(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) **1-0019363**

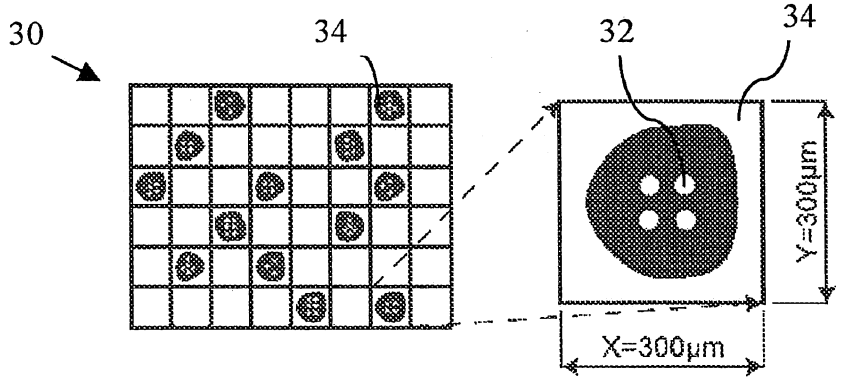
(51)[7] **H04N 1/32**, G07D 7/00, 7/20

(13) **B**

(21) 1-2014-03031
(22) 15.02.2013
(86) PCT/IB2013/051260 15.02.2013
(87) WO2013/121401 22.08.2013
(30) P1200097 15.02.2012 HU
(45) 25.07.2018 364
(43) 25.12.2014 321
(73) GLENISYS KFT. (HU)
Fészek u. 3., H-1125 Budapest, Hungary
(72) BIRó, Attila (HU), KRISTó, Gábor (HU), REMéNYI, Piroska (HU)
(74) Công ty TNHH Tầm nhìn và Liên danh (VISION & ASSOCIATES CO.LTD.)

(54) PHẦN TỬ BẢO MẬT VÀ PHƯƠNG PHÁP KIỂM TRA TÍNH XÁC THỰC CỦA ẤN PHẨM IN

(57) Sáng chế đề cập đến phần tử bảo mật được áp dụng lên các nền in (giấy bạc ngân hàng, trái phiếu, bao gói sản phẩm, nhãn mác/thẻ nhận dạng hoặc các tài liệu tương tự khác) bằng cách in, bao gồm ký hiệu nhận dạng độc nhất như là thông tin chính có thể nhìn thấy bằng mắt thường và thông tin phụ bảo vệ chống lại sự sao chép không thể nhìn thấy bằng mắt thường. Ký hiệu nhận dạng độc nhất thường là mã điểm. Thông tin phụ được thể hiện bằng cấu trúc có kích thước lớn nhất từ 2 đến 40 micrômet, và do sự biến dạng in phát sinh khi phần tử bảo mật được áp dụng lên nền in, nên thông tin phụ không thể tái tạo được từ bản in của phần tử bảo mật và đặc điểm cố hữu có thể phân tích được bằng thông kê liên quan tới nó. Sáng chế còn đề cập đến ấn phẩm in có phần tử bảo mật của sáng chế và đến phương pháp kiểm tra tính xác thực của ấn phẩm in có phần tử bảo mật theo sáng chế trong ánh sáng có thể nhìn thấy được (380-750nm).



Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập đến phần tử bảo mật, cũng như đến phương pháp xác định tính xác thực của bản in được bố trí trên nền in. Lĩnh vực ứng dụng của nó thuộc lĩnh vực bảo vệ các ấn phẩm in được tạo ra bởi các máy in hoặc các tài liệu được tạo ra bằng các máy in phun và/hoặc các máy in laze chống lại sự giả mạo.

Tình trạng kỹ thuật của sáng chế

Ngày nay, kỹ thuật sao chụp (photocopy) và in laze đạt được nhiều cải tiến vượt bậc. Kết quả là, nhờ các kỹ thuật này việc tái xuất bản các ấn phẩm in khác nhau với chất lượng rất cao đã được đơn giản hóa đáng kể. Đồng thời, điều không may là, việc giả mạo các ấn phẩm in có giá trị hoặc mang tính cá nhân cũng trở nên dễ dàng hơn. Do đó, việc bảo vệ các tài liệu như vậy chống lại sự giả mạo vẫn còn ở phía trước. Mọi tài liệu được tạo ra có vật mang dữ liệu, ví dụ như bản chữ viết hoặc bản vẽ, được tạo ra bởi, ví dụ máy in hoặc máy in phun và/hoặc máy in laze, có thể tạo ra ấn phẩm in cần được bảo vệ. Các ấn phẩm in như vậy, ví dụ là các nhãn mác trên bao gói khác nhau (ví dụ dùng cho thuốc, nắp đậy đĩa CD), các vé vào cửa có giá trị, giấy chứng nhận, giấy bạc, séc, tài liệu nhận dạng cá nhân, các chứng thư khác nhau, v.v.. Để tránh (hoặc để giảm đến mức tối thiểu) sự lạm dụng, các ấn phẩm in thường được tạo ra bởi các phần tử bảo mật thích hợp. Nhìn chung, các phần tử bảo mật được áp dụng và/hoặc sự kết hợp của chúng khá là phức tạp.

Đã có nhiều giải pháp được áp dụng trong lĩnh vực bảo vệ bản in. Theo một nhóm của lĩnh vực này, phần tử bảo mật tạo ra sự bảo vệ được ẩn trong chính ảnh được in. Công bố đơn sáng chế quốc tế số W099/35819 và đơn sáng chế Mỹ số 1996/019310 đã bộc lộ giải pháp dựa vào chính khái niệm này. Theo giải pháp này, ảnh phụ không thể nhìn thấy bằng mắt thường, nhưng có thể nhìn thấy đối với thiết bị giải mã nhất định được ẩn bên trong ảnh chính có thể nhìn thấy bằng mắt thường. Các thông số vật lý của

kỹ thuật này được sử dụng để tạo ra ảnh phụ nêu trên có thể được lựa chọn theo cách ảnh phụ biến mất một cách thuần túy khi sao chép lớp nền (tài liệu) được in trên đó với ảnh kết hợp. Tức là, thông tin này không thể tái tạo được từ bản sao của bản in. Tuy nhiên, để tiến hành các giải pháp liên quan, cần có máy in có độ chính xác cao (với độ phân giải ít nhất là 8000 dpi), và để kiểm tra tính xác thực của bản in, cũng cần phải có thấu kính giải mã. Vì các nhược điểm này, việc áp dụng các giải pháp nêu trên đã không/không thể trở nên phổ biến rộng rãi trong thực tiễn hàng ngày, trong đó, nhờ vào các tiến bộ đạt được trong in số, việc bảo vệ các ấn phẩm in với các bản in được tạo ra bởi các máy nhìn chung có độ phân giải thấp hơn nhiều (phổ biến là 600 dpi) phải được bảo vệ.

Phần tử bảo mật được bộc lộ trong bằng sáng chế Nga số 2,430,836 là phần tử bảo mật mạnh có thể kiểm tra bằng mắt thường và tạo ra trải nghiệm thẩm mỹ đặc biệt. Tuy nhiên, việc ứng dụng phần tử bảo mật này lên nền in cần sử dụng máy in riêng biệt (in khắc lõm). Các máy in này thường do các nhà in ngân hàng sở hữu, và do đó việc tiếp cận các máy in như vậy là khá hạn chế.

