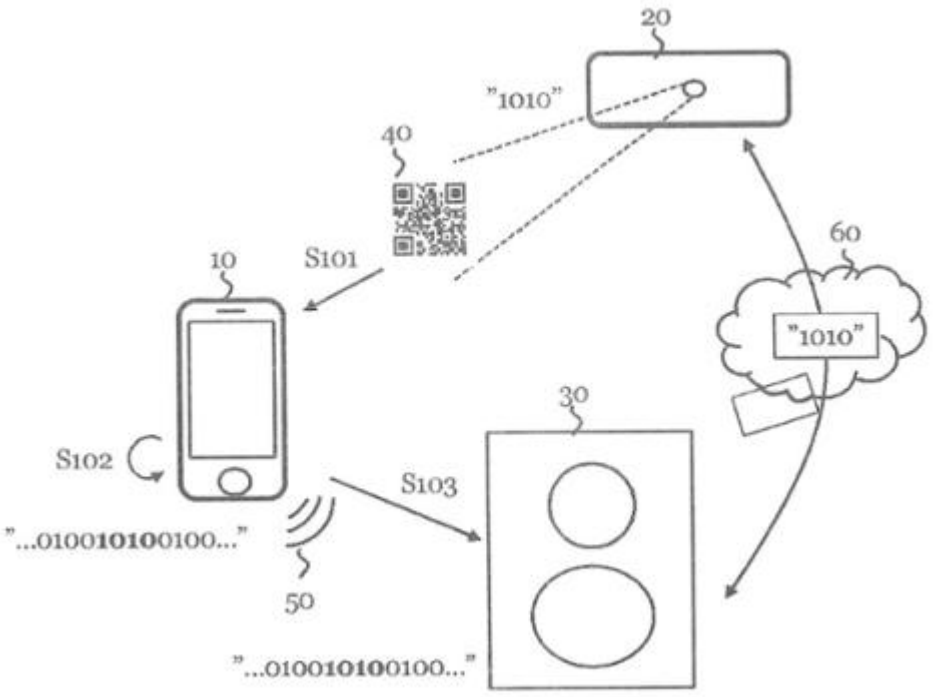
(12) BẢN MÔ TẢ SÁNG CHẾ THUỘC BẰNG ĐỘC QUYỀN SÁNG CHẾ
(19) **Cộng hòa xã hội chủ nghĩa Việt Nam (VN)**
CỤC SỞ HỮU TRÍ TUỆ
(11) **1-0035209**
(51)[8] **H04L 29/06**; H04W 12/04
(13) **B**

(21) 1-2018-01672
(22) 30/10/2015
(86) PCT/EP2015/075225 30/10/2015
(87) WO/2017/071770 04/05/2017
(45) 25/04/2023 421
(43) 25/07/2018 364A
(73) TELEFONAKTIEBOLAGET LM ERICSSON (PUBL) (SE)
SE-164 83 Stockholm, Sweden
(72) ZHANG, Guoqiang (CN); ANDERSSON, Lars (SE); ARAÚJO, José (PT).
(74) Công ty Luật TNHH T&G (TGVN)

(54) PHƯƠNG PHÁP THIẾT LẬP BÍ MẬT DÙNG CHUNG GIỮA THIẾT BỊ TRUYỀN THÔNG THỨ NHẤT VÀ ÍT NHẤT MỘT THIẾT BỊ TRUYỀN THÔNG THỨ HAI, PHƯƠNG TIỆN ĐỌC ĐƯỢC BẰNG MÁY TÍNH, VÀ THIẾT BỊ ĐIỆN TOÁN

(57) Sáng chế đề xuất phương pháp, được thực hiện bởi thiết bị điện toán (10), để thiết lập bí mật dùng chung giữa thiết bị truyền thông thứ nhất (20) và ít nhất một thiết bị truyền thông thứ hai (30). Phương pháp này bao gồm bước thu thập (S101), nhờ sử dụng phương tiện truyền thông thứ nhất với thiết bị truyền thông thứ nhất (20), sự biểu diễn dữ liệu thứ nhất mà từ đó bí mật dùng chung đó có thể được trích xuất. Phương pháp này còn bao gồm bước tạo ra (S102) sự biểu diễn dữ liệu thứ hai từ sự biểu diễn dữ liệu thứ nhất, từ sự biểu diễn dữ liệu thứ hai đó mà bí mật được dùng chung có thể được trích xuất. Ngoài ra, phương pháp này bao gồm bước cung cấp (S103), nhờ sử dụng phương tiện truyền thông thứ hai, sự biểu diễn dữ liệu thứ hai này cho thiết bị truyền thông thứ hai (30), phương tiện truyền thông thứ nhất này là khác với phương tiện truyền thông thứ hai này.



Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập đến các phương pháp thiết lập bí mật dùng chung giữa thiết bị truyền thông thứ nhất và ít nhất một thiết bị truyền thông thứ hai, và các thiết bị điện toán tương ứng. Sáng chế còn đề cập đến các chương trình máy tính để khiến các thiết bị điện toán thực hiện các phương pháp theo sáng chế, và các sản phẩm chương trình máy tính tương ứng.

Tình trạng kỹ thuật của sáng chế

Đối với các thiết bị điện tử, xét từ góc độ máy khách, thì người dùng thường cần một máy tính để bàn dành cho công việc hoặc lúc rảnh rỗi. Đối với các thiết bị điện tử khác, thì người dùng có thể có vài thiết bị, mỗi thiết bị dùng cho một ứng dụng cụ thể, chẳng hạn máy chơi game, hộp thu tín hiệu truyền hình, điện thoại thông minh và đồng hồ, máy tính bảng, máy chơi nhạc trên mạng, v.v..

Ngoài ra, kể từ khi có Internet vạn vật (Internet of Thing - IoT), thì người dùng có thể có nhiều thiết bị điện tử ở nhà mình, thường được gọi chung là các thiết bị giữa máy với máy (Machine to Machine - M2M) dưới dạng, ví dụ, bộ cảm biến nhiệt độ, quần áo thông minh, bộ điều khiển điều nhiệt, v.v..

Ví dụ, người dùng có thể đeo đồng hồ thông minh để theo dõi sức khoẻ và đeo thiết bị gắn trên đầu (Head-Mounted Device - HMD) để giải trí, và đồng thời có điện thoại thông minh để giao tiếp với đồng hồ thông minh và HMD này.

Khi số lượng thiết bị điện tử tăng lên trong cuộc sống hàng ngày, thì việc liên kết hoặc ghép đôi thiết bị sẽ đóng vai trò quan trọng cho việc chia sẻ dữ liệu giữa hai hoặc nhiều thiết bị. Trong nhiều tình huống, thì vài thiết bị điện tử cần phải được kết nối tạm thời để trao đổi thông tin, chẳng hạn chia sẻ hoá đơn ở nhà hàng, hoặc chia sẻ tệp tin PowerPoint giữa những người xem để trình chiếu.

Đã có nhiều giải pháp khác nhau để liên kết hoặc ghép đôi thiết bị. Ví dụ, máy tính bảng mà không có thẻ SIM (Subscriber Identity Module - môđun nhận dạng thuê bao), sau khi hoàn tất tiến trình xác thực thì sẽ có thể cài đặt kết nối WiFi cục bộ với điện thoại thông minh để dùng điện thoại thông minh đó làm HotSpot để truy cập mạng Internet.

Ví dụ khác, ứng dụng có tên là "Bump" (cú chạm) sẽ khởi tạo quá trình ghép đôi của hai thiết bị ngay khi người dùng chạm hai thiết bị đó vào nhau. Sau đó, dữ liệu cảm biến từ bộ cảm biến chuyển động và/hoặc bộ cảm biến gia tốc sẽ được xử lý để liên kết hai thiết bị đó. Có các ví dụ nữa mà trong đó các nhãn thị giác, chẳng hạn các mã phản hồi nhanh (Quick Response - QR) được dùng để liên kết nhiều thiết bị; thiết bị thứ nhất tạo ra và hiển thị nhãn thị giác trên màn hình của nó, và sau đó các thiết bị khác có thể quét nhãn thị giác này nhờ sử dụng camera của chúng để tham gia quá trình truyền thông nhóm. Theo ví dụ nữa, US 7,907,901 đề xuất giải pháp lắc hai thiết bị, trong đó nếu hai thiết bị được lắc theo cách giống nhau thì chúng sẽ tạo ra dữ liệu chuyển động giống nhau, mà dựa trên đó chúng có thể được ghép đôi sau đó.

Vấn đề của các giải pháp theo các ví dụ này là việc cùng một loại cảm biến và phương tiện truyền thông phải được sử dụng giữa các thiết bị; theo ví dụ thứ nhất, thì các thiết bị tham gia vào quá trình truyền thông vô tuyến, theo ví dụ thứ hai và ví dụ thứ tư, thì các bộ cảm biến hướng được sử dụng, còn theo ví dụ thứ ba, thì các thiết bị tương tác bằng cách truyền thông bằng hình.

Bản chất kỹ thuật của sáng chế

Mục đích của sáng chế là giải quyết, hay ít nhất là giảm bớt, vấn đề này trong lĩnh vực, và đề xuất phương pháp cải tiến để tạo điều kiện thuận lợi cho việc thiết lập bí mật mà được dùng chung giữa các thiết bị truyền thông.

