thiết lập thành 0, và giá trị mã hóa thu được sau khi thông tin ban đầu định trước được mã hóa vẫn là 0.

S3: Mặt khác, tính toán, bằng cách sử dụng thuật toán mã hóa định trước, giá trị mã hóa của dữ liệu được mã hóa bao gồm thông tin được công bố cuối cùng đứng trước thông tin cần được công bố, và thêm giá trị mã hóa của dữ liệu được mã hóa vào thông tin cần được công bố.

Nếu thông tin cần được công bố không phải là đoạn thông tin được công bố thứ nhất tương ứng với mục đích vụ công bố, thì giá trị mã hóa của dữ liệu được mã hóa bao gồm thông tin được công bố cuối cùng đứng trước thông tin cần được công bố có thể được tính toán, và giá trị mã hóa của dữ liệu được mã hóa được thêm vào thông tin cần được công bố.

Theo phương án thực hiện này, dữ liệu được mã hóa có thể là thông tin được công bố cuối cùng đứng trước thông tin cần được công bố. Sau đó, thông tin được công bố cuối cùng có thể được mã hóa bằng cách sử dụng thuật toán mã hóa định trước, để thu giá trị mã hóa của thông tin được công bố cuối cùng. Tất nhiên, theo các phương án thực hiện khác, dữ liệu được mã hóa có thể bao gồm dữ liệu sau.

Theo phương án thực hiện này của sáng chế, dữ liệu được mã hóa có thể còn bao gồm ít nhất một đoạn thông tin được công bố, mà đứng trước thông tin được công bố cuối cùng, thu được bằng cách sử dụng phương pháp định trước.

Theo phương án thực hiện này của sáng chế, phương pháp định trước có thể bao gồm ít nhất một trong số các bước sau: thu thông tin được công bố với số lượng khoảng thời gian được chỉ định trước thông tin cần được công bố; và thu thông tin được công bố nằm trong khoảng thời gian định trước trước thông tin cần được công bố.

Phương pháp định trước có thể là phương pháp tiếp nhận được xác định bởi người dùng dựa vào kịch bản ứng dụng thực tế. Ví dụ, trong một số kịch bản ứng dụng thực tế, thông tin về mục đích vụ công bố nhất định cần được công bố tương đối thường xuyên. Trong trường hợp này, nếu giá trị mã hóa của thông tin được công bố cuối cùng được tính toán mỗi lần thông tin được công bố, thì hiệu quả hoạt động của máy chủ phía sau chắc chắn bị ảnh hưởng. Cụ thể, trong kịch bản ứng dụng, các người dùng có thể thêm 500 bình luận về hàng hóa bán nhanh nhất định mỗi ngày. Trong kịch bản ứng dụng, phương pháp định trước có thể được thiết lập để tính toán giá trị mã hóa một lần đối với mỗi 20 bình luận trước đó. Ví dụ, các bình luận gốc được tạo

ra ở ngày thứ N bao gồm MSG-001, MSG-002, MSG-003, ..., MSG-499 và MSG-500. Khi bình luận thứ 21 MSG-021 được công bố, giá trị mã hóa của 20 bình luận trước đó được tính toán, để thu giá trị băm (1-20). Giá trị băm (1-20) và MSG-021 được công bố cùng nhau, và bình luận thứ 21 được công bố cuối cùng là MSG-N021. Khi bình luận thứ 41 MSG-041 được công bố, thì giá trị mã hóa của 20 bình luận từ bình luận thứ 21 đến bình luận thứ 40 được tính toán. Bình luận thứ 21 là MSG-N021, và bình luận thứ 22 đến bình luận thứ 40 là từ MSG-022 đến MSG-040. Giá trị mã hóa của bình luận thứ 21 đến bình luận thứ 40 được tính toán, để thu giá trị băm (21-40). Giá trị băm (21-40) và MSG-041 được công bố cùng nhau, và bình luận thứ 41 được công bố cuối cùng là MSG-N041. Hiển nhiên, trong một kịch bản ứng dụng thực hiện khác, các số lượng đoạn thông tin được công bố khác nhau có thể được sử dụng để tính toán giá trị mã hóa mỗi lần. Ví dụ, phương pháp thiết lập thời gian có thể được sử dụng. Giá trị mã hóa được tính toán một lần với mỗi N giờ. Cụ thể, giá trị mã hóa của thông tin được công bố trong N giờ trước đó mà ở trước thông tin cần được công bố có thể được tính toán. Giá trị mã hóa của các đoạn thông tin được công bố đứng trước thông tin cần được công bố được tính toán, sao cho tần suất hoạt động của máy chủ có thể được giảm xuống, và không gian lưu trữ của máy chủ hoặc thiết bị đầu cuối khách có thể được tiết kiệm.

Theo một phương án thực hiện của sáng chế, Fig.2 là lưu đồ về phương pháp minh họa một phương án thực hiện về phương pháp tính toán giá trị mã hóa, theo sáng chế. Như được thể hiện trên Fig.2, bước tính toán, bằng cách sử dụng thuật toán mã hóa định trước, giá trị mã hóa của dữ liệu được mã hóa bao gồm thông tin được công bố cuối cùng đứng trước thông tin cần được công bố có thể bao gồm các bước sau.

S11: Trích xuất dữ liệu thông tin được chỉ định từ thông tin được công bố có trong dữ liệu được mã hóa.

Nói chung, tất cả dữ liệu thông tin có thể được trích xuất từ thông tin được công bố có trong dữ liệu được mã hóa, và tất cả dữ liệu gốc của thông tin được công bố được sử dụng để tính toán mã hóa. Tuy nhiên, trong một số kịch bản ứng dụng, lượng dữ liệu gốc có trong thông tin được công bố là tương đối lớn, hoặc một số trong các dữ liệu gốc thay đổi nhỏ, hoặc một số trong các dữ liệu gốc có ảnh hưởng tương đối nhỏ đến các quyền lợi của các người dùng. Trong trường hợp này, một số thông tin có thể

được trích xuất từ dữ liệu gốc của thông tin được công bố làm dữ liệu thông tin được chỉ định. Ví dụ, trong mục dịch vụ công bố thông tin quyên góp, thông tin được công bố trên trang web phúc lợi công cộng thường bao gồm dữ liệu chẳng hạn như tên, địa chỉ, số tiền quyên góp và số điện thoại của người nguyên góp. Thông tin chẳng hạn như địa chỉ và số điện thoại của người nguyên góp có ảnh hưởng tương đối nhỏ đến tính xác thực của hoạt động quyên góp. Do đó, trong quy trình tính toán giá trị mã hóa, thông tin dữ liệu chẳng hạn như địa chỉ và số điện thoại của người quyên góp có thể được bỏ qua, và chỉ có tên và số tiền quyên góp của người quyên góp cần được sử dụng làm dữ liệu thông tin được chỉ định để tính toán mã hóa.

S12: Mã hóa dữ liệu thông tin được chỉ định đã trích xuất bằng cách sử dụng thuật toán mã hóa định trước, để tạo ra giá trị mã hóa.

Sau khi dữ liệu thông tin được chỉ định để tính toán mã hóa được xác định, thì giá trị mã hóa có thể được tính toán và tạo ra. Cụ thể, dữ liệu thông tin được chỉ định đã trích xuất có thể được mã hóa bằng cách sử dụng thuật toán mã hóa định trước, để tạo ra giá trị mã hóa. Tương tự với bước S2, thuật toán mã hóa định trước có thể là thuật toán băm, và một cách tương ứng, giá trị mã hóa là giá trị băm thu được sau khi việc xử lý được thực hiện bằng cách sử dụng thuật toán băm. Theo phương án thực hiện này, việc tính toán mã hóa có thể được thực hiện bằng cách sử dụng thuật toán băm theo các phương pháp sau làm thuật toán mã hóa định trước: Tóm lược thông điệp 2 (MD2), Tóm lược thông điệp 4 (MD4), Tóm lược thông điệp 5 (MD5), Thuật toán băm an toàn 1 (SHA1) và dạng như vậy.