Trong nhóm tiếp theo của việc bảo vệ bản in, mực in được sử dụng để áp dụng cho chính bản in và/hoặc nền in những nội dung được tạo ra cụ thể, và bản chất không sao chép được được cố gắng tạo ra theo cách này. Các giải pháp như vậy được bộc lộ, ví dụ trong các bằng sáng chế châu Âu số 2,004,414; 1,858,605; 1,827,864 và 1,779,335. Nhược điểm lớn nhất của các giải pháp trong các bằng sáng chế này là sử dụng mực in riêng biệt và do đó mực in khá đắt (ví dụ mực in có các chất màu biến đổi quang) hoặc sử dụng nền in riêng biệt chỉ có thể sản xuất với giá thành cao.

Trong nhóm khác nữa của việc bảo vệ bản in, bản in bao gồm một hoặc nhiều ký hiệu nhận dạng có thể hỗ trợ bản in bằng một cơ sở dữ liệu. Bằng sáng chế Mỹ số 6,952,485 đã bộc lộ cái gọi là dấu nước điện tử như là một ký hiệu nhận dạng. Ở đây, tiếng ồn được kết hợp vào trong ảnh và không thể nhìn thấy bằng mắt thường mang thông tin. Dấu nước điện tử có thể được tái tạo từ bản sao được chuẩn bị bằng cách tái sản xuất mà không cần bất kỳ thay đổi nào, tức là dấu nước điện tử luôn luôn được chuyển do sao

chép. Một lĩnh vực ứng dụng dấu nước điện tử là việc bảo vệ các giấy bạc chống lại sự sao chép. Cụ thể là, dấu nước điện tử như vậy có trong các tờ bạc của châu Âu như là phần tử bảo mật. Dấu nước này được nhận biết bởi bộ phận dẫn động của mỗi máy in được bán ngày nay, và sau đó chỉ từ chối in ra ảnh bao gồm dấu nước điện tử. Nhược điểm của kỹ thuật này nằm ở chỗ buộc phải có thỏa thuận rộng rãi giữa các nhà sản xuất máy in và máy quét đối với dấu nước điện tử được sử dụng cho việc bảo vệ sự sao chép. Điều này có nghĩa là loại bảo vệ bản in này chỉ có thể sử dụng được trên các ấn phẩm in rất đặc biệt. Ngoài ra, dấu nước bị cấm phải được "truyền đạt" tới mọi bộ phận dẫn động của máy in/máy quét. Một nhược điểm này nữa xuất phát chỉ từ phần nói đến sau: các máy in được sản xuất trước khi thỏa thuận được ký kết đơn giản là không nhận ra dấu nước bị cấm, và do đó chúng in ra ấn phẩm in được bảo vệ bởi dấu nước đã nêu.

Theo giải pháp được bộc lộ trong đơn sáng chế quốc tế số PCT/EP2009/061073, ký hiệu nhận dạng chính có thể nhìn thấy được và thành phần ảnh nhiễu ngẫu nhiên độc nhất (thông tin phụ) mà không thể nhìn thấy bằng mắt thường được bố trí trên vật phẩm cần được bảo vệ trong quá trình sản xuất. Ký hiệu nhận dạng và thành phần ảnh cũng được coi là thông tin phụ, được lưu giữ trong cơ sở dữ liệu trên Internet dưới dạng số. Khi kiểm tra tính xác thực của vật phẩm dựa vào thông tin chính, thì nhìn vào ảnh được lưu giữ trong cơ sở dữ liệu và sau đó so ánh với ảnh của vật phẩm được kiểm tra theo vết điểm. Nhược điểm của giải pháp này nằm ở chỗ để tiến hành kiểm tra, cần truy cập vào cơ sở dữ liệu từ xa trong mọi trường hợp cần đến khả năng kết nối liên lạc dữ liệu với băng tần thích hợp.

Trong một nhóm khác của bảo vệ bản in, để kiểm tra tính xác thực của bản in, giao thoa của thiết bị in và hỗ trợ in trong quá trình in được khai thác. Công bố đơn sáng chế Mỹ số 2002/0037093 đề cập đến giải pháp trong đó máy photocopy hoặc máy in laze "làm bẩn" (giấy) nền in đi qua máy một cách ngẫu nhiên cùng với mực in hoặc các vi ảnh mực không thể nhìn thấy bằng mắt thường khi tạo ra bản sao. Tức là, bằng cách phân tích ảnh số độ nét cao của tài liệu, nếu mực in hoặc các vi ảnh mực được xem xét đặc biệt

trong các phần của tài liệu nêu trên không mang bản in nào, thì có thể xác định rõ có hay không việc tài liệu này được tạo ra do sao chép. Nhược điểm của kỹ thuật này nằm ở chỗ để tiến hành nghiên cứu này, cần phải có phương tiện số có độ phân giải cao.

Công bố đơn sáng chế Nhật số 2009/034921 A bộc lộ ấn phẩm in có phương tiện chống giả mạo bao gồm hình ẩn dạng đường nét, tức là thông tin phụ. Ở ít nhất một mép bên của mỗi bên đường tạo ra hình ẩn nêu trên, có nhiều vùng lồi mở rộng được phủ mực được tạo ra nhô tương đối gần với nhau dọc theo hướng bề rộng của đường kẻ này. Khi tài liệu này bị sao chép, các khe hở giữa các vùng lồi mở rộng tương ứng bị mực che đi cùng với các đặc điểm tái tạo của máy sao chép. Do đó, độ rộng của đường nét của mỗi bên đường tạo ra tuyến đường nêu trên mở rộng mà thực tế tạo ra sự phát triển/sự xuất hiện của ảnh ẩn cũng như của thông tin phụ.

Hiện nay, mã vạch, các mã ma trận dữ liệu, các mã QR, các mã di động, và các mã tương tự khác (sau đây nhìn chung gọi là mã điểm) trở thành phương tiện mang thông tin phổ biến. Sự phổ biến của chúng chủ yếu là do sự phát triển của điện thoại di động, đặc biệt là điện thoại thông minh. Nhìn chung, nhược điểm của chúng nằm ở chỗ, chúng không chứa phần bảo vệ sao chép, và do đó việc ứng dụng chúng như là các phần tử bảo mật rất hạn chế.

Xem xét vấn đề nêu trên, điều rõ ràng là mặc dù hiện nay có nhiều kỹ thuật bảo vệ bản in để bảo vệ các bản in được trang bị cùng với bảo vệ sao chép và các nền in/các tài liệu có các bản in như vậy, nhưng các kỹ thuật này đắt hoặc phải cần đến các bộ thiết bị đặc biệt dùng cho việc tạo ra và/hoặc kiểm tra.

Tuy nhiên, một nhu cầu tự nhiên là có thể xác định một cách đơn giản và nhanh chóng tính xác thực của tài liệu bởi bất cứ ai và đặc biệt ở mọi nơi mà không cần đến năng lực hoặc thiết bị kỹ thuật bổ sung.

Bản chất kỹ thuật của sáng chế

Nhằm khắc phục các vấn đề kỹ thuật còn tồn tại như nêu trên, sáng chế có mục đích là đề xuất phần tử bảo mật được áp dụng vào nền in bằng cách in mà, một mặt, chứa dữ liệu nhận dạng liên quan tới chính ấn phẩm in như là thông tin chính và, mặt khác, còn tạo ra sự bảo vệ sao chép tin cậy đối với ấn phẩm in qua thông tin phụ ẩn.