Mục đích này là đạt được theo khía cạnh thứ nhất của sáng chế nhờ phương pháp, được thực hiện bởi thiết bị điện toán, để thiết lập bí mật được dùng chung giữa thiết bị truyền thông thứ nhất và ít nhất một thiết bị truyền thông thứ hai. Phương pháp này bao gồm bước thu thập, nhờ sử dụng phương tiện truyền thông thứ nhất với thiết bị truyền thông thứ nhất, sự biểu diễn dữ liệu thứ nhất mà từ đó bí mật được

dùng chung có thể được trích xuất. Phương pháp này còn bao gồm bước tạo ra sự biểu diễn dữ liệu thứ hai từ sự biểu diễn dữ liệu thứ nhất, từ sự biểu diễn dữ liệu thứ hai đó mà bí mật được dùng chung có thể được trích xuất. Ngoài ra, phương pháp này bao gồm bước cung cấp, nhờ sử dụng phương tiện truyền thông thứ hai, sự biểu diễn dữ liệu thứ hai cho thiết bị truyền thông thứ hai, phương tiện truyền thông thứ nhất là khác với phương tiện truyền thông thứ hai.

Mục đích này là đạt được theo khía cạnh thứ hai của sáng chế nhờ thiết bị điện toán được tạo cấu hình để thiết lập bí mật dùng chung giữa thiết bị truyền thông thứ nhất và ít nhất một thiết bị truyền thông thứ hai, thiết bị điện toán này bao gồm khối xử lý và bộ nhớ, bộ nhớ này chứa các lệnh thực thi được bằng khối xử lý này, nhờ đó thiết bị điện toán này hoạt động được để thu thập, nhờ sử dụng phương tiện truyền thông thứ nhất với thiết bị truyền thông thứ nhất, sự biểu diễn dữ liệu thứ nhất mà từ đó bí mật dùng chung này có thể được trích xuất. Thiết bị điện toán này còn hoạt động được để tạo ra sự biểu diễn dữ liệu thứ hai từ sự biểu diễn dữ liệu thứ nhất, từ sự biểu diễn dữ liệu thứ hai đó mà bí mật được dùng chung có thể được trích xuất. Ngoài ra, thiết bị điện toán này hoạt động được để cung cấp, nhờ sử dụng phương tiện truyền thông thứ hai, sự biểu diễn dữ liệu thứ hai cho thiết bị truyền thông thứ hai, phương tiện truyền thông thứ nhất là khác với phương tiện truyền thông thứ hai.

Mục đích này là đạt được theo khía cạnh thứ ba của sáng chế nhờ phương pháp, được thực hiện bởi thiết bị điện toán, để thiết lập bí mật được dùng chung giữa thiết bị truyền thông thứ nhất và ít nhất một thiết bị truyền thông thứ hai. Phương pháp này bao gồm bước thu thập dữ liệu cảm biến mà từ đó bí mật được dùng chung có thể được trích xuất, dữ liệu cảm biến này biểu diễn sự chuyển động mà cả thiết bị điện toán lẫn thiết bị truyền thông thứ nhất được gây ra. Phương pháp này còn bao gồm bước tạo ra sự biểu diễn dữ liệu thứ hai từ dữ liệu cảm biến này, từ sự biểu diễn thứ hai này mà bí mật được dùng chung có thể được trích xuất. Ngoài ra, phương pháp này bao gồm bước cung cấp sự biểu diễn dữ liệu thứ hai này cho thiết bị truyền thông thứ hai.

Mục đích này là đạt được theo khía cạnh thứ tư của sáng chế nhờ thiết bị điện toán được tạo cấu hình để thiết lập bí mật được dùng chung giữa thiết bị truyền thông thứ nhất và ít nhất một thiết bị truyền thông thứ hai, thiết bị điện toán này bao

gồm khối xử lý và bộ nhớ, bộ nhớ này chứa các lệnh thực thi được bằng khối xử lý này, và còn bao gồm bộ cảm biến chuyển động, nhờ đó mà thiết bị điện toán này hoạt động được để thu thập dữ liệu cảm biến của bộ cảm biến chuyển động này mà từ đó bí mật được dùng chung có thể được trích xuất. Dữ liệu cảm biến này biểu diễn sự chuyển động mà cả thiết bị điện toán lẫn thiết bị truyền thông thứ nhất được gây ra. Thiết bị điện toán này còn hoạt động được để tạo ra sự biểu diễn dữ liệu thứ hai từ dữ liệu cảm biến này, từ sự biểu diễn thứ hai này mà bí mật được dùng chung có thể được trích xuất. Ngoài ra, thiết bị điện toán này hoạt động được để cung cấp sự biểu diễn dữ liệu thứ hai này cho thiết bị truyền thông thứ hai.

Mục đích này là đạt được theo khía cạnh thứ năm của sáng chế nhờ chương trình máy tính bao gồm các lệnh thực thi được bằng máy tính để khiến thiết bị thực hiện các bước theo phương án của khía cạnh thứ nhất và/hoặc khía cạnh thứ ba của sáng chế khi các lệnh thực thi được bằng máy tính này được thực thi trên khối xử lý mà được bao gồm trong thiết bị này.

Mục đích này là đạt được theo khía cạnh thứ sáu của sáng chế nhờ sản phẩm chương trình máy tính bao gồm phương tiện đọc được bằng máy tính, phương tiện đọc được bằng máy tính này có chương trình máy tính theo khía cạnh thứ năm được thực hiện trên đó.

Ưu điểm là, với thiết bị điện toán hoạt động như thiết bị chuyển tiếp hoặc thiết bị ủy nhiệm để liên kết nhóm thiết bị với nhau, thì việc liên kết các thiết bị không đồng nhất, tức các thiết bị sử dụng các phương tiện truyền thông khác nhau, là được làm cho khả thi.

Ví dụ, theo khía cạnh thứ nhất của sáng chế, giả sử rằng thiết bị thứ nhất, dưới dạng máy chiếu, cần được ghép đôi/được liên kết với thiết bị thứ hai mà được thực hiện bằng điện thoại hội nghị; máy chiếu này được trang bị nguồn sáng để chiếu các đối tượng thị giác, còn điện thoại hội nghị này thì được trang bị micrô mà qua đó nó có thể nhận các tín hiệu audio.

Do đó, người dùng có thể cho máy chiếu này hiển thị nhãn thị giác, chẳng hạn mã phản hồi nhanh (Quick Response - QR), v.v.. Điều này có thể được thực hiện, ví dụ, bằng cách lệnh cho máy chiếu theo đó bằng cách nhấn nút dành riêng trên cái

điều khiển từ xa mà được liên kết với máy chiếu này, hoặc bằng cách cho máy chiếu này hiển thị mã QR đó ngay khi bật nguồn.

Do đó, người dùng cài đặt quá trình truyền thông giữa máy chiếu và thiết bị chuyển tiếp theo sáng chế, mà là, ví dụ, điện thoại thông minh, nhờ sử dụng phương tiện truyền thông thứ nhất, theo phương án ví dụ này là bằng cách cho điện thoại thông minh này đọc mã QR mà máy chiếu hiển thị lên tường hoặc màn chiếu, bằng camera của điện thoại thông minh này. Mã QR đọc được này cấu thành sự biểu diễn dữ liệu thứ nhất mà từ đó bí mật dùng chung giữa máy chiếu và điện thoại thông minh này có thể được trích xuất, ví dụ, dưới dạng chuỗi nhị phân cụ thể.

Sau đó, người dùng cài đặt quá trình truyền thông giữa điện thoại hội nghị và điện thoại thông minh của mình thông qua phương tiện truyền thông thứ hai, theo ví dụ này là bằng cách truyền tín hiệu audio, mà micrô của điện thoại hội nghị này thu được, để cung cấp bí mật dùng chung đó cho điện thoại hội nghị này.

Trước khi cung cấp tín hiệu audio đó, thì điện thoại thông minh này tạo ra sự biểu diễn dữ liệu thứ hai từ sự biểu diễn dữ liệu thứ nhất thu thập được, từ sự biểu diễn dữ liệu thứ hai này mà điện thoại hội nghị này có thể trích xuất bí mật dùng chung đó. Do đó, để cung cấp cho điện thoại hội nghị dữ liệu mà từ đó bí mật dùng chung có thể được trích xuất, thì sự biểu diễn dữ liệu thứ nhất được mã hoá vào tín hiệu audio mà được truyền đến điện thoại hội nghị. Nhờ đó, sự biểu diễn dữ liệu thứ hai được tạo ra, mà từ đó bí mật dùng chung (dưới dạng chuỗi nhị phân nêu trên) có thể được điện thoại hội nghị trích xuất.

Ưu điểm là, điện thoại thông minh này cho phép truyền thông bảo mật giữa máy chiếu và điện thoại hội nghị; sau đó, khi hai thiết bị này thiết lập quá trình truyền thông qua, ví dụ, Bluetooth, WiFi, hoặc mạng Internet, v.v, thì chúng đều có truy cập đến bí mật dùng chung đó, tức chuỗi nhị phân mà được dùng làm ví dụ trên đây, và quá trình truyền thông bảo mật có thể được thực hiện.

Theo khía cạnh thứ hai của sáng chế, giả sử rằng thiết bị thứ nhất, dưới dạng máy tính bảng, cần được ghép đôi/được liên kết với thiết bị thứ hai, vẫn được thực hiện bằng điện thoại hội nghị; máy tính bảng này được trang bị bộ cảm biến chuyển động, chẳng hạn gia tốc kế, còn điện thoại hội nghị này được trang bị micrô mà qua đó nó có thể nhận các tín hiệu audio.