Một số dữ liệu được chọn từ dữ liệu gốc có trong thông tin được công bố như dữ liệu thông tin được chỉ định để tính toán mã hóa, sao cho một số dữ liệu mà có ảnh hưởng nhỏ đến tính nguyên gốc và tính xác thực của thông tin được công bố có thể được loại bỏ, lượng hoạt động của máy chủ có thể được giảm bớt, và không gian lưu trữ của máy chủ hoặc thiết bị đầu cuối khách có thể được tiết kiệm.

Theo một phương án thực hiện khác của sáng chế, phương pháp này có thể còn bao gồm bước sau: thu thông tin dữ liệu bổ sung, trong đó một cách tương ứng, dữ liệu được mã hóa bao gồm thông tin dữ liệu bổ sung.

Trong dữ liệu gốc có trong thông tin được công bố, một số dữ liệu có thể có ảnh hưởng nhỏ đến các quyền lợi của các người dùng. Tuy nhiên, một số dữ liệu mà có thể

có ảnh hưởng lớn đến các quyền lợi của các người dùng không có trong dữ liệu gốc. Ví dụ, thông tin thông báo kịp thời được công bố bởi một số công ty hoặc tổ chức không thể nhất thiết bao gồm thời gian mà thông tin được công bố tại đó. Tuy nhiên, đối với các người dùng, thời gian công bố của thông tin kịp thời có thể được sử dụng làm cơ sở để xác định xem công ty hoặc tổ chức có trì hoãn việc công bố hoặc can thiệp vào thời gian công bố hay không. Theo phương án thực hiện này, thông tin dữ liệu bổ sung có thể được thu thêm nữa, và thông tin dữ liệu bổ sung này được sử dụng làm một phần của dữ liệu để tính toán mã hóa. Ngoài ra, thông tin dữ liệu bổ sung có thể được thu từ tập tin chẳng hạn như nhật ký hoạt động của máy chủ. Cụ thể, trong kịch bản ứng dụng, thông tin thông báo kịp thời gốc được công bố bởi nhà bán lẻ trực tuyến cho các người dùng bao gồm MEG-1, MEG-2, ... và MEG- N . Trong quy trình tính toán giá trị mã hóa, thông tin thời gian có thể được thêm vào dữ liệu được mã hóa. Khi MEG-1 được công bố, thì giá trị băm (MEG-0+ T_0), nghĩa là, thông tin ban đầu định trước MEG-0 cộng thời gian ban đầu định trước T_0 , có thể được tính toán. Giá trị băm (MEG-0+ T_0) và MEG-1 được công bố cùng nhau, và đoạn thông tin thông báo kịp thời thứ nhất được công bố cuối cùng là MEG- T_1 . Khi thông tin thông báo kịp thời thứ hai MEG-2 được công bố, thì giá trị băm (MEG-1+ T_1), nghĩa là, MEG- T_1 cộng thời gian công bố T_1 của MEG- T_1 , có thể được tính toán. Giá trị băm (MEG-1+ T_1) và MEG-2 được công bố cùng nhau, và thông tin thông báo kịp thời thứ hai được công bố cuối cùng là MEG- T_2 . Hiển nhiên, theo một phương án thực hiện khác, thông tin dữ liệu bổ sung có thể là thông tin chẳng hạn như mã của máy chủ công bố thông tin hoặc mã tổ chức của bộ phận công bố thông tin.

Thông tin dữ liệu bổ sung trong dữ liệu gốc có trong dữ liệu được công bố được sử dụng làm dữ liệu được mã hóa để tính toán mã hóa, sao cho tính duy nhất và tính xác thực của dữ liệu được mã hóa có thể được nâng cao thêm nữa, sự khó khăn trong việc can thiệp vào thông tin được công bố có thể được tăng lên, và độ bảo mật của thông tin được công bố có thể được bảo đảm.

Đáng lưu ý rằng một mục đích của phương pháp xử lý thông tin được công bố được đề xuất theo sáng chế là để cho phép các người dùng tham gia vào việc giám sát tính nguyên gốc và tính toàn vẹn của thông tin được công bố. Theo một phương án thực hiện khác của sáng chế, sau đó, thuật toán mã hóa định trước, dữ liệu thông tin

được chỉ định hoặc thông tin dữ liệu bổ sung được sử dụng để tạo ra giá trị mã hóa thông qua việc tính toán có thể được công bố thêm nữa cho các người dùng, sao cho các người dùng có thể xác minh tính nguyên gốc và tính toàn vẹn của thông tin được công bố dựa vào thông tin dữ liệu bổ sung.

Theo phương án thực hiện này, giá trị mã hóa của dữ liệu được mã hóa bao gồm thông tin được công bố cuối cùng đứng trước thông tin cần được công bố được thêm vào thông tin cần được công bố, sao cho các đoạn thông tin được công bố liên kết được kết hợp với nhau, và hệ thống mã hóa đã liên kết được tạo thành trong toàn bộ mục đích vụ công bố. Các người dùng có thể xác định, bằng cách sử dụng chỉ thuật toán mã hóa định trước đã bộc lộ và dữ liệu được mã hóa để tính toán mã hóa, xem thông tin được công bố có bị can thiệp vào hay không. Trong hệ thống mã hóa đã liên kết, bộ nội suy thông tin cần sửa đổi tất cả các bản ghi thông tin được công bố sau khi sửa đổi thông tin được công bố tương ứng, sao cho tất cả dữ liệu có vẻ hoàn hảo. Điều này yêu cầu các chi phí cao, và có thể được xác định một cách dễ dàng. Do đó, phương pháp xử lý thông tin được công bố được đề xuất theo sáng chế này có độ đáng tin cao trong việc duy trì tính nguyên gốc và tính toàn vẹn của dữ liệu.

S4: Hiện thị, dựa vào định dạng định trước, thông tin cần được công bố mà giá trị mã hóa được thêm vào đó.

Sau khi thông tin cần được công bố được cập nhật, thì thông tin cần được công bố thực tế bao gồm hai phần: dữ liệu gốc cần được công bố, và giá trị mã hóa đã thêm của dữ liệu được mã hóa bao gồm thông tin được công bố cuối cùng đứng trước thông tin cần được công bố. Thông tin đã cập nhật cần được công bố có thể được hiển thị bằng cách sử dụng nhiều phương pháp. Theo một phương án thực hiện của sáng chế, giá trị mã hóa có thể được thêm trực tiếp vào vị trí đầu của dữ liệu gốc của thông tin gốc cần được công bố. Theo một phương án thực hiện khác của sáng chế, liên kết đối với giá trị mã hóa có thể được tạo ra trong thông tin được công bố gốc, và các người dùng có thể thu giá trị mã hóa bằng cách nhấp vào liên kết này. Theo một phương án thực hiện khác của sáng chế, bảng để lưu trữ thông tin cần được công bố và giá trị mã hóa được thêm vào thông tin cần được công bố có thể được tạo ra ở trang hiển thị của mục đích vụ. Các người dùng có thể tìm kiếm giá trị mã hóa trong bảng.