Mục đích khác của sáng chế là đề xuất kỹ thuật bảo vệ bản in, cụ thể là phương pháp kiểm tra/xác định tính xác thực của bản in mà cho phép kiểm tra tính xác thực của ấn phẩm in cho mọi người bằng phần tử bảo mật theo sáng chế và không cần xác định an toàn thông tin ngay lập tức và ngay tại chỗ bằng các thiết bị ít nhất có độ phân giải trung bình (tức là, từ 300 đến 1200 dpi) sẵn có để sử dụng hàng ngày, ví dụ như điện thoại di động, máy tính bảng, điện thoại thông minh, máy quay web (web camera), v.v..

Từ các nghiên cứu, tác giả sáng chế đi đến kết luận rằng phần tử bảo mật đạt được mục đích của sáng chế có thể đạt được bằng cách kết hợp mã chọn thích hợp mang thông tin chính cùng với phần thông tin phụ, trong đó thông tin phụ không thể tái tạo được từ chính bản in (hoặc bản sao của nó) nhưng vẫn tạo ra đặc điểm cố hữu có thể phân tích được bằng phương pháp thống kê. Cơ cấu mang thông tin phụ đó có thể được tạo ra dưới dạng các vùng được kết hợp (tốt hơn là bởi nhà sản xuất) thành mã mang thông tin chính phù hợp với khái niệm/thuật toán mã hóa định trước và không được in trực tiếp trên đó. Do sự bất định/biến dạng in, ví dụ như sự biến dạng của nền in và/hoặc khuôn in khi tiếp xúc với nhau hoặc sự làm ướt do mực không thể tránh được của mực in áp dụng lên nền in, phát sinh khi thực hiện việc in, nên các vùng trắng từ việc in trực tiếp trở nên được phủ bằng mực nhiều hoặc ít. Theo các nghiên cứu của tác giả sáng chế, điều kiện để có thể phát hiện bằng mắt thường (các) vùng trắng trong bản in của phần tử bảo mật là kích thước lớn nhất của (các) vùng trắng bên trong bản in dọc theo ít nhất một chiều là từ 2 đến 40 micrômet, tùy thuộc vào kỹ thuật in được áp dụng và chất lượng của nền in. Mặc dù, do tính bất định của việc in, nên mắt thường sẽ không thể đọc được chút thông tin phụ nào liên quan trong bản in của phần tử bảo mật, kể cả bản chất có trật tự của nó có thể nhận biết được qua kính lúp (với hệ số phóng đại 2-20x), nên đã phát hiện ra rằng sự kết

hợp thông tin phụ nêu trên làm thay đổi chỉ số thang đo xám của phần đó của phần biểu diễn dạng số của bản in mà nó thực sự được kết hợp. Qua việc thay đổi chỉ số thang đo xám, thông tin phụ được cho là phần tử bảo mật có đặc điểm cố hữu có thể phân tích được bằng phương pháp thống kê, trong đó kết quả của phân tích này là đặc trưng của bản thân phần tử bảo mật và do đó nó có thể được sử dụng làm thành phần bảo vệ sao chép cho phần tử bảo mật, cũng như cho nền in có phần tử bảo mật đó.

Mô tả vắn tắt các hình vẽ

Dưới đây, sáng chế được mô tả chi tiết hơn có dựa vào các hình vẽ kèm theo, trong đó:

Fig.1A là sơ đồ khối thể hiện phương pháp sản xuất phần tử bảo mật theo sáng chế và để áp dụng nó lên nền in;

Fig.1 B là sơ đồ khối thể hiện phương pháp kiểm tra tính xác thực dựa vào ứng dụng của phần tử bảo mật theo sáng chế;

Fig.2 là hình vẽ thể hiện cách tạo ra mã kết hợp, tạo thành phần tử bảo mật, từ các mã mang thông tin chính và thông tin phụ;

Fig.3 là hình vẽ thể hiện một phần của mã kết hợp trên Fig.2 được phóng to;

Fig.4 là hình vẽ thể hiện sự phân hủy của phần mã kết hợp được thể hiện trên Fig.3 thành các nhóm theo thông tin phụ, được thực hiện cùng với khái niệm/thuật toán mã hóa được thiết lập bởi nhà sản xuất;

Fig.5 là hình vẽ thể hiện ô mã được khái quát hóa có thể áp dụng khi thông tin phụ được đưa vào trong mã điểm;

Fig.6 là hình vẽ thể hiện các phương án ưu tiên của (các) vùng trắng (các điểm ảnh) thể hiện thông tin phụ có thể áp dụng trong phần tử bảo mật theo sáng chế;

Fig.7 là hình vẽ thể hiện nhiều mã điểm làm ví dụ (có thể nhìn thấy bằng mắt thường) mang thông tin chính có kích thước lớn nhất lớn hơn 50 micrômet;

Fig.8 là hình vẽ minh họa bề ngoài theo lý thuyết (như được tạo ra trong khuôn in) và bề ngoài thực sự (như được nhìn thấy sau khi in lên trên nền in) của phần của phần tử bảo mật được tạo ra bởi mã kết hợp; và

Fig.9A và Fig.9B là các hình vẽ minh họa một đoạn thông tin (ẩn) thứ hai có kích thước lớn nhất 50 micrômet dọc theo ít nhất một chiều, được ẩn thành kiểu mẫu giống điểm và giống đường kẻ, tương ứng trước và sau khi in.

Mô tả chi tiết sáng chế

Phương pháp chung để sản xuất phần tử bảo mật theo sáng chế được tạo ra bằng mã kết hợp được thể hiện trên Fig.1A. Theo phương pháp này, một mã mang thông tin được chọn (bước 100) được tạo ra bằng một ký hiệu mã đã biết (ví dụ mã vạch, mã QR (Quick Response code-mã đáp ứng nhanh), mã ma trận dữ liệu, mã di động) hoặc mã điểm hoặc vạch được mã hóa độc đáo. Theo một khả năng khác, mã mang thông tin chính cũng có thể được tạo ra bằng mã điểm hoặc vạch được ẩn bên trong phần minh họa đồ họa trang trí của bản in. Ngoài ra, bản thân mã mang thông tin chính có thể là thông tin chính, được in lên nền in theo cách được giải mã. Nền in có thể là tài liệu hoặc bề mặt bất kỳ của đối tượng cần được bảo vệ; Cụ thể là, ví dụ giấy bạc ngân hàng, trái phiếu, hóa đơn, bao gói sản phẩm, nhãn mác/thẻ nhận dạng, bìa sách, vé vào cửa, giấy chứng nhận, các tài liệu cá nhân, chứng thư hoặc các tài liệu tương tự bất kỳ khác. Thông tin chính là đoạn tin liên quan đến tài liệu cần được bảo vệ, nhìn chung, dữ liệu nhận dạng chính tài liệu. Điều quan trọng là mã mang thông tin chính có thể được phân đoạn, tức là có thể được phủ bằng mắt lưới có kích thước định trước và phổ biến có hình dạng cân đối (Cụ thể là, hình chữ nhật), được quay tùy ý một góc định trước so với mã mang thông tin chính. Do tiêu chuẩn thiết kế, nên yêu cầu nói đến sau được đáp ứng một cách tự động đối với các ký hiệu mã đã biết nêu trên.