Người dùng khởi tạo quá trình ghép đôi, ví dụ, bằng cách chạm thiết bị chuyển tiếp là điện thoại thông minh của mình vào máy tính bảng, hoặc theo cách khác là bằng cách lắc điện thoại thông minh cùng với máy tính bảng. Theo cách nào thì bộ cảm biến chuyển động của điện thoại thông minh cũng sẽ tạo ra dữ liệu cảm biến mà từ đó bí mật dùng chung có thể được trích xuất, dữ liệu cảm biến này biểu diễn sự chuyển động mà cả điện thoại thông minh lẫn máy tính bảng này được gây ra. Bí mật dùng chung này có thể được biểu diễn bằng chuỗi nhị phân cụ thể.

Tương tự như phương án ví dụ đã nêu đối với khía cạnh thứ nhất của sáng chế, sự biểu diễn dữ liệu thứ hai, mà từ đó bí mật dùng chung có thể được trích xuất, là được điện thoại thông minh này tạo ra và được cung cấp cho điện thoại hội nghị.

Tuy nhiên, theo khía cạnh thứ hai, thì điện thoại thông minh tạo ra sự biểu diễn dữ liệu thứ hai từ dữ liệu cảm biến thu thập được, từ sự biểu diễn dữ liệu thứ hai đó mà bí mật dùng chung đó có thể được điện thoại hội nghị trích xuất. Do đó, để cung cấp cho điện thoại hội nghị dữ liệu mà từ đó bí mật dùng chung có thể được trích xuất, thì ít nhất một phần của dữ liệu cảm biến này được mã hoá vào tín hiệu audio mà được truyền đến điện thoại hội nghị. Nhờ đó, sự biểu diễn dữ liệu thứ hai được tạo ra, mà từ đó bí mật dùng chung (dưới dạng chuỗi nhị phân nêu trên) có thể được điện thoại hội nghị trích xuất.

Ưu điểm là, điện thoại thông minh này cho phép truyền thông bảo mật giữa máy tính bảng và điện thoại hội nghị; sau đó, khi hai thiết bị này thiết lập quá trình truyền thông qua, ví dụ, Bluetooth, WiFi, hoặc mạng Internet, v.v, thì chúng đều có truy cập đến bí mật dùng chung đó, tức chuỗi nhị phân mà được tạo ra ngay khi chạm hoặc lắc máy tính bảng và điện thoại thông minh cùng nhau, và quá trình truyền thông bảo mật có thể được thực hiện.

Theo một phương án của sáng chế, dữ liệu cảm biến chuyển động này biểu thị sự tiếp xúc vật lý với thiết bị truyền thông thứ nhất. Do đó, thiết bị điện toán và thiết bị truyền thông thứ nhất có thể, theo cách có lợi, được chạm vào nhau để khởi tạo quá trình thiết lập bí mật được dùng chung.

Theo phương án khác của sáng chế, dữ liệu cảm biến chuyển động này biểu diễn mẫu chuyển động chung với thiết bị truyền thông thứ nhất. Do đó, thiết bị điện

toán và thiết bị truyền thông thứ nhất có thể được lắc theo cách có lợi cùng nhau để khởi tạo quá trình thiết lập bí mật được dùng chung.

Theo phương án nữa của sáng chế, bí mật dùng chung giữa thiết bị truyền thông thứ nhất và nhóm thiết bị truyền thông thứ hai được thiết lập, trong trường hợp đó, nhóm thiết bị truyền thông thứ hai này được cung cấp sự biểu diễn dữ liệu thứ hai.

Theo phương án khác nữa của sáng chế, nhất hai trong số các thiết bị truyền thông thứ hai trong nhóm này là được cung cấp sự biểu diễn dữ liệu thứ hai thông qua các phương tiện truyền thông khác nhau. Ví dụ, một trong số các thiết bị truyền thông thứ hai này được cung cấp sự biểu diễn dữ liệu thứ hai về mặt thị giác, còn thiết bị còn lại thì được cung cấp sự biểu diễn dữ liệu thứ hai về mặt thính giác.

Theo phương án khác nữa của sáng chế, thì thiết bị điện toán trích xuất bí mật dùng chung từ sự biểu diễn dữ liệu thứ nhất hoặc dữ liệu cảm biến chuyển động, tuỳ theo cái nào áp dụng được, và thiết lập quá trình truyền thông bảo mật với thiết bị truyền thông thứ nhất và/hoặc ít nhất một thiết bị truyền thông thứ hai nhờ sử dụng bí mật dùng chung trích xuất được.

Theo một phương án, bước thu thập sự biểu diễn dữ liệu thứ nhất, mà từ đó bí mật dùng chung có thể được trích xuất, bao gồm một trong số các bước: thu thập, về mặt thị giác, sự biểu diễn dữ liệu thứ nhất, thu thập, về mặt thính giác, sự biểu diễn dữ liệu thứ nhất, và thu thập sự biểu diễn dữ liệu thứ nhất qua kênh truyền thông vô tuyến không dây.

Theo phương án khác, bước cung cấp sự biểu diễn dữ liệu thứ hai, mà từ đó bí mật dùng chung có thể được trích xuất, bao gồm một trong số các bước: cung cấp, về mặt thị giác, sự biểu diễn dữ liệu thứ hai, cung cấp, về mặt thính giác, sự biểu diễn dữ liệu thứ hai, và cung cấp sự biểu diễn dữ liệu thứ hai qua kênh truyền thông vô tuyến không dây.

Nói chung, tất cả các thuật ngữ mà được sử dụng ở các điểm yêu cầu bảo hộ là cần được hiểu theo nghĩa thông thường của chúng trong lĩnh vực kỹ thuật này, trừ khi được xác định khác đi một cách rõ ràng. Tất cả những sự viện dẫn đến "phần tử, thiết bị, thành phần, phương tiện, bước, v.v." là cần được hiểu theo cách mở dưới dạng viện dẫn đến ít nhất một hiện thân của phần tử, thiết bị, thành phần, phương tiện, bước đó, v.v., trừ khi được nói khác đi một cách rõ ràng. Các bước của phương

pháp bất kỳ được bộc lộ ở đây là không nhất thiết phải được thực hiện chính xác theo thứ tự được bộc lộ, trừ khi được nêu rõ.

Mô tả vắn tắt các hình vẽ

Sáng chế sẽ được mô tả làm ví dụ có dựa vào các hình vẽ kèm theo, trong đó:

Fig.1 là hình vẽ thể hiện thiết bị điện toán theo một phương án của sáng chế, được tạo cấu hình để thiết lập bí mật được dùng chung giữa thiết bị truyền thông thứ nhất và ít nhất một thiết bị truyền thông thứ hai;

Fig.2 là hình vẽ thể hiện lưu đồ, theo một phương án, của phương pháp được thực hiện bởi thiết bị điện toán trên Fig.1, để thiết lập bí mật được dùng chung giữa thiết bị truyền thông thứ nhất và thiết bị truyền thông thứ hai;

Fig.3 là hình vẽ thể hiện thiết bị điện toán theo phương án khác của sáng chế, được tạo cấu hình để thiết lập bí mật được dùng chung giữa thiết bị truyền thông thứ nhất và ít nhất một thiết bị truyền thông thứ hai;

Fig.4 là hình vẽ thể hiện lưu đồ, theo một phương án, của phương pháp được thực hiện bởi thiết bị điện toán trên Fig.3, để thiết lập bí mật được dùng chung giữa thiết bị truyền thông thứ nhất và thiết bị truyền thông thứ hai;

Fig.5 là hình vẽ thể hiện thiết bị điện toán theo một phương án của sáng chế;

Fig.6 là hình vẽ thể hiện thiết bị điện toán theo phương án khác của sáng chế;

Fig.7 là hình vẽ thể hiện thiết bị điện toán theo phương án nữa của sáng chế, được tạo cấu hình để thiết lập bí mật được dùng chung giữa thiết bị truyền thông thứ nhất và nhóm thiết bị truyền thông thứ hai;

Fig.8 là hình vẽ thể hiện thiết bị điện toán theo một phương án của sáng chế; và

Fig.9 là hình vẽ thể hiện thiết bị điện toán theo phương án khác của sáng chế.

Mô tả chi tiết sáng chế

Sáng chế sẽ được mô tả đầy đủ hơn dưới đây dựa vào các hình vẽ kèm theo, trong đó các phương án nhất định của sáng chế được thể hiện. Tuy nhiên, sáng chế có thể được thực hiện dưới nhiều dạng khác nhau chứ không chỉ giới hạn ở các phương án được nêu ở đây; thay vào đó, các phương án này chỉ được cung cấp làm ví dụ để bản mô tả này trở nên hoàn chỉnh, và sẽ chuyển tải đầy đủ phạm vi của sáng

chế đến những người có kiến thức trung bình trong lĩnh vực. Các số chỉ dẫn giống nhau được dùng để chỉ các phần tử giống nhau trong suốt bản mô tả này.

Fig.1 là hình vẽ thể hiện thiết bị điện toán 10 theo một phương án của sáng chế, được tạo cấu hình để thiết lập bí mật được dùng chung giữa thiết bị truyền thông thứ nhất 20 và ít nhất một thiết bị truyền thông thứ hai 30.

Fig.2 là hình vẽ thể hiện lưu đồ, theo một phương án, của phương pháp được thực hiện bởi thiết bị điện toán 10 trên Fig.1, để thiết lập bí mật được dùng chung giữa thiết bị truyền thông thứ nhất 20 và thiết bị truyền thông thứ hai 30.

Thiết bị điện toán 10 được thực hiện dưới dạng điện thoại thông minh trên Fig.1, còn thiết bị truyền thông thứ nhất 20 được thực hiện dưới dạng máy chiếu, và thiết bị truyền thông thứ hai 30 được thực hiện dưới dạng điện thoại hội nghị.