Sáng chế còn đề xuất một phương án thực hiện về phương pháp xử lý thông tin

được công bố được thực hiện từ góc nhìn của thiết bị đầu cuối khách. Fig.3 là lưu đồ về phương pháp minh họa một phương án thực hiện khác về phương pháp xử lý thông tin được công bố, theo sáng chế. Như được thể hiện trên Fig.3, phương pháp này có thể bao gồm các bước sau.

S101: Đọc, từ thông tin được công bố, giá trị mã hóa thứ nhất mà là của dữ liệu được mã hóa bao gồm thông tin được công bố cuối cùng của thông tin được công bố bằng cách sử dụng thuật toán mã hóa định trước; hoặc khi thông tin được công bố là đoạn thông tin được công bố thứ nhất của mục đích vụ công bố, thì đọc, từ thông tin được công bố, giá trị mã hóa thứ nhất mà là của thông tin ban đầu định trước và được tính toán bằng cách sử dụng thuật toán mã hóa định trước.

Sau khi thu thông tin được công bố, thiết bị đầu cuối khách có thể xác minh xem thông tin được công bố cuối cùng đứng trước thông tin được công bố có bị can thiệp vào hay không. Trước tiên, giá trị mã hóa thứ nhất mà là của dữ liệu được mã hóa bao gồm thông tin được công bố cuối cùng đứng trước thông tin được công bố và được tính toán bằng cách sử dụng thuật toán mã hóa định trước có thể được đọc từ thông tin được công bố; hoặc khi thông tin được công bố là đoạn thông tin được công bố thứ nhất của mục đích vụ công bố, thì giá trị mã hóa thứ nhất mà là của thông tin ban đầu định trước và được tính toán bằng cách sử dụng thuật toán mã hóa định trước có thể được đọc từ thông tin được công bố. Giá trị mã hóa thứ nhất có thể được thu trực tiếp bằng cách sử dụng phương pháp hiển thị được đề xuất ở bước S4 trước đó.

S102: Tính toán, dựa vào thuật toán mã hóa định trước đã bộc lộ và thông tin được công bố cuối cùng mà đứng trước thông tin được công bố và bao gồm giá trị mã hóa, giá trị mã hóa thứ hai của thông tin được công bố cuối cùng mà bao gồm giá trị mã hóa.

Sau khi xác minh xem thông tin được công bố cuối cùng đứng trước thông tin được công bố có bị can thiệp vào hay không, thiết bị đầu cuối khách có thể xác định, thông qua việc tính toán, xem giá trị mã hóa thực tế của thông tin được công bố cuối cùng mà đứng trước thông tin được công bố và bao gồm giá trị mã hóa có giống với giá trị mã hóa có trong thông tin được công bố hay không. Cụ thể, thiết bị đầu cuối khách có thể tính toán, dựa vào thuật toán mã hóa định trước đã bộc lộ và thông tin được công bố cuối cùng mà đứng trước thông tin được công bố, bao gồm giá trị mã

hóa và được sử dụng để tính toán giá trị mã hóa, giá trị mã hóa thứ hai của thông tin được công bố cuối cùng mà bao gồm giá trị mã hóa.

S103: Xác định xem giá trị mã hóa thứ nhất có giống với giá trị mã hóa thứ hai hay không.

S104: Nếu kết quả xác định là không, thì xác định rằng ít nhất một đoạn thông tin được công bố trước thông tin được công bố được xóa hoặc sửa đổi.

Khi giá trị mã hóa thứ nhất và giá trị mã hóa thứ hai là khác nhau, thì có thể xác định được rằng ít nhất một đoạn thông tin công bố trước thông tin được công bố bị can thiệp vào (được xóa hoặc sửa đổi).

Theo phương pháp xử lý thông tin được công bố được đề xuất theo sáng chế, mối quan hệ kết hợp có thể được thiết lập giữa thông tin được công bố độc lập lẫn nhau, và hệ thống mã hóa đã liên kết được tạo thành trong mục đích vụ công bố mà bao gồm thông tin được công bố. Trong hệ thống mã hóa đã liên kết, bộ nội suy thông tin cần sửa đổi tất cả các bản ghi thông tin được công bố sau khi sửa đổi thông tin được công bố tương ứng, sao cho tất cả dữ liệu có vẻ hoàn hảo sau khi thông tin được công bố được sửa đổi. Điều này yêu cầu các chi phí cao, và có thể được xác định một cách dễ dàng. Do đó, theo phương pháp theo phương án thực hiện này, sự khó khăn trong việc can thiệp vào bản ghi thông tin được công bố có thể được tăng lên, tính nguyên gốc và tính toàn vẹn của bản ghi thông tin được công bố được duy trì, và độ đáng tin của thông tin được công bố được cải thiện nhiều. Ngoài ra, theo phương pháp xử lý thông tin được công bố được đề xuất theo sáng chế, các người dùng có thể xác minh, bằng cách sử dụng thiết bị đầu cuối khách, xem giá trị mã hóa của thông tin được công bố có khớp với giá trị mã hóa đã bộc lộ hay không, và sau đó xác định xem bản ghi thông tin được công bố có bị can thiệp vào hay không. Do đó, theo phương pháp theo phương án thực hiện này, vai trò của các người dùng trong việc giám sát các bản ghi thông tin được công bố có thể được nâng cao thêm nữa, và độ đáng tin của thông tin được công bố được cải thiện nhiều, và nhà công bố thông tin được tin tưởng cao bởi các người dùng.

Dựa vào phương pháp xử lý thông tin được công bố được đề xuất theo các phương án thực hiện của sáng chế, sáng chế còn đề xuất thiết bị xử lý thông tin được công bố. Fig.4 là sơ đồ cấu trúc sơ lược minh họa các môđun theo một phương án thực

hiện về thiết bị xử lý thông tin được công bố, theo sáng chế. Như được thể hiện trên Fig.4, thiết bị 40 có thể bao gồm các bộ phận sau: bộ phận tiếp nhận thông tin cần được công bố 41, được tạo cấu hình để thu thông tin cần được công bố, và xác định xem thông tin cần được công bố có phải là đoạn thông tin được công bố thứ nhất tương ứng với mục đích vụ công bố hay không; bộ phận tính toán giá trị mã hóa dữ liệu định trước 42, được tạo cấu hình để tính toán giá trị mã hóa của thông tin ban đầu định trước bằng cách sử dụng thuật toán mã hóa định trước, và thêm giá trị mã hóa của thông tin ban đầu định trước vào thông tin cần được công bố nếu kết quả xác định của bộ phận tiếp nhận thông tin cần được công bố là có; bộ phận tính toán giá trị mã hóa 43, được tạo cấu hình để tính toán, bằng cách sử dụng thuật toán mã hóa định trước, giá trị mã hóa của dữ liệu được mã hóa bao gồm thông tin được công bố cuối cùng đứng trước thông tin cần được công bố, và thêm giá trị mã hóa của dữ liệu được mã hóa vào thông tin cần được công bố nếu kết quả xác định của bộ phận tiếp nhận thông tin cần được công bố là không; và bộ phận hiển thị thông tin cần được công bố 44, được tạo cấu hình để hiển thị, dựa vào định dạng định trước, thông tin cần được công bố mà giá trị mã hóa được thêm vào đó.