Sau khi chọn mã mang thông tin chính, mã mang thông tin phụ được tạo ra (bước 110). Bước này được tiến hành phù hợp với khái niệm/thuật toán mã hóa thiết lập trước

theo cách được thảo luận chi tiết đối với ví dụ cụ thể về những nội dung theo số chỉ dẫn từ Fig.2 đến Fig.4. Cụ thể là, thông tin phụ được mang bởi các vùng trắng từ bản in của mã mang thông tin chính. Do kích thước của nó, nên mã mang thông tin phụ là đoạn thông tin ẩn, tức là không thể nhìn thấy khi kiểm tra bằng mắt thường. Thông tin phụ minh họa như vậy được xác định bởi các vùng trắng được thể hiện trên Fig.3 và Fig.6. Thông tin phụ tốt hơn là có được từ thông tin chính, ví dụ từ thành phần/dữ liệu của nó.

Sau khi tạo ra mã mang thông tin phụ, các mã mang thông tin chính và thông tin phụ được kết hợp với nhau (bước 120), kết quả là thu được mã kết hợp tương ứng với phần tử bảo mật của sáng chế.

Cuối cùng, ấn phẩm in có phần tử bảo mật được tạo ra bằng cách áp dụng phần tử bảo mật như vậy lên trên nền in qua kỹ thuật in được lựa chọn (bước 130).

Phần tử bảo mật của ấn phẩm in được tạo ra bởi phương pháp này được thể hiện trên Fig.1A, một mặt chứa dữ liệu có thể được sử dụng để nhận biết ấn phẩm in (thông tin chính) nêu trên và, mặt khác, thích hợp để bảo vệ ấn phẩm in nêu trên chống lại sự sao chép, như là thông tin phụ là một thông tin ẩn không thể nhìn thấy bằng mắt thường và biến mất hoặc trở nên méo mó theo cách có thể đọc được khi được in/sao chép.

Các hình vẽ từ Fig.2 đến Fig.4 minh họa các bước kết hợp các mã mang thông tin thứ nhất và thứ hai trong trường hợp cụ thể, trong đó mã mang thông tin chính được tạo ra bởi mã điểm (xem Fig.2) được tạo ra bởi các chấm mực in 20 và biểu diễn con số "0" được in với độ phân giải 600 dpi, trong đó sự phân đoạn được thực hiện bởi lưới 30 có các mắt lưới 34 có dạng hình vuông (xem Fig.3). Ở đây, cỡ của mỗi mắt lưới 34 ít nhất là 300 micrômet dọc cả hai hường X và Y. Đã phát hiện ra rằng cỡ 300 micrômet là đủ để bảo đảm rằng từng chấm mực in riêng lẻ 20 rơi vào trong mắt lưới riêng rẽ 34 và cách xa các biên của mắt lưới 34 (tức là, thực tế là vào giữa mắt lưới 34). Ngoài ra, mỗi mắt lưới 34 được chia thành bảy điểm ảnh 40 (trong trường hợp cụ thể này); các điểm ảnh 40 tạo thành các đơn vị phân chia là các "khối xây dựng" đối với các vùng trắng 42 giải mã

thông tin phụ. Điều rõ ràng đối với người có hiểu biết trung bình về lĩnh vực kỹ thuật này là sự phân đoạn có thể được tiến hành với các kích thước mắt lưới khác nhau và/hoặc với nhiều điểm ảnh khác nhau dọc theo các hướng X, Y trên các mắt lưới đối với loại ký hiệu mã khác. Mắt lưới hình chữ nhật phổ biến 50 và mắt lưới (ij) 52 có thể áp dụng cho sự phân đoạn được thể hiện trên Fig.5. Cũng cần lưu ý rằng nếu sử dụng độ phân giải cao hơn, thì số lượng điểm ảnh dọc theo mỗi trong các hướng này phải được tăng thích hợp.

Khi đã phân đoạn mã mang thông tin chính, thì tiến hành nhập mã mang thông tin phụ. Về vấn đề này, các mắt lưới 34 của mã mang thông tin chính thu được bằng sự phân đoạn và chứa chấm mực in, được phân thành nhiều nhóm. Ở đây, số lượng các nhóm khác nhau được chọn để rơi vào bốn và sáu nhóm, tuy nhiên, số lượng nhóm bất kỳ khác cũng có thể được sử dụng như nhau. Do sau khi in phần tử bảo mật của sáng chế, thông tin phụ tạo ra đặc điểm có thể phân tích được bằng kỹ thuật thống kê, tốt hơn là có ít nhất mười mắt lưới 34 trong mỗi nhóm. Việc phân loại nêu trên có thể diễn ra theo cách thường xuyên hoặc ngẫu nhiên, tuy nhiên, nó luôn tiếp theo từ mã mang thông tin chính. Trong ví dụ hiện tại, việc phân loại được thực hiện theo số lượng điểm ảnh tạo ra vùng trắng bên trong mỗi mắt lưới. Ở đây, số lượng được ghi vào trong mắt lưới nhất định tương ứng với kích thước của vùng trắng bên trong mắt lưới, được thể hiện bằng các điểm ảnh. Kích thước của vùng trắng thay đổi từ nhóm này sang nhóm khác theo cách tăng nghiêm ngặt. Do đó, ví dụ nhóm thứ nhất giữ nguyên không đổi (tức là không có vùng trắng trong đó), nhóm thứ hai sẽ có vùng trắng của một điểm ảnh, nhóm thứ ba sẽ có vùng trắng của ít nhất hai điểm ảnh, nhóm thứ tư sẽ có vùng trắng của ít nhất ba điểm ảnh, và v.v..

Kích thước của vùng trắng trong mỗi mắt lưới 34 phụ thuộc vào kỹ thuật in cần áp dụng: kích cỡ/kích thước của vùng trắng luôn được lựa chọn theo cách sao cho kỹ thuật in được áp dụng là không thích hợp để in vùng trắng nêu trên một cách sắc nét. Do đó, do sự bất định của việc in của các vùng trắng, nên các vùng này sẽ không thể nhìn thấy được một chút nào trong phần tử bảo mật được in khi kiểm tra bằng mắt thường. Ngoài ra,

cũng không thể nhận biết được bản chất trật tự của thông tin phụ bằng kính lúp (ở hệ số phóng đại 2-20x).

Có nhiều ví dụ về hình dạng có thể có được của các vùng trắng được tạo ra từ các điểm ảnh được thể hiện trên Fig.6. Hình dạng và kích thước của vùng trắng không thể tùy tiện, kích thước được giới hạn bởi kỹ thuật in cần áp dụng, như được nêu trên. Trong Bảng 1 dưới đây, vài độ rộng đường nét có khả năng in trắng được đề xuất để sản xuất phần tử bảo mật của sáng chế, thu được theo kinh nghiệm bằng cách tiến hành các thử nghiệm sự làm ẩm do mực trên nền in được thu gom đối với các kỹ thuật in khác nhau. Các phép đo sự làm ẩm do mực được tiến hành bằng mực in được điều chỉnh theo các kỹ thuật in khác nhau, tức là, ví dụ bằng màu đen của mực in từ Hewlett Packard, bằng màu đen của mực in từ MEMJET, bằng mực in màu đen của KODAK Prosper và màu đen của mực in từ EPSON, trong đó giấy có xơ được sử dụng điển hình trong in bảo mật được sử dụng làm nền in ở nhiệt độ từ 18-22°C (nhiệt độ phòng) và ở áp suất môi trường 101 kPa. Ở đây cần lưu ý là các giá trị liệt kê trong Bảng 1 cũng có giá trị cho các loại giấy khác, mặc dù độ phân giải bắt buộc nhìn chung thay đổi. Cụ thể là, nếu nền in, ví dụ là giấy ảnh bóng, thì việc in phải được thực hiện ở độ phân giải ít nhất là 600-1200 dpi thay vì 300-600 dpi.