Để thiết lập bí mật được dùng chung giữa máy chiếu 20 và điện thoại hội nghị 30 để cho phép quá trình truyền thông bảo mật sau đó giữa hai thiết bị này, thì người dùng có thể cho máy chiếu hiển thị nhãn thị giác, mà theo ví dụ cụ thể này là mã QR 40.

Người dùng sẽ cho điện thoại thông minh 10 đọc mã QR 40 bằng camera để thu thập sự biểu diễn dữ liệu thứ nhất mà từ đó bí mật dùng chung có thể được trích xuất. Theo ví dụ được thể hiện trên Fig.1, thì sự biểu diễn dữ liệu thứ nhất bao gồm chuỗi nhị phân "...010010100100..." mà từ đó bí mật dùng chung này có thể được trích xuất. Theo ví dụ cụ thể này, bí mật dùng chung này được thực hiện bởi chuỗi 4 bit "1010" được đặt rải rác vào sự biểu diễn dữ liệu thứ nhất.

Ở bước S102, điện thoại di động 10 tạo ra sự biểu diễn dữ liệu thứ hai từ sự biểu diễn dữ liệu thứ nhất, từ sự biểu diễn dữ liệu thứ hai đó mà bí mật được dùng chung có thể được trích xuất.

Theo ví dụ này, sự biểu diễn dữ liệu thứ hai này được cung cấp cho điện thoại hội nghị 30 từ điện thoại thông minh 10 qua tín hiệu audio 50 mà micrô của điện thoại hội nghị 30 thu được. Do đó, để cung cấp cho điện thoại hội nghị dữ liệu mà từ đó bí mật dùng chung có thể được trích xuất, thì sự biểu diễn dữ liệu thứ nhất được mã hoá vào tín hiệu audio 50 mà được truyền đến điện thoại hội nghị 30 ở bước S103. Nhờ đó, sự biểu diễn dữ liệu thứ hai được tạo ra, mà từ đó bí mật dùng chung (dưới dạng chuỗi 4 bit nêu trên) có thể được điện thoại hội nghị trích xuất.

Ưu điểm là điện thoại thông minh 10 cho phép quá trình truyền thông bảo mật giữa máy chiếu 20 và điện thoại hội nghị 30, mà mỗi trong số đó đều truyền thông với điện thoại thông minh 10 bằng các phương tiện truyền thông khác nhau. Sau đó, khi hai thiết bị này thiết lập quá trình truyền thông qua, ví dụ, mạng WiFi cục bộ 60, thì chúng đều có truy cập đến bí mật được dùng chung nêu trên, tức chuỗi 4 bit "1010", và quá trình truyền thông bảo mật có thể được thực hiện.

Cần lưu ý rằng bí mật được dùng chung và sự biểu diễn dữ liệu thứ nhất và sự biểu diễn dữ liệu thứ hai có thể có cấu trúc khác so với như được thể hiện trên Fig.1. Cần lưu ý thêm rằng việc thiết lập quá trình truyền thông bảo mật giữa máy chiếu 20 và điện thoại hội nghị 30 có thể được thực hiện thông qua thiết bị chẳng hạn như máy chủ (không được thể hiện trên hình vẽ), trước khi kênh truyền thông bảo mật có thể được cài đặt giữa hai thiết bị này. Ngoài ra, sự biểu diễn dữ liệu thứ nhất và sự biểu diễn dữ liệu thứ hai được thể hiện là bao gồm bí mật dùng chung 4 bit được đặt rải rác trong mã dài hơn. Tuy nhiên, cũng có thể thấy rằng sự biểu diễn dữ liệu thứ nhất và sự biểu diễn dữ liệu thứ hai trên thực tế chỉ bao gồm bí mật được dùng chung này.

Fig.3 là hình vẽ thể hiện thiết bị điện toán 10 theo phương án nữa của sáng chế, được tạo cấu hình để thiết lập bí mật được dùng chung giữa thiết bị truyền thông thứ nhất 20 và ít nhất một thiết bị truyền thông thứ hai 30.

Fig.4 là hình vẽ thể hiện lưu đồ, theo một phương án, của phương pháp được thực hiện bởi thiết bị điện toán 10 trên Fig.3, để thiết lập bí mật được dùng chung giữa thiết bị truyền thông thứ nhất 20 và thiết bị truyền thông thứ hai 30.

Thiết bị điện toán 10 vẫn được thực hiện dưới dạng điện thoại thông minh, và thiết bị truyền thông thứ hai 30 vẫn được thực hiện dưới dạng điện thoại hội nghị, còn thiết bị truyền thông thứ nhất 20 theo phương án cụ thể này thì được thực hiện bằng máy tính bảng.

Theo phương án này, để thiết lập bí mật được dùng chung giữa máy tính bảng 20 và điện thoại hội nghị 30 để cho phép quá trình truyền thông bảo mật sau đó giữa hai thiết bị này, thì người dùng chạm điện thoại thông minh 10 của mình vào máy tính bảng. Khối đo quán tính (Inertia Measurement Unit - IMU) tương ứng ở điện thoại thông minh 10 và máy tính bảng 20 sẽ ghi nhận sự chuyển động mà hai

thiết bị này được gây ra. IMU này có thể là gia tốc kế, con quay hồi chuyển, từ kế hoặc tổ hợp của hai hoặc nhiều trong số các loại cảm biến chuyển động này.

Từ sự chuyển động mà điện thoại thông minh 10 và máy tính bảng 20 được gây ra, thì có thể xác định xem có đúng là hai thiết bị này được làm chạm vào nhau hay không, do đó, bí mật dùng chung có thể được thiết lập. Như đã nêu trên, sự chuyển động này có thể được thực hiện bởi sự di chuyển của điện thoại thông minh 10 và máy tính bảng theo mẫu chung, chẳng hạn người dùng cầm hai thiết bị này trong cùng một bàn tay và lắc chúng qua lại.

Bằng cách lắc hai thiết bị này, thì sự chuyển động (tức gia tốc) mà hai thiết bị này được gây ra sẽ được dùng để tạo ra bí mật, chẳng hạn khoá, sau đó khoá này được dùng để thiết lập kết nối bảo mật. Do hai thiết bị này được di chuyển cùng nhau, nên chúng thực hiện sự chuyển động giống nhau, do đó, ghi được dữ liệu chuyển động gần như giống nhau. Từ dữ liệu chuyển động giống nhau này, thì các bản sao giống nhau của bí mật dùng chung đó có thể được thiết lập.

Do đó, điện thoại thông minh 10 thu được dữ liệu cảm biến ở bước S201 từ IMU của nó, từ dữ liệu đó mà bí mật dùng chung có thể được trích xuất. Dữ liệu cảm biến thu thập được này biểu diễn sự chuyển động chạm vào nhau mà điện thoại thông minh 10 và máy tính bảng 20 được gây ra. Theo ví dụ được thể hiện trên Fig.3, thì dữ liệu cảm biến này bao gồm chuỗi nhị phân "...0100**1010**0100..." mà từ đó bí mật dùng chung có thể được trích xuất. Theo ví dụ cụ thể này, thì bí mật dùng chung này được thực hiện bởi chuỗi 4 bit "1010" được đặt rải rác vào dữ liệu cảm biến này.

Cũng như theo phương án đã mô tả trên đây dựa vào Fig.1, điện thoại thông minh 10 cần phải tạo ra sự biểu diễn dữ liệu thứ hai ở định dạng mà có thể được truyền đến, và được hiểu bởi, điện thoại hội nghị 30.

Do đó, ở bước S202, điện thoại di động 10 tạo ra sự biểu diễn dữ liệu thứ hai từ dữ liệu cảm biến này, từ sự biểu diễn dữ liệu thứ hai này mà bí mật dùng chung có thể được trích xuất.

Sự biểu diễn dữ liệu thứ hai này cũng vẫn được cung cấp cho điện thoại hội nghị 30 từ điện thoại thông minh 10 qua tín hiệu audio 50 mà micrô của điện thoại hội nghị 30 thu được. Do đó, để cung cấp cho điện thoại hội nghị dữ liệu mà từ đó bí

mật dùng chung có thể được trích xuất, thì dữ liệu cảm biến này được mã hoá vào tín hiệu audio 50 mà được truyền đến điện thoại hội nghị 30 ở bước S203. Nhờ đó, sự biểu diễn dữ liệu thứ hai được tạo ra, mà từ đó bí mật dùng chung (dưới dạng chuỗi 4 bit nêu trên) có thể được điện thoại hội nghị 30 trích xuất.

Ưu điểm là điện thoại thông minh 10 cho phép truyền thông bảo mật giữa máy tính bảng 20 và điện thoại hội nghị 30. Sau đó, khi máy tính bảng 20 và điện thoại hội nghị 30 này thiết lập quá trình truyền thông qua mạng WiFi 60, thì chúng đều có truy cập đến bí mật được dùng chung nêu trên, tức chuỗi 4 bit "1010", và quá trình truyền thông bảo mật có thể được thực hiện.