Theo thiết bị xử lý thông tin được công bố được đề xuất theo sáng chế, mối quan hệ kết hợp có thể được thiết lập giữa thông tin được công bố độc lập lẫn nhau, và hệ thống mã hóa đã liên kết được tạo thành trong mục đích vụ công bố mà bao gồm thông tin được công bố. Trong hệ thống mã hóa đã liên kết, bộ nội suy thông tin cần sửa đổi tất cả các bản ghi thông tin được công bố sau khi sửa đổi thông tin được công bố tương ứng, sao cho tất cả dữ liệu có vẻ hoàn hảo. Điều này yêu cầu các chi phí cao, và có thể được xác định một cách dễ dàng. Do đó, theo thiết bị theo phương án thực hiện này, sự khó khăn trong việc can thiệp vào bản ghi thông tin được công bố có thể được tăng lên, tính nguyên gốc và tính toàn vẹn của bản ghi thông tin được công bố được bảo đảm, và độ đáng tin của thông tin được công bố được cải thiện nhiều.

Theo một phương án thực hiện của sáng chế, dữ liệu được mã hóa có thể còn bao gồm ít nhất một đoạn thông tin được công bố, mà đứng trước thông tin được công bố cuối cùng, thu được bằng cách sử dụng phương pháp định trước.

Theo phương án thực hiện này, ít nhất một đoạn thông tin được công bố trước thông tin được công bố cuối cùng được thêm vào dữ liệu được mã hóa, sao cho các

đoạn thông tin được công bố liên kết được kết hợp với nhau, hệ thống mã hóa đã liên kết được tạo thành trong toàn bộ mục đích vụ công bố, và độ bảo mật của hệ thống mã hóa đối với mục đích vụ công bố được cải thiện.

Theo một phương án thực hiện, phương pháp định trước có thể được thiết lập để thu thông tin được công bố với số lượng khoảng thời gian được chỉ định trước thông tin cần được công bố hoặc thu thông tin được công bố nằm trong khoảng thời gian định trước trước thông tin cần được công bố. Do đó, theo một phương án thực hiện khác về thiết bị theo sáng chế, thiết bị xử lý có thể còn bao gồm các bộ phận sau: bộ phận tiếp nhận thông tin số lượng định trước, được tạo cấu hình để thu thông tin được công bố với số lượng khoảng thời gian được chỉ định trước thông tin cần được công bố; và bộ phận tiếp nhận thông tin thời gian định trước, được tạo cấu hình để thu thông tin được công bố nằm trong khoảng thời gian định trước trước thông tin cần được công bố.

Thông tin được công bố với số lượng khoảng thời gian được chỉ định hoặc thông tin được công bố nằm trong khoảng thời gian định trước trước thông tin cần được công bố thu được bằng cách sử dụng bộ phận tiếp nhận thông tin số lượng định trước hoặc bộ phận tiếp nhận thông tin thời gian định trước, sao cho khi máy chủ tính toán giá trị mã hóa của các đoạn thông tin được công bố đứng trước thông tin cần được công bố, tần suất hoạt động của máy chủ có thể được giảm bớt, và không gian lưu trữ của máy chủ hoặc thiết bị đầu cuối khách có thể được tiết kiệm.

Fig.5 là sơ đồ cấu trúc sơ lược minh họa các môđun theo một phương án thực hiện về bộ phận tính toán giá trị mã hóa, theo sáng chế. Như được thể hiện trên Fig.5, bộ phận tính toán giá trị mã hóa 43 có thể bao gồm các bộ phận sau: bộ phận lựa chọn thông tin thứ nhất 51, được tạo cấu hình để trích xuất dữ liệu thông tin được chỉ định từ thông tin được công bố có trong dữ liệu được mã hóa; và bộ phận tạo ra giá trị mã hóa thứ nhất 52, được tạo cấu hình để mã hóa dữ liệu thông tin được chỉ định đã trích xuất bằng cách sử dụng thuật toán mã hóa định trước, để tạo ra giá trị mã hóa.

Một số dữ liệu được chọn từ dữ liệu gốc có trong thông tin được công bố làm dữ liệu thông tin được chỉ định để tính toán mã hóa bằng cách sử dụng bộ phận tính toán giá trị mã hóa 43, sao cho một số dữ liệu mà có ảnh hưởng nhỏ đến tính nguyên gốc và tính xác thực của thông tin được công bố có thể được loại bỏ, lượng tính toán

của máy chủ có thể được giảm bớt, và không gian lưu trữ của máy chủ hoặc thiết bị đầu cuối khách có thể được tiết kiệm.

Fig.6 là sơ đồ cấu trúc sơ lược minh họa các môđun theo một phương án thực hiện khác về thiết bị xử lý thông tin được công bố, theo sáng chế. Như được thể hiện trên Fig.6, thiết bị 60 có thể còn bao gồm các bộ phận sau: bộ phận tiếp nhận dữ liệu bổ sung 61, được tạo cấu hình để thu thông tin dữ liệu bổ sung, trong đó một cách tương ứng, dữ liệu được mã hóa trong bộ phận tính toán giá trị mã hóa 43 bao gồm thông tin dữ liệu bổ sung.

Thông tin dữ liệu bổ sung trong dữ liệu gốc có trong dữ liệu được công bố được sử dụng làm dữ liệu được mã hóa để tính toán mã hóa bằng cách sử dụng bộ phận tiếp nhận dữ liệu bổ sung 61, sao cho tính duy nhất và tính xác thực của dữ liệu được mã hóa có thể được nâng cao thêm nữa, sự khó khăn trong việc can thiệp vào thông tin được công bố có thể được tăng lên, và độ bảo mật của thông tin được công bố có thể được bảo đảm.

Theo một phương án thực hiện của sáng chế, thuật toán mã hóa định trước là thuật toán băm, và giá trị mã hóa là giá trị băm thu được sau khi việc xử lý được thực hiện bằng cách sử dụng thuật toán băm. Giá trị mã hóa duy nhất có thể thu được thông qua việc tính toán bằng cách sử dụng thuật toán băm, và độ bảo mật của dữ liệu được mã hóa được bảo đảm. Theo phương án thực hiện này, việc tính toán mã hóa có thể được thực hiện bằng cách sử dụng thuật toán băm theo các phương pháp sau làm thuật toán mã hóa định trước: Tóm lược thông điệp 2 (MD2), Tóm lược thông điệp 4 (MD4), Tóm lược thông điệp 5 (MD5), Thuật toán băm an toàn 1 (SHA1) và dạng như vậy. Hiển nhiên, thuật toán mã hóa định trước có thể là thuật toán mã hóa được chọn dựa vào yêu cầu mã hóa hoặc yêu cầu xử lý dữ liệu, hoặc thậm chí có thể là thuật toán mã hóa được xác định bởi người dùng.

Theo một phương án thực hiện của sáng chế, mục đích vụ công bố có thể bao gồm ít nhất một trong số các mục sau: quản lý bình luận của người dùng, thông tin thông báo kịp thời, thông tin quyên góp, dữ liệu cung ứng từ cộng đồng, bản ghi thông tin thanh toán, bản ghi dữ liệu đặt hàng và dạng như vậy.