Phù hợp với phần nêu trên, khi xuất hiện một công nghệ in mới, sự làm ẩm do mực có thể được xác định trên bản in thử nghiệm và sau đó độ rộng khổ in trắng được đề xuất cho vùng trắng được thể hiện bằng nhiều điểm ảnh có thể thu được đối với công nghệ mới này. Về vấn đề này các công thức theo kinh nghiệm sau đây cũng có thể được sử dụng:

Độ rộng khổ [micrômet] = 1,2 * làm ẩm do mực [micrômet].

Độ rộng khổ [điểm ảnh] = số nguyên lớn nhất của {(1,2 * làm ẩm do mực [micrômet] * độ phân giải [dpi] /25,4)/1000 +0,5}, nhưng ít nhất là 1.

Kỹ thuật	Độ phân giải phổ biến	Làm ẩm do mực [micrômet] (phụ thuộc giấy)	Độ rộng khổ có thể in trắng (của diện tích mất đi từ in trực tiếp)	
			[micrômet]	[điểm ảnh]
In phun	600	10-50	12-60	1-2
In laze	720	30-40	36-48	2-3
In offset	8000	10-20	12-24	4-8

Bảng 1. Độ rộng khổ của các vùng trắng mang thông tin phụ.

Mặc dù các vùng trắng từ in trực tiếp là không thể nhìn thấy bằng mắt thường trong bản in của phần tử bảo mật, do sự bất định của việc in nên chúng làm thay đổi thang đo xám của mắt lưới được xác định bởi công thức

chỉ số thang đo xám = (số lượng của các điểm ảnh màu đen trong mắt lưới)/(số lượng của tổng các điểm ảnh in trong mắt lưới);

Ở đây, sự thay đổi tỷ lệ nghịch với sự tăng về số lượng của các điểm ảnh của vùng xóa đi bên trong nhóm được xem xét. Do đó, phần tử bảo mật của sáng chế được tạo ra bởi mã kết hợp nêu trên thể hiện đặc điểm cố hữu dưới dạng các chỉ số thang đo xám xác định trên đây mà có thể liên quan tới thông tin phụ ẩn; sau khi in phần tử bảo mật và tạo ra phần biểu diễn dạng số của bản in thu được thì đặc điểm cố hữu nêu trên có thể được phân tích theo phương pháp thống kê.

Tiến hành giải mã phần tử bảo mật của sáng chế được áp dụng lên nền in và, nhờ đó, việc quyết định tính xác thực của ấn phẩm in liên quan được tiến hành theo sơ đồ được thể hiện trên Fig.1B. Theo đó, trong bước thứ nhất phần biểu diễn dạng số của ký hiệu mã mang thông tin chính của phần tử bảo mật được tạo ra (bước 160) trong ánh sáng có thể nhìn thấy được rơi vào khoảng bước sóng từ 380 đến 750 nm hoặc bằng cách sử dụng nguồn ánh sáng tạo ra sự chiếu sáng về mặt quang phổ tương ứng với ánh sáng tự nhiên rơi vào khoảng bước sóng nêu trên bằng một phương tiện tạo ảnh kỹ thuật số thích hợp, như điện thoại di động, điện thoại thông minh, máy quét (cầm tay), máy quay web (web camera), tùy ý máy quay, thường có độ phân giải trung bình.

Sau bước này, việc xử lý sơ bộ ảnh của ký hiệu mã được thực hiện (bước 170), trong đó đầu tiên chất lượng của ảnh được kiểm tra: trong trường hợp của ảnh có chất lượng không thỏa đáng (do, ví dụ sự chiếu sáng không thỏa đáng), thì ảnh của ký hiệu mã được bỏ qua và ảnh của ký hiệu mã mới được ghi lại. Nếu ký hiệu mã được ẩn vào trong phần minh họa có tính chất trang trí, thì tách rời ảnh của ký hiệu mã từ phần minh họa có tính chất trang trí cũng được thực hiện trong quá trình xử lý sơ bộ. Cách thức tiến hành tách phụ thuộc vào cách ẩn ảnh; về vấn đề này, Công bố đơn sáng chế quốc tế số W099/35819 nêu trên, bộc lộ chi tiết giải pháp minh họa có thể. Các phương pháp tách khác đã biết đối với người có hiểu biết trung bình về lĩnh vực kỹ thuật này và, do đó không được thảo luận chi tiết ở đây. Đối với bước kết thúc của bước xử lý sơ bộ, ảnh của ký hiệu mã được chuyển đổi thành ảnh bóng mờ xám và nhờ đó ảnh thang đo xám thu được được lưu giữ để tiếp tục phân tích.

Sau khi hoàn thiện các bước xử lý sơ bộ nêu trên theo trật tự bình thường, việc kiểm tra thông tin phụ được đưa vào thành mã mang thông tin chính ở thời điểm tạo ra phần tử bảo mật được áp dụng cho ấn phẩm in (bước 180). Về vấn đề này, việc phân loại các chấm dựa vào mã mang thông tin chính được thực hiện một lần nữa. Sau khi hoàn thành việc phân loại, tiến hành phân tích thống kê các chỉ số thang đo xám của các nhóm thu được. Đối với ảnh chụp của bản in gốc, các chỉ số thang đo xám của các nhóm phải giảm liên tục. Buộc phải tiến hành phân tích thống kê vì sự biến dạng của máy quay. Ở đây, thử nghiệm-t hai mẫu thử là phương pháp thích hợp với giả thuyết trung bình1 =trung bình2 ngược lại với giả thuyết thay thế trung bình1 <trung bình2 với mức đáng kể là p=0,05. Điều rõ ràng đối với người có hiểu biết trung bình về lĩnh vực kỹ thuật này là, thay vì thử nghiệm-t, trong trường hợp này các thử nghiệm thống kê khác có khả năng áp dụng như nhau.

Khi sao chép, các đảo điểm ảnh tạo ra vùng trắng rất nhỏ trở nên gần lại với nhau, và do đó sự tăng các chỉ số trung bình thang đo xám thu được của các nhóm không còn tồn tại. Việc gần lại với nhau sinh ra do các bước trong quá trình sao chép. Về qui trình

này, số lượng của các điểm ảnh tạo ra vùng trắng và cách bố trí của các điểm ảnh nêu trên là rất quan trọng. Vùng trắng phải thể hiện khổ rộng, dọc theo ít nhất một chiều của nó, tương ứng độ rộng khổ có thể in màu trắng nêu trong Bảng 1 sao cho máy quét hoặc máy photocopy được sử dụng có thể chắc chắn loại bỏ các điểm ảnh của vùng xóa đi. Trong trường hợp như vậy, ấn phẩm in được kiểm tra được xem là "giả mạo". Nhờ vào sự phân tích thống kê, nếu có thể nói rằng sự tăng các chỉ số trung bình thang đo xám thu được của các nhóm bảo vệ, thì ấn phẩm in được kiểm tra có trang bị phần tử bảo mật của sáng chế được coi là "thật".