Như được thể hiện trên các hình vẽ Fig.5 và Fig.6, các bước của phương pháp mà được thực hiện bởi thiết bị điện toán 10 theo các phương án của sáng chế trên thực tế là được thực hiện bởi khối xử lý 11 mà được thực hiện dưới dạng một hoặc nhiều bộ vi xử lý mà được bố trí để thực thi chương trình máy tính 12 mà được tải xuống phương tiện lưu trữ 13 phù hợp mà được liên kết với bộ vi xử lý này, chẳng hạn bộ nhớ truy cập ngẫu nhiên (Random Access Memory - RAM), bộ nhớ flash hoặc ổ đĩa cứng. Khối xử lý 11 được bố trí để làm cho thiết bị điện toán 10 thực hiện phương pháp theo các phương án của sáng chế khi chương trình máy tính 12 thích hợp, mà bao gồm các lệnh thực thi được bằng máy tính, được tải xuống phương tiện lưu trữ 13 và được thực thi bởi khối xử lý 11. Phương tiện lưu trữ 13 này cũng có thể là sản phẩm chương trình máy tính mà bao gồm chương trình máy tính 12. Theo cách khác, chương trình máy tính 12 có thể được chuyển sang phương tiện lưu trữ 13 bằng sản phẩm chương trình máy tính phù hợp, chẳng hạn đĩa DVD (Digital Versatile Disc - đĩa đa năng kỹ thuật số) hoặc thẻ nhớ. Theo phương án khác nữa, chương trình máy tính 12 có thể được tải xuống phương tiện lưu trữ 13 qua mạng. Theo cách khác, khối xử lý 11 có thể được thực hiện dưới dạng bộ xử lý tín hiệu số (Digital Signal Processor - DSP), mạch tích hợp chuyên dụng (Application Specific Integrated Circuit - ASIC), mảng cổng lập trình được dạng trường (Field-Programmable Gate Array - FPGA), thiết bị logic phức lập trình được (Complex Programmable Logic Device - CPLD), v.v..

Như được thể hiện trên Fig.6, trong trường hợp dữ liệu cảm biến chuyển động được thu thập mà từ đó bí mật dùng chung có thể được trích xuất, thì thiết bị điện

toán 10 được trang bị IMU 14 như đã mô tả trên đây. Sẽ có lợi nếu thiết bị điện toán 10 được thực hiện bằng điện thoại thông minh, vì điện thoại thông minh thì thường có IMU 14.

Fig.7 là hình vẽ thể hiện thiết bị điện toán 10 theo phương án nữa của sáng chế, được tạo cấu hình để thiết lập bí mật dùng chung giữa máy tính bảng 20 và nhóm thiết bị truyền thông thứ hai, theo phương án ví dụ này thì điện thoại hội nghị 30 và máy chơi nhạc trên mạng 70 đang giao tiếp qua, ví dụ, các tín hiệu hồng ngoại (InfraRed - IR).

Để thiết lập bí mật dùng chung giữa máy tính bảng 20, điện thoại hội nghị 30 và máy chơi nhạc trên mạng 70 để cho phép truyền thông bảo mật sau đó giữa ba thiết bị này, thì người dùng chạm điện thoại thông minh 10 vào máy tính bảng 20. IMU tương ứng ở điện thoại thông minh 10 và máy tính bảng 20 sẽ ghi nhận sự chuyển động mà hai thiết bị này được gây ra, như đã được mô tả dựa vào Fig.3.

Do đó, điện thoại thông minh 10 thu được dữ liệu cảm biến ở bước S201 từ IMU của nó, từ dữ liệu đó mà bí mật dùng chung có thể được trích xuất. Dữ liệu cảm biến thu thập được này biểu diễn sự chuyển động chạm vào nhau mà điện thoại thông minh 10 và máy tính bảng 20 được gây ra. Theo ví dụ được thể hiện trên Fig.7, thì dữ liệu cảm biến này bao gồm chuỗi nhị phân "...010010100100..." mà từ đó bí mật dùng chung có thể được trích xuất. Bí mật dùng chung này cũng vẫn được thực hiện bởi chuỗi 4 bit "1010" được đặt rải rác vào dữ liệu cảm biến này.

Ở bước S202, thì điện thoại di động 10 tạo ra sự biểu diễn dữ liệu thứ hai từ dữ liệu cảm biến này, từ sự biểu diễn dữ liệu thứ hai này mà bí mật dùng chung có thể được trích xuất. Trong trường hợp nhóm thiết bị truyền thông thứ hai đang truyền thông với điện thoại thông minh 10 qua các phương tiện truyền thông giống nhau, thì nhóm thiết bị này có thể đã sử dụng cùng một sự biểu diễn dữ liệu thứ hai.

Tuy nhiên, theo phương án ví dụ này, thì điện thoại thông minh 10 cần phải tạo ra sự biểu diễn dữ liệu thứ hai ở định dạng mà có thể được truyền đến, và được hiểu bởi, điện thoại hội nghị 30 cũng như máy chơi nhạc trên mạng 70.

Như đã mô tả trước đó, sự biểu diễn dữ liệu thứ hai này là được cung cấp cho điện thoại hội nghị 30 từ điện thoại thông minh 10 qua tín hiệu audio 50 mà micrô của điện thoại hội nghị 30 thu được. Do đó, để cung cấp cho điện thoại hội nghị dữ

liệu mà từ đó bí mật dùng chung có thể được trích xuất, thì dữ liệu cảm biến này được mã hoá vào tín hiệu audio 50 mà được truyền đến điện thoại hội nghị 30 ở bước S203. Nhờ đó, sự biểu diễn dữ liệu thứ hai được tạo ra, mà từ đó bí mật dùng chung (dưới dạng chuỗi 4 bit nêu trên) có thể được điện thoại hội nghị 30 trích xuất.

Ngoài ra, sự biểu diễn dữ liệu thứ hai này được cung cấp cho máy chơi nhạc trên mạng 70 từ điện thoại thông minh 10 thông qua tín hiệu IR 80 mà bộ cảm biến IR của máy chơi nhạc 70 thu được. Do đó, để cung cấp cho máy chơi nhạc trên mạng dữ liệu mà từ đó bí mật dùng chung có thể được trích xuất, thì dữ liệu cảm biến này được mã hoá vào tín hiệu IR 80 mà được truyền đến máy chơi nhạc trên mạng 70 ở bước S203, nhờ sử dụng giao thức phù hợp. Nhờ đó, sự biểu diễn dữ liệu thứ hai được tạo ra, mà từ đó bí mật dùng chung 4-bit đó có thể được máy chơi nhạc trên mạng 70 trích xuất.

Theo phương án cụ thể này, thì máy chơi nhạc trên mạng 70 được cung cấp sự biểu diễn dữ liệu thứ hai thông qua phương tiện truyền thông thứ ba - trong trường hợp này là các tín hiệu IR - khác với phương tiện truyền thông thứ hai (và phương tiện truyền thông thứ nhất), mà trong trường hợp này là các tín hiệu audio. Cần lưu ý rằng các phương tiện truyền thông mà được dùng để cung cấp sự biểu diễn dữ liệu thứ hai cho điện thoại hội nghị 30 và máy chơi nhạc trên mạng 70 là có thể giống nhau.

Ưu điểm là điện thoại thông minh 10 cho phép truyền thông bảo mật giữa máy tính bảng 20, điện thoại hội nghị 30 và máy chơi nhạc 70. Sau đó, khi máy tính bảng 20 thiết lập quá trình truyền thông qua mạng WiFi 60 với điện thoại hội nghị 30 và máy chơi nhạc trên mạng 70, thì chúng đều có truy cập đến bí mật dùng chung đó, tức chuỗi 4 bit "1010", và quá trình truyền thông bảo mật có thể được thực hiện.

Cần lưu ý rằng sự biểu diễn dữ liệu thứ nhất/dữ liệu cảm biến, và sau đó là sự biểu diễn dữ liệu thứ hai, là có thể bao gồm các thông tin chẳng hạn như số nhận dạng của phiên truyền thông bảo mật cần được thiết lập, thời lượng cho phép của phiên, vị trí địa lý, mốc thời gian, số lượng thiết bị tối đa tham gia vào quá trình truyền thông, v.v..

Theo phương án nữa của sáng chế, thì (các) kênh truyền thông bảo mật có thể được cài đặt giữa thiết bị điện toán và thiết bị truyền thông thứ nhất 20, và có thể là

với một hoặc nhiều thiết bị bất kỳ trong số (các) thiết bị truyền thông thứ hai 30, 70, và do đó, thiết bị điện toán 10 có thể tham gia vào quá trình thiết lập phiên truyền thông; thiết bị điện toán 10 dễ dàng có truy cập đến sự biểu diễn dữ liệu thứ nhất/dữ liệu cảm biến mà từ đó bí mật dùng chung có thể được trích xuất.

Fig.8 là hình vẽ thể hiện thiết bị điện toán 10 theo phương án nữa của sáng chế, được tạo cấu hình để thiết lập bí mật được dùng chung giữa thiết bị truyền thông thứ nhất và ít nhất một thiết bị truyền thông thứ hai. Thiết bị điện toán 10 này bao gồm phương tiện thu thập 101 được làm thích ứng để thu thập, nhờ sử dụng phương tiện truyền thông thứ nhất với thiết bị truyền thông thứ nhất, sự biểu diễn dữ liệu thứ nhất mà từ đó bí mật dùng chung có thể được trích xuất, phương tiện tạo 102 được làm thích ứng để tạo ra sự biểu diễn dữ liệu thứ hai từ sự biểu diễn dữ liệu thứ nhất, từ sự biểu diễn dữ liệu thứ hai này mà bí mật dùng chung đó có thể được trích xuất, và phương tiện cung cấp 103 được làm thích ứng để cung cấp, nhờ sử dụng phương tiện truyền thông thứ hai, sự biểu diễn dữ liệu thứ hai này cho thiết bị truyền thông thứ hai, phương tiện truyền thông thứ nhất này là khác với phương tiện truyền thông thứ hai này.