Một khía cạnh khác của sáng chế còn đề xuất thiết bị xử lý thông tin được công bố dùng cho thiết bị đầu cuối khách. Fig.7 là sơ đồ cấu trúc sơ lược minh họa các

môđun theo một phương án thực hiện khác về thiết bị xử lý thông tin được công bố, theo sáng chế. Như được thể hiện trên Fig.7, thiết bị 70 có thể bao gồm các bộ phận sau: bộ phận tiếp nhận giá trị mã hóa thứ nhất 71, được tạo cấu hình để đọc, từ thông tin được công bố, giá trị mã hóa thứ nhất mà là của dữ liệu được mã hóa bao gồm thông tin được công bố cuối cùng đứng trước thông tin được công bố và được tính toán bằng cách sử dụng thuật toán mã hóa định trước; hoặc khi thông tin được công bố là đoạn thông tin được công bố thứ nhất của mục đích vụ công bố, thì đọc, từ thông tin được công bố, giá trị mã hóa thứ nhất mà là của thông tin ban đầu định trước và được tính toán bằng cách sử dụng thuật toán mã hóa định trước; bộ phận tính toán giá trị mã hóa thứ hai 72, được tạo cấu hình để tính toán, dựa vào thuật toán mã hóa định trước đã bộc lộ và thông tin được công bố cuối cùng mà đứng trước thông tin được công bố và bao gồm giá trị mã hóa, giá trị mã hóa thứ hai của thông tin được công bố cuối cùng mà bao gồm giá trị mã hóa; bộ phận xác định giá trị mã hóa 73, được tạo cấu hình để xác định xem giá trị mã hóa thứ nhất có giống với giá trị mã hóa thứ hai hay không; và bộ phận xác định sửa đổi 74, được tạo cấu hình để xác định rằng ít nhất một đoạn thông tin được công bố trước thông tin được công bố được xóa hoặc sửa đổi nếu kết quả xác định của bộ phận xác định giá trị mã hóa là không.

Theo thiết bị xử lý thông tin được công bố được đề xuất theo sáng chế, các người dùng có thể xác minh, bằng cách sử dụng thiết bị đầu cuối khách, xem giá trị mã hóa của thông tin được công bố có khớp với giá trị mã hóa đã bộc lộ hay không, và sau đó xác định xem bản ghi thông tin được công bố có bị can thiệp vào hay không. Do đó, theo thiết bị theo phương án thực hiện này, vai trò của các người dùng trong việc giám sát các bản ghi thông tin được công bố có thể được nâng cao thêm nữa, và độ đáng tin của thông tin được công bố được cải thiện nhiều, và nhà công bố thông tin được tin tưởng cao bởi các người dùng.

Dựa vào phương pháp và thiết bị xử lý thông tin được công bố, theo các phương án thực hiện của sáng chế, sáng chế còn đề xuất hệ thống công bố thông tin, và hệ thống này có thể bao gồm giao diện I/O và bộ xử lý.

Giao diện I/O được tạo cấu hình để thu thông tin cần được công bố, và gửi thông tin đã xử lý cần được công bố đến bộ phận xử lý hiển thị được chỉ định.

Bộ xử lý được tạo cấu hình để xác định xem thông tin cần được công bố có phải

là đoạn thông tin được công bố thứ nhất tương ứng với mục đích vụ công bố hay không. Nếu kết quả xác định là có, thì tính toán giá trị mã hóa của thông tin ban đầu định trước bằng cách sử dụng thuật toán mã hóa định trước, và thêm giá trị mã hóa của thông tin ban đầu định trước vào thông tin cần được công bố; hoặc nếu không thì, tính toán, bằng cách sử dụng thuật toán mã hóa định trước, giá trị mã hóa của dữ liệu được mã hóa bao gồm thông tin được công bố cuối cùng đứng trước thông tin cần được công bố, và thêm giá trị mã hóa của dữ liệu được mã hóa vào thông tin cần được công bố; và tạo ra thông tin đã xử lý cần được công bố. Trong hệ thống công bố thông tin, mối quan hệ kết hợp có thể được thiết lập giữa thông tin được công bố độc lập lẫn nhau, và hệ thống mã hóa đã liên kết được tạo thành trong mục đích vụ công bố mà bao gồm thông tin được công bố. Do đó, theo hệ thống công bố thông tin theo phương án thực hiện này, sự khó khăn trong việc can thiệp vào bản ghi thông tin được công bố có thể được tăng lên, tính nguyên gốc và tính toàn vẹn của bản ghi thông tin được công bố được duy trì, và độ đáng tin của thông tin được công bố được cải thiện nhiều.

Mặc dù việc xử lý và hiển thị dữ liệu chẳng hạn như các phương pháp mã hóa dữ liệu băm khác nhau, phương pháp thêm giá trị mã hóa vào thông tin cần được công bố, phương pháp trích xuất dữ liệu thông tin và phương pháp hiển thị thông tin theo các phương án thực hiện được mô tả theo sáng chế. Sáng chế không bị giới hạn ở trường hợp hiển thị và xử lý dữ liệu mà hoàn toàn tuân theo tiêu chuẩn công nghiệp, tiêu chuẩn thực thi ngôn ngữ máy tính nhất định, hoặc các phần mô tả theo phương án thực hiện này. Một phương án thực hiện được cải biến dựa vào các phương án thực hiện hoặc các ngôn ngữ máy tính được chuẩn hóa nhất định cũng có thể đạt được hiệu quả thực hiện giống với, tương đương với hoặc tương tự với hiệu quả thực hiện mà đạt được theo phương án thực hiện nêu trên, hoặc đạt được hiệu quả thực hiện dự đoán được sau khi phương án thực hiện nêu trên được biến đổi. Hiển nhiên, ngay cả khi các phương pháp xử lý và xác định dữ liệu không được sử dụng, thì cùng ứng dụng vẫn có thể được thực hiện dựa vào phương pháp mã hóa dữ liệu, trao đổi thông tin và phương pháp phản hồi xác định thông tin của các phương án thực hiện nêu trên theo sáng chế. Các chi tiết được lược bỏ trong bản mô tả này để đơn giản.

Mặc dù sáng chế đề xuất các bước hoạt động về phương pháp được mô tả theo các phương án thực hiện hoặc các lưu đồ, nhưng nhiều hoặc ít bước hoạt động hơn có

thể được bao gồm dựa vào phương tiện thông thường hoặc không sáng tạo. Trình tự bước làm ví dụ theo các phương án thực hiện chỉ là một trong số các trình tự thực thi bước, và không thể hiện trình tự thực thi duy nhất. Khi đang được thực hiện trong thiết bị thực tế hoặc sản phẩm thiết bị đầu cuối khách, các bước hoạt động có thể được thực hiện dựa vào trình tự phương pháp được thể hiện theo các phương án thực hiện hoặc các hình vẽ kèm theo, hoặc có thể được thực hiện song song (ví dụ, trong môi trường trong đó có các bộ xử lý song song hoặc việc xử lý đa luồng được thực hiện).

Các bộ phận, thiết bị, hệ thống và các môđun được mô tả theo các phương án thực hiện nêu trên có thể được thực hiện bởi chip máy tính hoặc thực thể, hoặc được thực hiện bởi sản phẩm mà có chức năng nhất định. Để dễ dàng mô tả, thiết bị nêu trên được mô tả dựa vào sự phân chia các chức năng thành các môđun khác nhau. Hiển nhiên, khi sáng chế được thực hiện, thì các chức năng của mỗi môđun có thể được thực hiện trong một hoặc nhiều đoạn phần mềm và/hoặc phần cứng. Hiển nhiên, môđun thực hiện cùng chức năng với môđun bộ phận nhất định được mô tả theo sáng chế cũng có thể được thực hiện bởi các môđun con hoặc sự kết hợp của các môđun con này.

Người có hiểu biết trung bình trong lĩnh vực kỹ thuật cũng biết rằng, ngoài thực hiện bộ điều khiển bằng cách sử dụng mã chương trình đọc được bằng máy tính, việc lập trình logic có thể được thực hiện đối với các bước phương pháp để cho phép bộ điều khiển thực hiện cùng chức năng dưới các dạng cổng logic, bộ chuyển mạch, mạch tích hợp cho ứng dụng cụ thể, bộ điều khiển logic lập trình được và bộ vi điều khiển nhúng. Do đó, bộ điều khiển có thể được coi là thành phần phần cứng, và thiết bị mà có trong bộ điều khiển và được sử dụng để thực hiện các chức năng khác nhau cũng có thể được coi là cấu trúc trong thành phần phần cứng. Hoặc, thiết bị được tạo cấu hình để thực hiện các chức năng khác nhau thậm chí có thể được coi là cả môđun phần mềm thực hiện phương pháp và cấu trúc trong thành phần phần cứng.