Fig.7 minh họa một vài mã điểm làm ví dụ mang thông tin chính (có thể nhìn thấy bằng mắt thường), cụ thể là, từ trái sang phải, mã vạch, mã QR, mã ma trận dữ liệu và cái gọi là mã thiết kế, trong đó mỗi trong số các mã này thể hiện kích thước lớn nhất vượt qua 50 micrômet. Để tạo ra phần tử bảo mật theo sáng chế, tất cả các mã này đều có thể sử dụng được.

Sự gần lại nhau của các đảo trắng mang thông tin phụ của bản in được tạo ra bởi máy in phun được thể hiện trên Fig.8 được chụp bởi kính hiển vi trường ở hệ số phóng đại là 50x. Mặc dù vùng trắng của khuôn in ở phía bên trái biểu thị các đường ranh giới sắc nét, nhưng các vùng trắng khó có thể phát hiện được trong bản in ở phía bên phải. Ngoài ra, khi sao chép, các điểm không chắc chắn này bị đóng bởi máy photocopy, và bản sao chụp trở thành màu đen 100%.

Fig.9A và Fig.9B thể hiện một vài ví dụ về đoạn thông tin phụ ẩn trong các thiết kế.

Như vậy, để thực hiện sáng chế, tuyệt đối không cần đến thiết bị kiểm tra cụ thể; về vấn đề này, ảnh được chụp, ví dụ bởi điện thoại thông minh và phần mềm giải mã và phân tích dựa vào phương pháp được thể hiện trên Fig.1B được cài đặt trong điện thoại là đủ. (Tuy nhiên, ảnh hoặc phần biểu diễn dạng số của phần tử bảo mật có thể được chụp bằng máy quay bất kỳ, và phần mềm phân tích có thể thực hiện bằng máy tính có khả

năng tính toán thích hợp.) Thiết bị kiểm tra có thể là thiết bị chế tạo theo đơn đặt hàng riêng; thiết bị này cần chứa bộ đọc (CCD, CMOS), ví dụ máy quay số, để tạo ra phần biểu diễn dạng số của phần tử bảo mật, bộ xử lý dữ liệu, ví dụ bộ vi điều khiển hoặc bộ xử lý, ưu tiên là bộ nhớ, cũng như chính phần mềm giải mã. Việc áp dụng phần tử bảo mật của sáng chế trên nền in không cần đến máy in có độ chính xác cao; về vấn đề này máy in phun có độ phân giải khoảng 600 dpi là thích hợp. Điều này cho phép khả năng áp dụng rộng rãi đối với giải pháp của sáng chế.

Nhìn chung, do thông tin phụ không được lưu giữ trong cơ sở giữ liệu, nên để kiểm tra tính xác thực của ấn phẩm in có phần tử bảo mật theo sáng chế, không cần phải có đường link (đường liên kết) liên lạc dữ liệu. Thông tin (thứ hai) ẩn có thể được suy ra từ thông tin chính, và do đó, nó chỉ thuần túy là một thiết bị kiểm tra thực sự cần để kiểm tra tính xác thực.

Tuy nhiên, điều rõ ràng đối với người có hiểu biết trung bình về lĩnh vực kỹ thuật này là khái niệm/thuật toán mã hóa được chọn trước đây cho thông tin phụ (hoặc chìa khóa tạo ra của nó) có thể được lưu giữ trong cơ sở giữ liệu từ xa. Trong trường hợp như vậy, trong khuôn khổ của phương pháp kiểm tra tính xác thực, thiết bị kiểm tra xác lập sự kết nối với cơ sở giữ liệu qua kênh thông tin giữ liệu thích hợp, thẩm vấn chìa khóa tạo ra nếu cần, và sau đó tiến hành kiểm tra tính xác thực của ấn phẩm in bị thử thách. Một ưu điểm khác của phương án này là thiết bị kiểm tra cũng có thể tạo ra thông tin chính xác cho cơ sở dữ liệu về vị trí địa lý của sự thẩm vấn chìa khóa như là kết quả của việc liên lạc dữ liệu được thiết lập. Nếu thiết bị kiểm tra là điện thoại di động hoặc điện thoại thông minh, thì thông tin nêu trên có thể dễ dàng được tạo ra dưới dạng là cơ sở dữ liệu di động hoặc các tọa độ GPS.

Ngoài ra, khi phần tử bảo mật của sáng chế cần áp dụng, thì không cần đến cả (các) mực in đắt đỏ của chế phẩm cụ thể lẫn các nền in đắt đỏ được tạo ra một cách đặc biệt. Điều rõ ràng với người có hiểu biết trung bình về lĩnh vực kỹ thuật là, phần tử bảo mật của sáng chế cũng có thể được tạo ra trên/tròn bề mặt của đối tượng cần được bảo vệ

bằng cắt bằng laze thay vì in bằng mực. Trong trường hợp ứng dụng như vậy, lớp nền dựa trên giấy được thay thế bằng vật liệu bất kỳ có thể gia công được bằng máy bằng cắt laze.

Điều cũng rõ ràng đối với người có hiểu biết trung bình về lĩnh vực kỹ thuật này là phần tử bảo mật theo sáng chế có thể được sử dụng theo cách riêng rẽ hoặc kết hợp với các phần tử bảo mật khác như là thành phần bổ sung.

YÊU CẦU BẢO HỘ

1. Phần tử bảo mật khi được áp dụng lên nền in như là bản in, phần tử bảo mật này bao gồm: mã mang thông tin chính và có thể phát hiện được bằng mắt thường trong ánh sáng có thể nhìn thấy được trong khoảng bước sóng từ 380 đến 750 nm, và được kết hợp vào đó, một mã mang thông tin phụ và không thể đọc được bằng mắt thường, khác biệt ở chỗ, kích thước lớn nhất của mã mang thông tin phụ theo ít nhất một hướng nằm ngang là từ 2 đến 40 micrômet, và mã mang thông tin phụ là không thể tái tạo được từ bản in và coi là phần tử bảo mật có đặc điểm có thể phân tích được bằng phương pháp thống kê.

2. Phần tử bảo mật theo điểm 1, khác biệt ở chỗ, đặc điểm có thể phân tích được bằng phương pháp thống kê được tạo ra bởi các chỉ số thang đo xám của các đoạn của ảnh của bản in của phần tử bảo mật nêu trên được chụp trong ánh sáng có thể nhìn thấy được trong khoảng bước sóng từ 380 đến 750 nm, các đoạn nêu trên được chọn theo khái niệm mã hóa thiết lập trước.

3. Phần tử bảo mật theo điểm 1 hoặc 2, khác biệt ở chỗ, mã mang thông tin chính được chọn từ nhóm bao gồm: các mã vạch, các mã đáp ứng nhanh (mã QR), các mã ma trận dữ liệu, và các mã được phát triển độc nhất bằng cách mã hóa ẩn.

4. Phần tử bảo mật theo điểm 1 hoặc 2, khác biệt ở chỗ, nền in được tạo ra có phần minh họa đồ họa trang trí và mã mang thông tin chính được ẩn trong phần minh họa này.

5. Phần tử bảo mật theo điểm bất kỳ trong số các điểm từ 1 đến 4, khác biệt ở chỗ, thông tin phụ có được từ thông tin chính.