Các phương tiện từ 101 đến 103 này có thể bao gồm giao diện truyền thông để nhận và cung cấp các thông tin, và còn bao gồm bộ lưu trữ cục bộ để lưu dữ liệu, và (tương tự như phần mô tả liên quan đến Fig.5) có thể được thực hiện bằng bộ xử lý mà được thực hiện dưới dạng một hoặc nhiều bộ vi xử lý mà được bố trí để thực hiện chương trình máy tính mà được tải xuống phương tiện lưu trữ phù hợp mà được liên kết với bộ vi xử lý này, chẳng hạn RAM, bộ nhớ Flash hoặc ổ đĩa cứng.

Fig.9 là hình vẽ thể hiện thiết bị điện toán 10 theo phương án nữa của sáng chế, được tạo cấu hình để thiết lập bí mật được dùng chung giữa thiết bị truyền thông thứ nhất và ít nhất một thiết bị truyền thông thứ hai. Thiết bị điện toán 10 này bao gồm phương tiện thu thập 201 được làm thích ứng để thu thập dữ liệu cảm biến mà từ đó bí mật dùng chung có thể được trích xuất, dữ liệu cảm biến này biểu diễn sự chuyển động mà cả thiết bị điện toán lẫn thiết bị truyền thông thứ nhất được gây ra, phương tiện tạo 202 được làm thích ứng để tạo ra sự biểu diễn dữ liệu thứ hai từ dữ liệu cảm biến này, từ sự biểu diễn thứ hai này mà bí mật dùng chung có thể được trích xuất,

và phương tiện cung cấp 203 được làm thích ứng để cung cấp sự biểu diễn dữ liệu thứ hai này cho thiết bị truyền thông thứ hai.

Các phương tiện từ 201 đến 203 này có thể bao gồm giao diện truyền thông để nhận và cung cấp các thông tin, và còn bao gồm bộ lưu trữ cục bộ để lưu dữ liệu, và (tương tự như phần mô tả liên quan đến Fig.6) có thể được thực hiện bằng bộ xử lý mà được thực hiện dưới dạng một hoặc nhiều bộ vi xử lý mà được bố trí để thực hiện chương trình máy tính mà được tải xuống phương tiện lưu trữ phù hợp mà được liên kết với bộ vi xử lý này, chẳng hạn RAM, bộ nhớ Flash hoặc ổ đĩa cứng.

Sáng chế đã được mô tả chủ yếu trên đây dựa vào một số phương án. Tuy nhiên, người có kiến thức trung bình trong lĩnh vực có thể dễ dàng thấy rằng các phương án khác với các phương án đã được bộc lộ trên đây là có thể được tạo ra trong phạm vi của sáng chế, như được xác định bởi các điểm yêu cầu bảo hộ kèm theo.

YÊU CẦU BẢO HỘ

1. Phương pháp thiết lập bí mật dùng chung giữa thiết bị truyền thông thứ nhất (20) và ít nhất một thiết bị truyền thông thứ hai (30), trong đó phương pháp này được thực hiện bởi thiết bị điện toán (10) và bao gồm các bước:

thu thập (S201) dữ liệu cảm biến mà từ đó bí mật dùng chung đó có thể được trích xuất, dữ liệu cảm biến này biểu diễn sự chuyển động mà cả thiết bị điện toán (10) lẫn thiết bị truyền thông thứ nhất (20) được gây ra;

tạo ra (S202) sự biểu diễn dữ liệu thứ hai từ dữ liệu cảm biến này, từ sự biểu diễn thứ hai này mà bí mật dùng chung đó có thể được trích xuất; và

cung cấp (S203) sự biểu diễn dữ liệu thứ hai này cho thiết bị truyền thông thứ hai (30).

2. Phương pháp theo điểm 1, trong đó dữ liệu cảm biến biểu diễn sự tiếp xúc vật lý với thiết bị truyền thông thứ nhất (20).

3. Phương pháp theo điểm 1, trong đó dữ liệu cảm biến biểu diễn mẫu chuyển động chung với thiết bị truyền thông thứ nhất (20).

4. Phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 3, trong đó bí mật dùng chung giữa thiết bị truyền thông thứ nhất (20) và nhóm thiết bị truyền thông thứ hai (30, 70) đã được thiết lập, phương pháp này còn bao gồm bước:

cung cấp sự biểu diễn dữ liệu thứ hai cho nhóm thiết bị truyền thông thứ hai (30, 70) này.

5. Phương pháp theo điểm 4, trong đó ít nhất một trong số các thiết bị truyền thông thứ hai (30, 70) trong nhóm nêu trên là được cung cấp sự biểu diễn dữ liệu thứ hai qua phương tiện truyền thông thứ ba mà khác với phương tiện truyền thông thứ hai.

6. Phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 5, trong đó phương pháp này còn bao gồm các bước:

trích xuất bí mật dùng chung từ dữ liệu cảm biến; và

thiết lập truyền thông với thiết bị truyền thông thứ nhất (20) và/hoặc ít nhất một thiết bị truyền thông thứ hai (30) nhờ sử dụng bí mật dùng chung trích xuất được.

7. Phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 6, trong đó bước cung cấp (S103, S203) sự biểu diễn dữ liệu thứ hai, mà từ đó bí mật dùng chung có thể được trích xuất, bao gồm một trong số các bước: cung cấp, về mặt thị giác, sự biểu diễn dữ liệu thứ hai, cung cấp, về mặt thính giác, sự biểu diễn dữ liệu thứ hai, và cung cấp sự biểu diễn dữ liệu thứ hai qua kênh truyền thông vô tuyến không dây.

8. Phương tiện đọc được bằng máy tính (13) có lưu giữ chương trình máy tính (12) bao gồm các lệnh thực thi được bằng máy tính để khiến thiết bị (10) thực hiện phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 7 khi các lệnh thực thi được bằng máy tính này được thực thi trên khối xử lý (11) mà được bao gồm trong thiết bị này.

9. Thiết bị điện toán (10) được tạo cấu hình để thiết lập bí mật dùng chung giữa thiết bị truyền thông thứ nhất (20) và ít nhất một thiết bị truyền thông thứ hai (30), thiết bị điện toán (10) này bao gồm khối xử lý (11) và bộ nhớ (13), bộ nhớ này chứa các lệnh (12) thực thi được bởi khối xử lý này, và bộ cảm biến chuyển động (14), nhờ đó thiết bị điện toán (10) này hoạt động được để:

thu thập dữ liệu cảm biến của bộ cảm biến chuyển động (14) mà từ đó bí mật dùng chung đó có thể được trích xuất, dữ liệu cảm biến này biểu diễn sự chuyển động mà cả thiết bị điện toán (10) lẫn thiết bị truyền thông thứ nhất (20) được gây ra;

tạo ra sự biểu diễn dữ liệu thứ hai từ dữ liệu cảm biến này, từ sự biểu diễn thứ hai này mà bí mật dùng chung đó có thể được trích xuất; và

cung cấp sự biểu diễn dữ liệu thứ hai này cho thiết bị truyền thông thứ hai (30).

10. Thiết bị điện toán (10) theo điểm 9, trong đó dữ liệu cảm biến biểu diễn sự tiếp xúc vật lý với thiết bị truyền thông thứ nhất (20).

11. Thiết bị điện toán (10) theo điểm 9, trong đó dữ liệu cảm biến biểu diễn mẫu chuyển động chung với thiết bị truyền thông thứ nhất (20).

12. Thiết bị điện toán (10) theo điểm bất kỳ trong số các điểm từ 9 đến 11, trong đó bí mật dùng chung giữa thiết bị truyền thông thứ nhất (20) và nhóm thiết bị truyền thông thứ hai (30, 70) được thiết lập, thiết bị điện toán này còn hoạt động được để:

cung cấp sự biểu diễn dữ liệu thứ hai cho nhóm thiết bị truyền thông thứ hai (30, 70) này.

13. Thiết bị điện toán (10) theo điểm 12, trong đó ít nhất hai trong số các thiết bị truyền thông thứ hai (30, 70) trong nhóm nêu trên là được cung cấp sự biểu diễn dữ liệu thứ hai thông qua các phương tiện truyền thông khác nhau.

14. Thiết bị điện toán (10) theo điểm bất kỳ trong số các điểm từ 9 đến 13, trong đó thiết bị này còn hoạt động được để:

trích xuất bí mật dùng chung nêu trên; và

thực hiện việc ghép đôi với thiết bị truyền thông thứ nhất (20) và/hoặc ít nhất một thiết bị truyền thông thứ hai (30) nhờ sử dụng bí mật dùng chung trích xuất được.

15. Thiết bị điện toán (10) theo điểm bất kỳ trong số các điểm từ 9 đến 14, trong đó bước cung cấp sự biểu diễn dữ liệu thứ hai, mà từ đó bí mật dùng chung có thể được trích xuất, bao gồm một trong số các bước: cung cấp, về mặt thị giác, sự biểu diễn dữ liệu thứ hai, cung cấp, về mặt thính giác, sự biểu diễn dữ liệu thứ hai, và cung cấp sự biểu diễn dữ liệu thứ hai qua kênh truyền thông vô tuyến không dây.

16. Thiết bị điện toán (10) theo điểm 15, trong đó thiết bị này còn bao gồm một hoặc nhiều trong số điện thoại hội nghị, thiết bị hiển thị, bộ phát quang, và bộ phát tần số vô tuyến, để cung cấp sự biểu diễn dữ liệu thứ hai.