Sáng chế có thể được mô tả theo ngữ cảnh chung của các lệnh thực thi được bằng máy tính mà được thực thi bởi máy tính, ví dụ, môđun chương trình. Nói chung, môđun chương trình bao gồm đoạn chương trình, chương trình, đối tượng, thành phần, cấu trúc dữ liệu, kiểu và dạng như vậy, mà thực hiện tác vụ cụ thể hoặc thực hiện kiểu dữ liệu trừu tượng cụ thể. Sáng chế cũng có thể được thực hiện trong các môi trường

tính toán phân tán. Trong các môi trường tính toán phân tán, các tác vụ được thực hiện bởi các thiết bị xử lý từ xa được kết nối với mạng truyền thông. Trong môi trường tính toán phân tán, môđun chương trình có thể nằm trong cả vật ghi lưu trữ bằng máy tính cục bộ và từ xa bao gồm các thiết bị lưu trữ.

Có thể thấy được từ các phần mô tả về các phương án thực hiện mà, người có hiểu biết trung bình trong lĩnh vực kỹ thuật có thể hiểu một cách rõ ràng rằng sáng chế có thể được thực hiện bằng cách sử dụng phần mềm ngoài nền tảng phần cứng đa năng cần thiết. Dựa vào việc hiểu này, các giải pháp kỹ thuật theo sáng chế về cơ bản, hoặc một phần đóng góp vào công nghệ hiện có, có thể được thực hiện dưới dạng sản phẩm phần mềm. Sản phẩm phần mềm máy tính có thể được lưu trữ trong vật ghi lưu trữ, chẳng hạn như ROM/RAM, đĩa từ hoặc đĩa quang, và bao gồm một số lệnh để lệnh cho thiết bị máy tính (mà có thể là máy tính cá nhân, thiết bị di động, máy chủ, thiết bị mạng và dạng như vậy) thực hiện các phương pháp được mô tả theo các phương án thực hiện hoặc theo một số phần của các phương án thực hiện của sáng chế.

Các phương án thực hiện trong bản mô tả này được mô tả theo phương pháp lũy tiến. Đối với các phần giống hoặc tương tự nhau theo các phương án thực hiện, có thể thực hiện tham chiếu đối với nhau. Mỗi phương án thực hiện tập trung vào sự khác biệt với các phương án thực hiện khác. Sáng chế có thể được sử dụng trong nhiều môi trường hoặc cấu hình về thiết bị máy tính dùng cho mục đích chung hoặc được dành riêng, ví dụ, các máy tính cá nhân, máy tính chủ, thiết bị cầm tay hoặc di động, thiết bị dạng bảng, thiết bị đa bộ xử lý, thiết bị dựa trên bộ vi xử lý, bộ giải mã tín hiệu truyền hình (set-top box), thiết bị điện tử lập trình được, PC mạng, máy tính loại nhỏ, máy tính khung chính, môi trường tính toán phân tán bao gồm thiết bị bất kỳ trong số các thiết bị hoặc dụng cụ được mô tả nêu trên và dạng như vậy.

Mặc dù sáng chế được mô tả bằng cách sử dụng các phương án thực hiện, nhưng người có hiểu biết trung bình trong lĩnh vực kỹ thuật biết được rằng nhiều cải biến và thay đổi của sáng chế có thể được thực hiện mà không lệch khỏi mục đích của sáng chế. Dự tính được rằng các điểm yêu cầu bảo hộ bao gồm các cải biến và thay đổi này mà không lệch khỏi mục đích của sáng chế.

YÊU CẦU BẢO HỘ

1. Phương pháp xử lý thông tin được công bố, trong đó phương pháp này bao gồm các bước:

thu thông tin cần được công bố (SS1) để hiển thị trực quan;

xác định xem thông tin cần được công bố có phải là đoạn thông tin được công bố thứ nhất tương ứng với mục đích vụ công bố hay không (SS2);

đáp lại việc xác định rằng thông tin cần được công bố là đoạn thông tin được công bố thứ nhất tương ứng với mục đích vụ công bố:

tính toán giá trị mã hóa của thông tin ban đầu định trước bằng cách sử dụng thuật toán mã hóa định trước, và

thêm giá trị mã hóa của thông tin ban đầu định trước vào thông tin cần được công bố (S2); hoặc

đáp lại việc xác định rằng thông tin cần được công bố không phải là đoạn thông tin được công bố thứ nhất tương ứng với mục đích vụ công bố:

tính toán, bằng cách sử dụng thuật toán mã hóa định trước, giá trị mã hóa của dữ liệu được mã hóa bao gồm thông tin được công bố cuối cùng đứng trước thông tin cần được công bố, và

thêm giá trị mã hóa của dữ liệu được mã hóa vào thông tin cần được công bố (S3); và

hiển thị trực quan, dựa vào định dạng định trước, thông tin cần được công bố mà giá trị mã hóa được thêm vào đó (S4).

2. Phương pháp xử lý thông tin được công bố theo điểm 1, trong đó dữ liệu được mã hóa còn bao gồm ít nhất một đoạn thông tin được công bố để hiển thị trực quan mà thu được bằng cách sử dụng phương pháp định trước và đứng trước thông tin được công bố cuối cùng.

3. Phương pháp xử lý thông tin được công bố theo điểm 2, trong đó phương pháp định trước bao gồm ít nhất một trong số các bước sau:

thu thông tin được công bố với số lượng khoảng thời gian được chỉ định trước

thông tin cần được công bố; và

thu thông tin được công bố nằm trong khoảng thời gian định trước trước thông tin cần được công bố.

4. Phương pháp xử lý thông tin được công bố theo điểm 1 hoặc điểm 2, trong đó bước tính toán, bằng cách sử dụng thuật toán mã hóa định trước, giá trị mã hóa của dữ liệu được mã hóa bao gồm thông tin được công bố cuối cùng đứng trước thông tin cần được công bố, bao gồm các bước:

trích xuất dữ liệu thông tin được chỉ định từ thông tin được công bố có trong dữ liệu được mã hóa (S11); và

mã hóa dữ liệu thông tin được chỉ định đã trích xuất bằng cách sử dụng thuật toán mã hóa định trước, để tạo ra giá trị mã hóa (S12).

5. Phương pháp xử lý thông tin được công bố theo điểm 1 hoặc điểm 2, trong đó phương pháp này còn bao gồm bước thu thông tin dữ liệu bổ sung, trong đó một cách tương ứng, dữ liệu được mã hóa bao gồm thông tin dữ liệu bổ sung.

6. Phương pháp xử lý thông tin được công bố theo điểm 1 hoặc điểm 2, trong đó:

thuật toán mã hóa định trước là thuật toán băm; và

giá trị mã hóa là giá trị băm thu được sau khi bước xử lý được thực hiện bằng cách sử dụng thuật toán băm.

7. Phương pháp xử lý thông tin được công bố theo điểm 1 hoặc điểm 2, trong đó mục đích vụ công bố bao gồm ít nhất một trong số các kiểu dịch vụ:

quản lý bình luận của người dùng, thông tin thông báo kịp thời, thông tin quyên góp, dữ liệu cung ứng từ cộng đồng (crowdsourcing), bản ghi thông tin thanh toán và bản ghi dữ liệu đặt hàng.