6. Phần tử bảo mật theo điểm bất kỳ trong số các điểm từ 1 đến 4, trong đó mã mang thông tin phụ được tạo ra từ các vùng của mã mang thông tin chính không được in trực tiếp lên đó.

7. Phần tử bảo mật theo điểm bất kỳ trong số các điểm từ 1 đến 6, khác biệt ở chỗ, nền in được chọn từ nhóm bao gồm: giấy bạc ngân hàng, trái phiếu, hóa đơn, bao gói sản phẩm,

nhãn mác/thẻ nhận dạng, bìa sách, vé vào cửa, giấy chứng nhận, các tài liệu cá nhân, chứng thư hoặc các tài liệu bất kỳ khác hoặc các bề mặt đối tượng cần được trang bị bảo vệ sao chép.

8. Ấn phẩm in, khác biệt ở chỗ, ấn phẩm in này bao gồm nền in và ít nhất một phần tử bảo mật theo điểm bất kỳ trong số các điểm từ 1 đến 7, được áp dụng lên nền in bằng cách in.

9. Phương pháp kiểm tra tính xác thực của ấn phẩm in có phần tử bảo mật theo điểm bất kỳ trong số các điểm từ 1 đến 7, phương pháp này bao gồm các bước:

ghi ảnh của mã mang thông tin chính của phần tử bảo mật khi chiếu sáng bằng ánh sáng có thể nhìn thấy trong khoảng bước sóng từ 380 đến 750 nm;

chuyển đổi ảnh thu được thành ảnh thang đo xám và lưu giữ ảnh thang đo xám này;

phân đoạn ảnh thang đo xám được lưu giữ;

phân loại các đoạn của ảnh thang đo xám đã phân đoạn thành số lượng các nhóm nhất định phù hợp với thuật giải mã hóa thiết lập trước;

ấn định chỉ số trung bình thang đo xám như là đặc điểm có thể phân tích được bằng phương pháp thống kê, cho mỗi nhóm bằng cách đưa các nhóm nêu trên sang phân tích thống kê nhóm nọ sau nhóm kia;

tạo ra xu thế từ các chỉ số trung bình thang đo xám thu được thay đổi nhóm theo nhóm;

đưa ra quyết định về tính xác thực của ấn phẩm in nêu trên dựa vào hình dạng của xu thế nêu trên.

10. Phương pháp theo điểm 9, trong đó ảnh nêu trên được tạo ra bằng thiết bị tạo ảnh có độ phân giải từ 300 đến 1200 dpi.

11. Phương pháp theo điểm 9 hoặc 10, trong đó phương pháp này còn bao gồm bước tách ảnh của mã mang thông tin chính ra khỏi phần minh họa có tính chất trang trí nếu mã nêu trên được ẩn trong phần minh họa có tính chất trang trí trước khi chuyển đổi ảnh được ghi nhận của mã nêu trên thành ảnh thang đo xám.

12. Phương pháp theo điểm bất kỳ trong số các điểm từ 9 đến 11, trong đó việc phân tích thống kê các nhóm được tiến hành bởi thử nghiệm-t hai mẫu của các cặp nhóm.

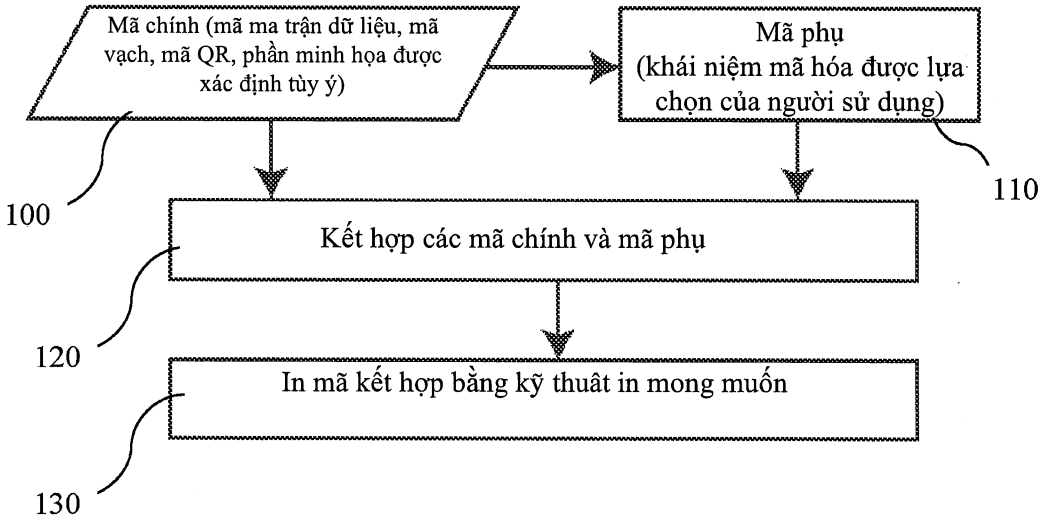

Mã chính (mã ma trận dữ liệu, mã vạch, mã QR, phần minh họa được xác định tùy ý)
Mã phụ (khái niệm mã hóa được lựa chọn của người sử dụng)
100
110
Kết hợp các mã chính và mã phụ
120
In mã kết hợp bằng kỹ thuật in mong muốn
130

Fig. 1A

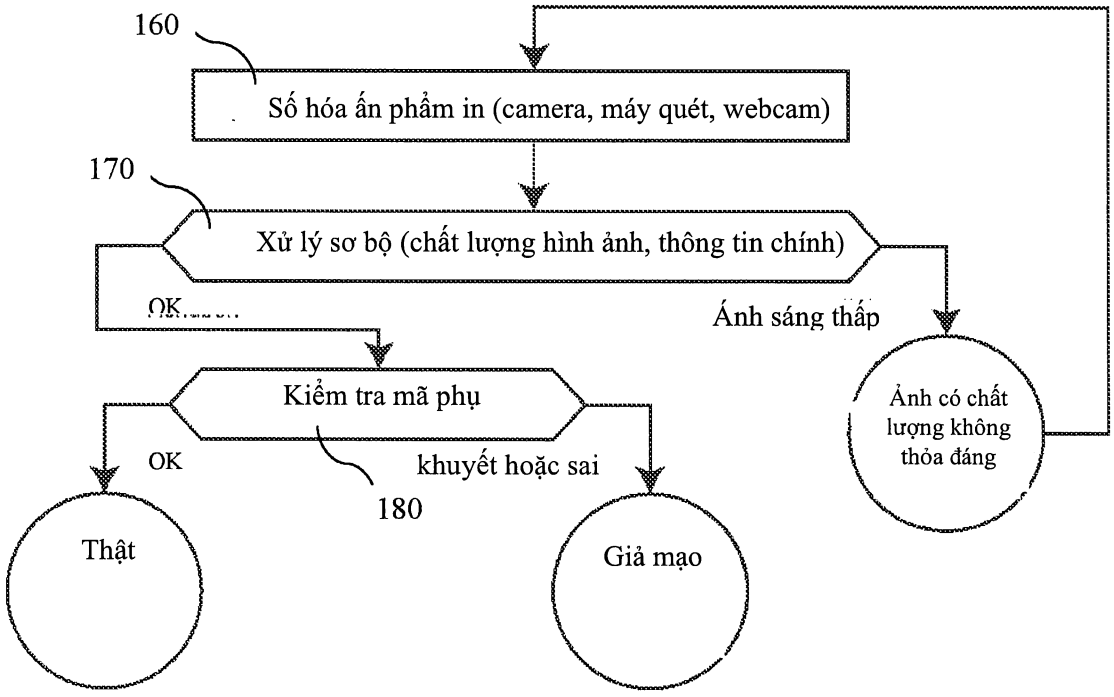

160
Số hóa ấn phẩm in (camera, máy quét, webcam)
170
Xử lý sơ bộ (chất lượng hình ảnh, thông tin chính)
OK
Ánh sáng thấp
Kiểm tra mã phụ
Ảnh có chất lượng không thỏa đáng
OK
khuyết hoặc sai
180
Thật
Giả mạo