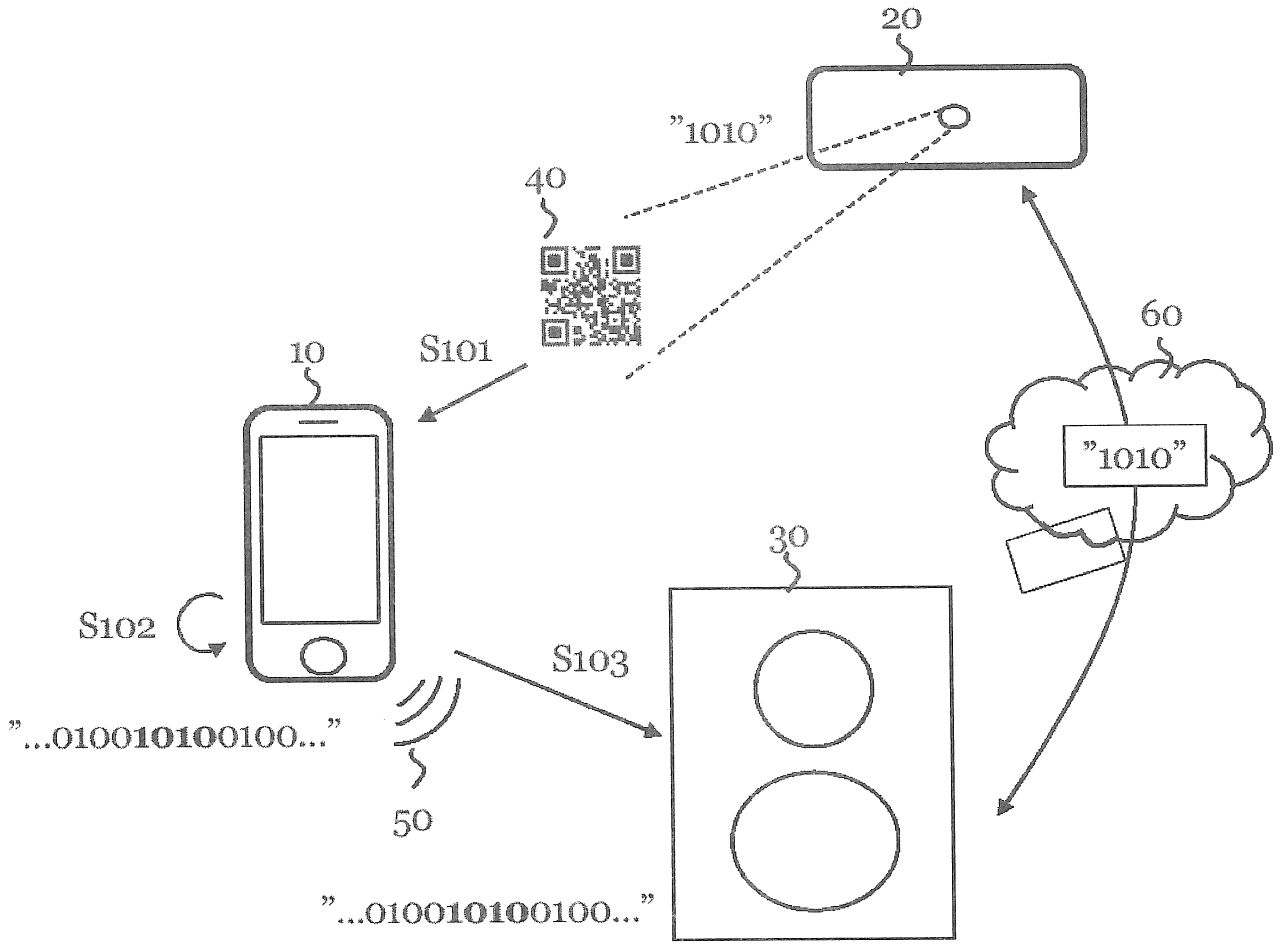

20
"1010"
40
60
10
S101
"1010"
30
S102
S103
"...0100**1010**0100..."
50
"...0100**1010**0100..."

Fig.1

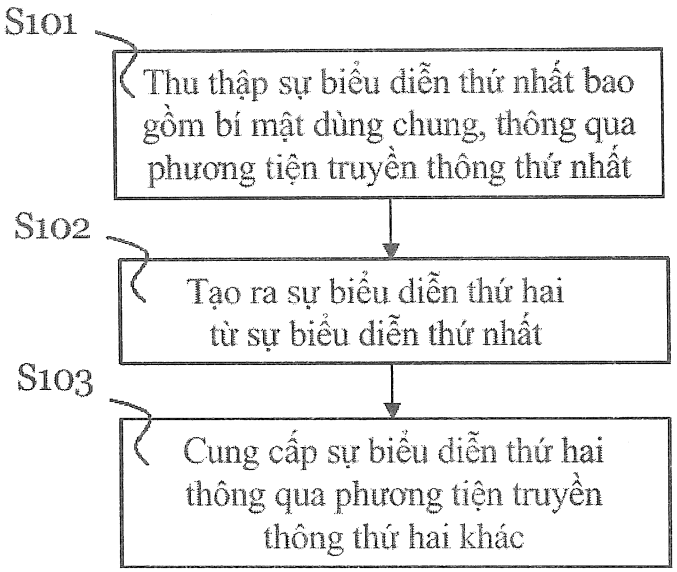

S101
Thu thập sự biểu diễn thứ nhất bao gồm bí mật dùng chung, thông qua phương tiện truyền thông thứ nhất
S102
Tạo ra sự biểu diễn thứ hai từ sự biểu diễn thứ nhất
S103
Cung cấp sự biểu diễn thứ hai thông qua phương tiện truyền thông thứ hai khác

Fig.2

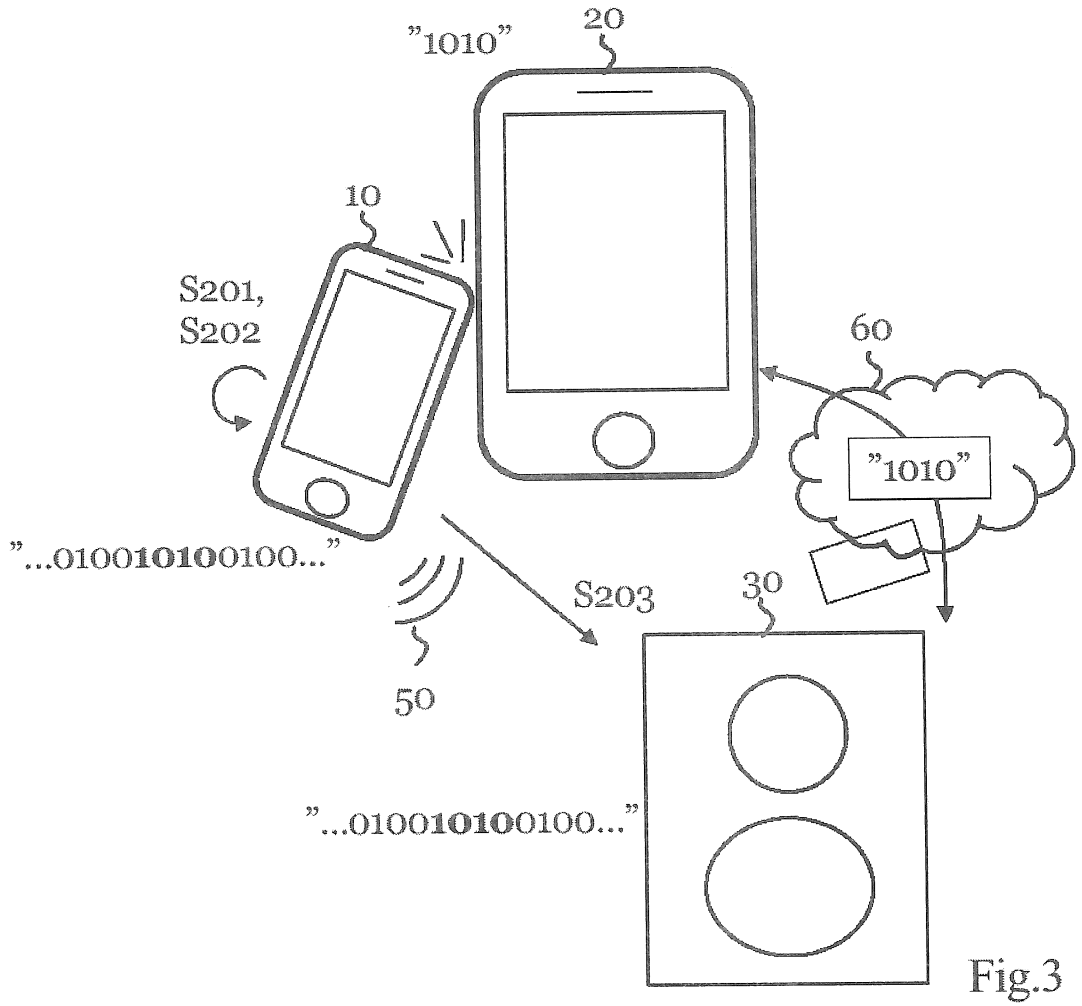

"1010"
20
10
S201,
S202
60
"1010"
"...0100101000100..."
S203
30
50
"...0100101000100..."