8. Phương pháp xử lý thông tin được công bố, trong đó phương pháp này bao gồm các bước:

đọc, từ thông tin được công bố để hiển thị trực quan dựa vào định dạng định trước, giá trị mã hóa thứ nhất mà là của dữ liệu được mã hóa bao gồm thông tin được công bố cuối cùng đứng trước thông tin được công bố và được tính toán bằng cách sử dụng thuật toán mã hóa định trước; hoặc khi thông tin được công bố là đoạn thông tin

được công bố thứ nhất của mục dịch vụ công bố, thì đọc, từ thông tin được công bố, giá trị mã hóa thứ nhất mà là của thông tin ban đầu định trước và được tính toán bằng cách sử dụng thuật toán mã hóa định trước (S101);

tính toán, dựa vào thuật toán mã hóa định trước đã bộc lộ và thông tin được công bố cuối cùng mà đứng trước thông tin được công bố và bao gồm giá trị mã hóa, giá trị mã hóa thứ hai của thông tin được công bố cuối cùng mà bao gồm giá trị mã hóa (S102);

xác định xem giá trị mã hóa thứ nhất có giống với giá trị mã hóa thứ hai hay không (S103); và

đáp lại việc xác định rằng giá trị mã hóa thứ nhất không giống với giá trị mã hóa thứ hai, thì xác định rằng ít nhất một đoạn thông tin được công bố trước thông tin được công bố được sửa đổi (S104).

9. Thiết bị xử lý thông tin được công bố, trong đó thiết bị này bao gồm nhiều bộ phận được tạo cấu hình để thực hiện các hoạt động theo phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 7.

10. Thiết bị xử lý thông tin được công bố, trong đó thiết bị này bao gồm nhiều bộ phận được tạo cấu hình để thực hiện các hoạt động theo phương pháp theo điểm 8.