Fig.1B

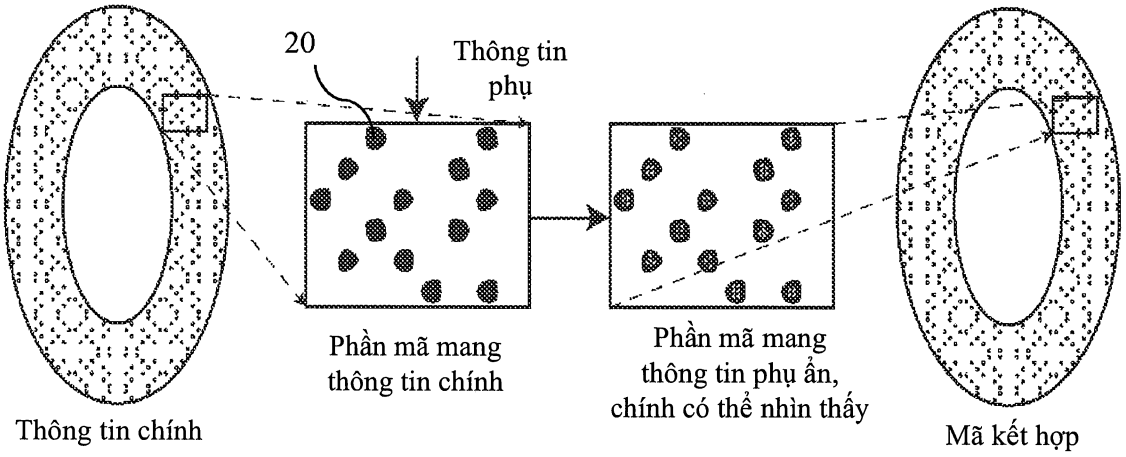


Fig.2

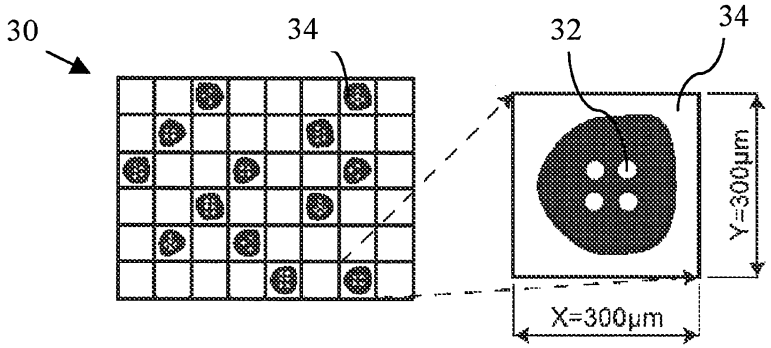


Fig.3

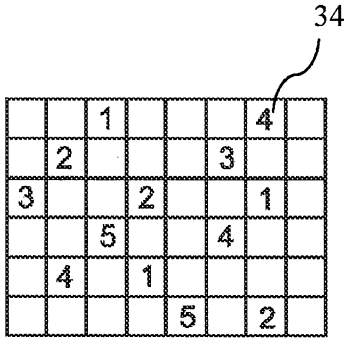


Fig.4

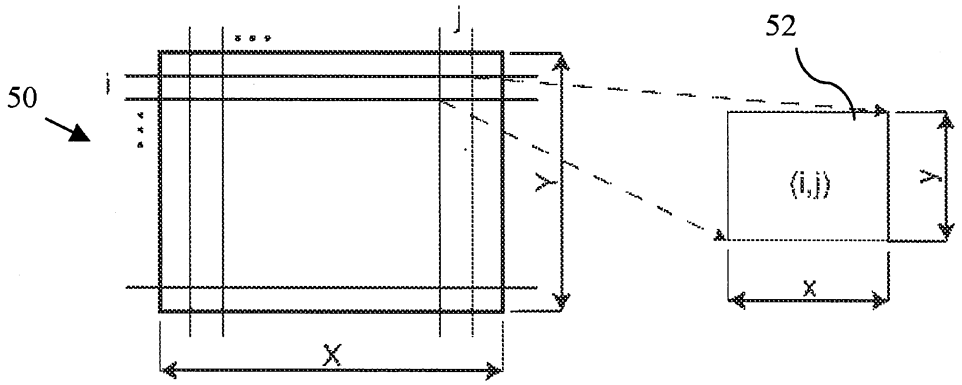


Fig. 5

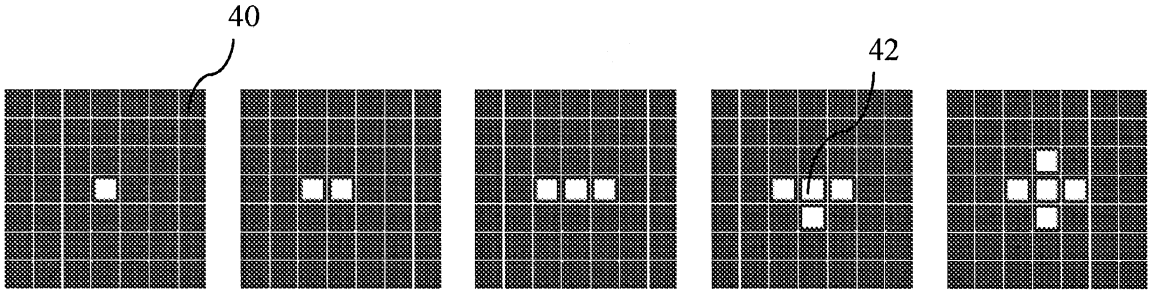


Fig. 6

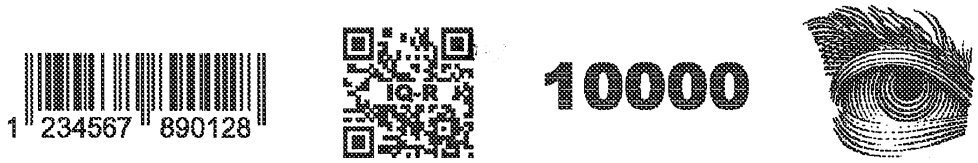


Fig. 7

Fig. 8

Fig. 9A

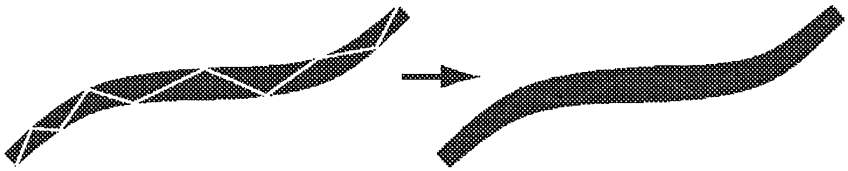


Fig. 9B