Fig.3

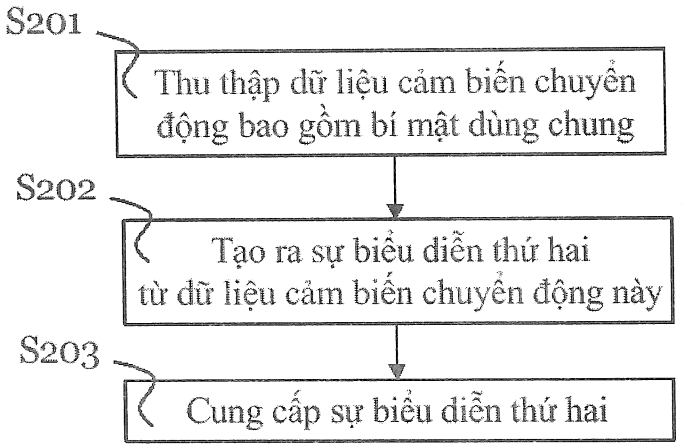

S201
Thu thập dữ liệu cảm biến chuyển động bao gồm bí mật dùng chung
S202
Tạo ra sự biểu diễn thứ hai từ dữ liệu cảm biến chuyển động này
S203
Cung cấp sự biểu diễn thứ hai

Fig.4

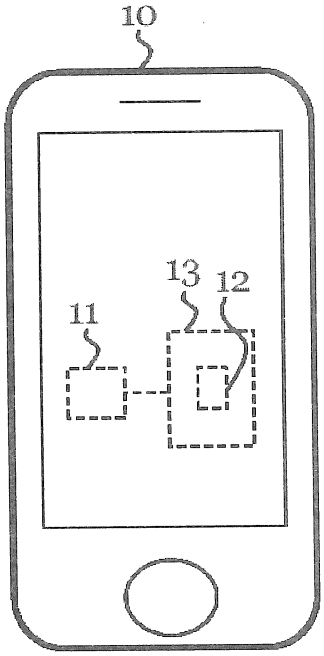


Fig.5

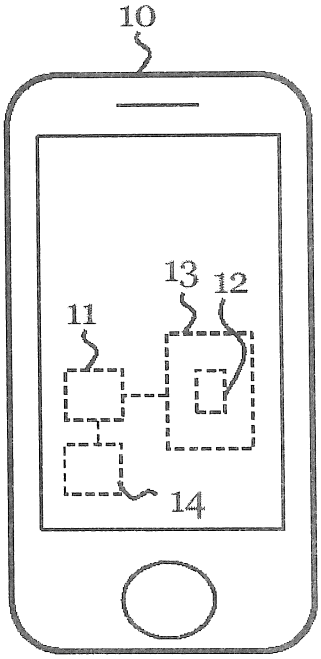


Fig.6

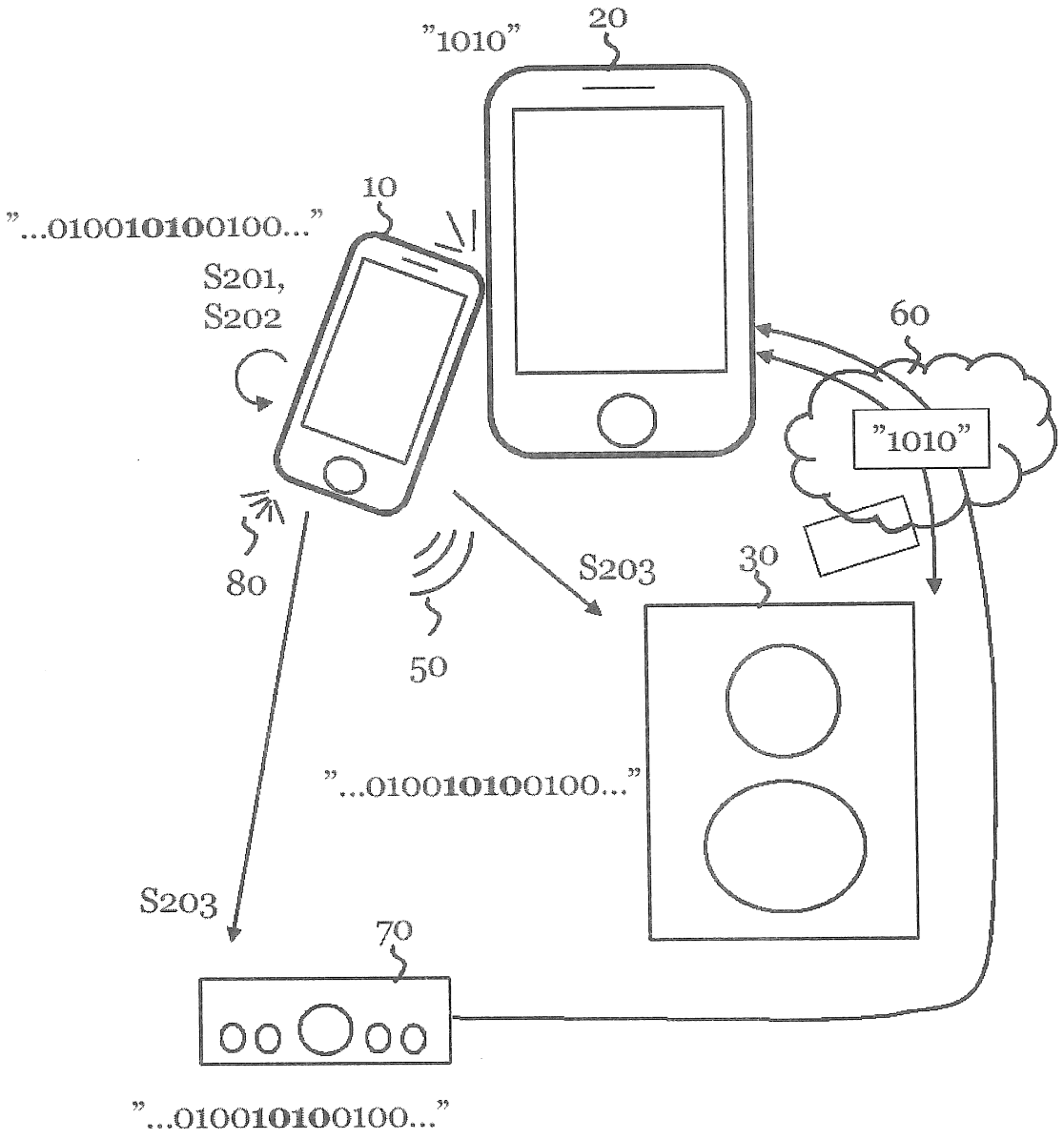

"1010"
20
10
"...0100**1010**0100..."
S201,
S202
60
"1010"
80
50
S203
30
"...0100**1010**0100..."
S203
70
"...0100**1010**0100..."

Fig.7

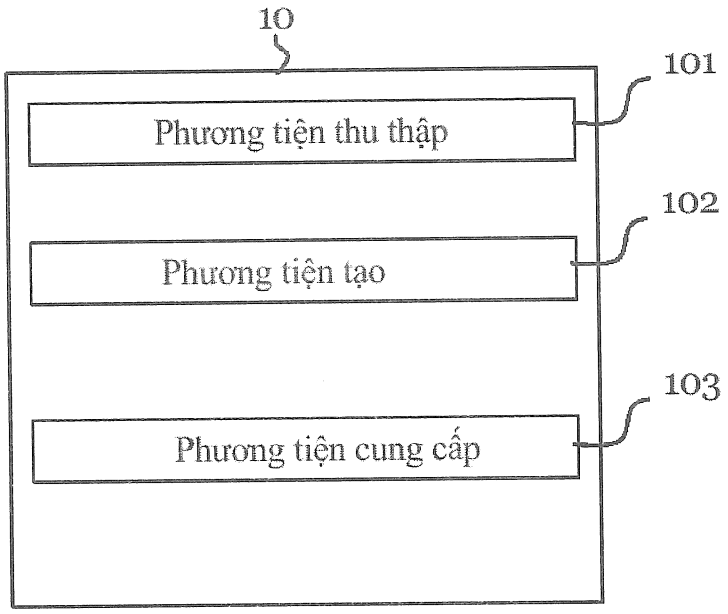

10
101
Phương tiện thu thập
102
Phương tiện tạo
103
Phương tiện cung cấp

Fig.8

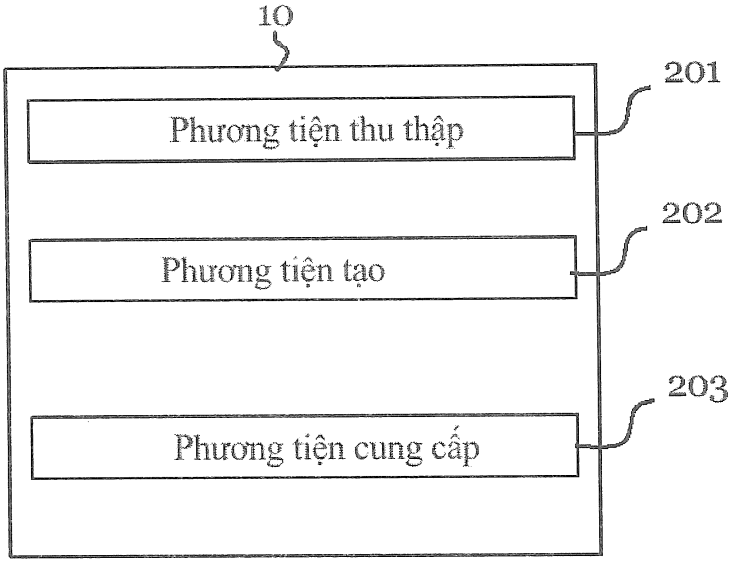

10
201
Phương tiện thu thập
202
Phương tiện tạo
203
Phương tiện cung cấp

Fig.9