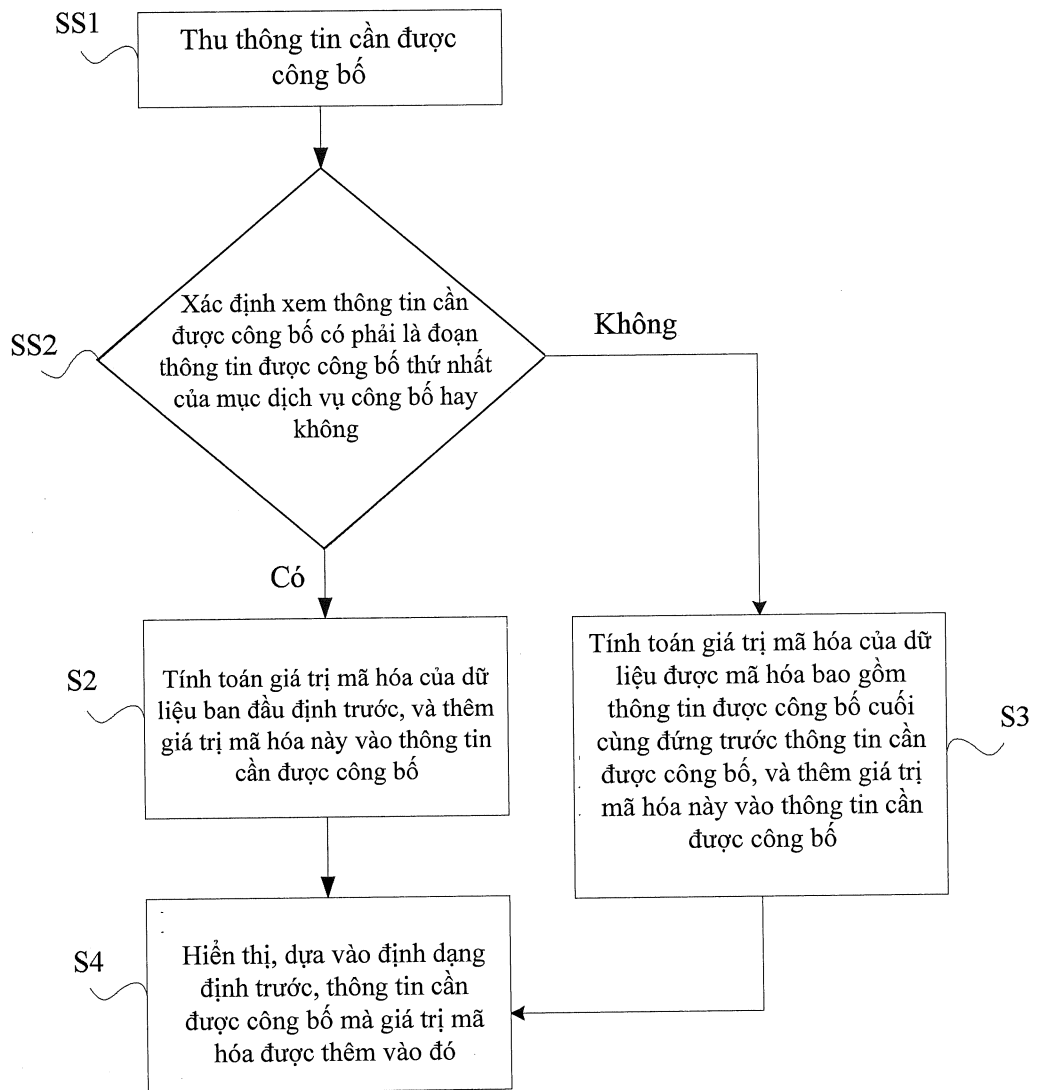


FIG. 1

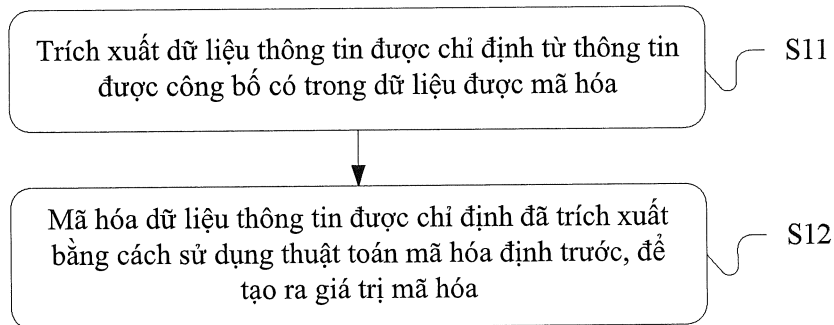


FIG. 2

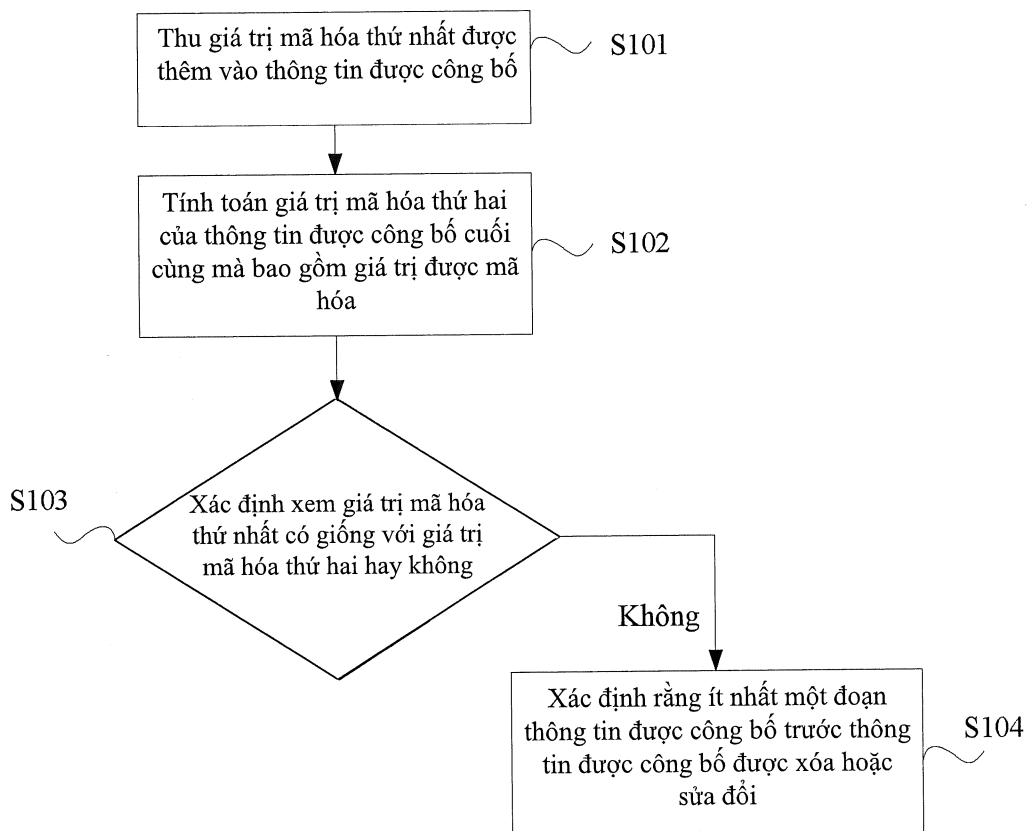


FIG. 3

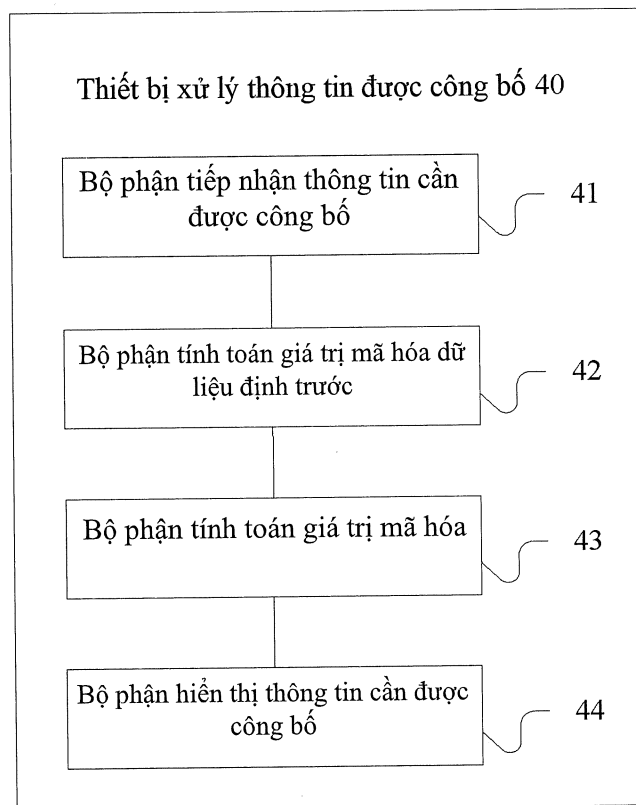


FIG. 4

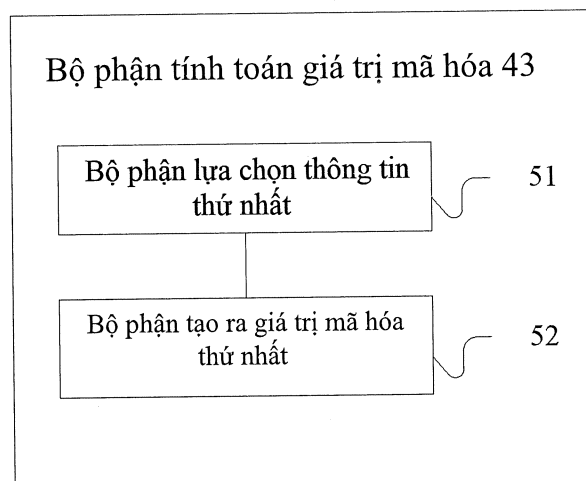


FIG. 5

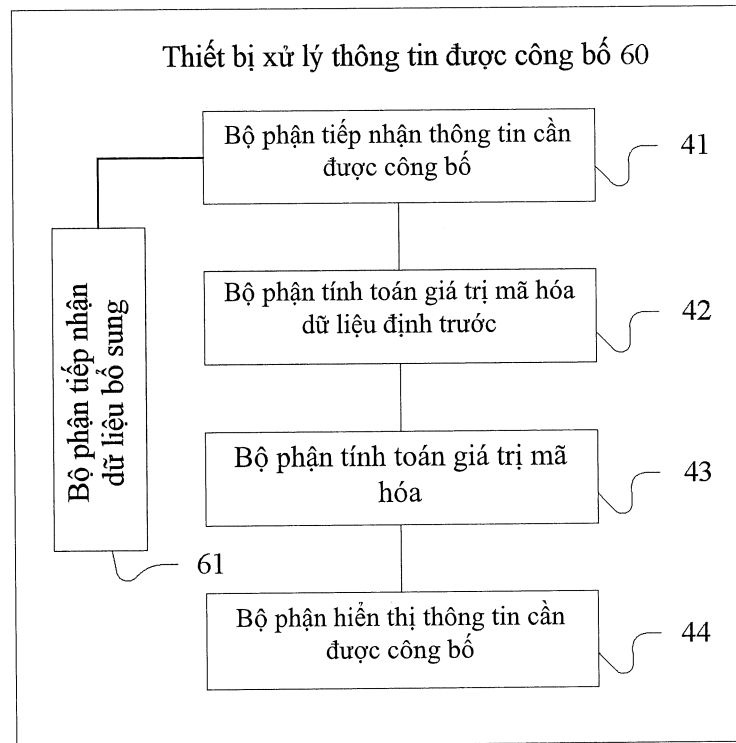


FIG. 6

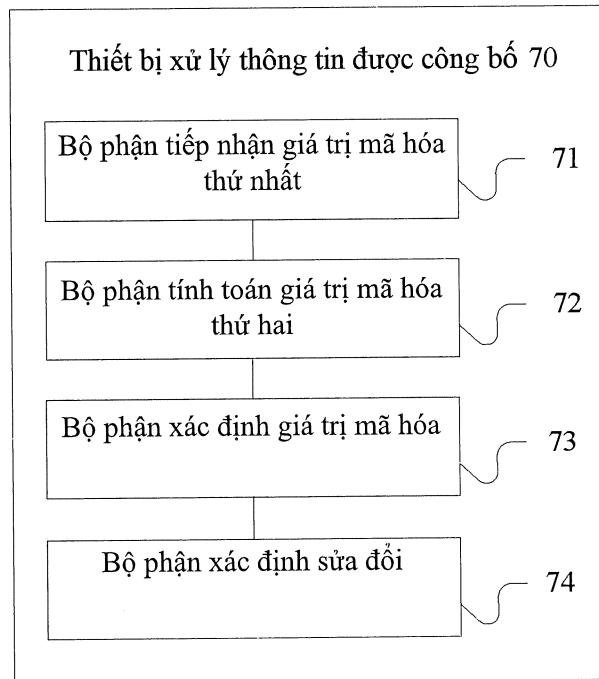


FIG. 7