República Federativa do Brasil

Ministério do Desenvolvimento, Indústria, Comércio e Serviços

Instituto Nacional da Propriedade Industrial

(11) BR 112014020232-0 B1

(22) Data do Depósito: 15/02/2013

(45) Data de Concessão: 31/01/2023

(54) Título: ELEMENTO DE SEGURANÇA, MATERIAL IMPRESSO E MÉTODO PARA INSPECIONAR AUTENTICIDADE DE TAL MATERIAL

(51) Int.Cl.: H04N 1/32; G07D 7/202.

(52) CPC: H04N 1/32251; H04N 1/32325; H04N 1/32352; G07D 7/2041.

(30) Prioridade Unionista: 15/02/2012 HU P1200097.

(73) Titular(es): GLENISYS KFT..

(72) Inventor(es): ATTILA BIRÓ; GÁBOR KRISTÓ; PIROSKA REMÉNYI.

(86) Pedido PCT: PCT IB2013051260 de 15/02/2013

(87) Publicação PCT: WO 2013/121401 de 22/08/2013

(85) Data do Início da Fase Nacional: 15/08/2014

(57) Resumo: ELEMENTO DE SEGURANÇA, MATERIAL IMPRESSO E MÉTODO PARA VERIFICAR AUTENTICIDADE DE TAL MATERIAL. A invenção refere-se a um elemento de segurança aplicado em substratos de impressão (notas de banco, valores mobiliários, embalagens de produto, cartões/etiquetas de identidade ou outros documentos similares) por impressão, compreendendo um identificador único como informação primária visível a olho nu e informação secundária contra cópia não visível a olho nu. O identificador único é normalmente um código de ponto. Referida informação secundária é representada por uma estrutura com a dimensão maior de 2 a 40 (Mi)m, e, devido às distorções de impressão resultantes quando o elemento de segurança é aplicado sobre um substrato de impressão, referida informação secundária é não reconstruível a partir da impressão do elemento de segurança e uma característica inerente estatisticamente analisável é associada a ele. A invenção também se refere a um material impresso com um tal elemento de segurança inventivo e a um método para verificar autenticidade de um material impresso com o elemento de segurança inventivo em luz visível (380 -750 nm).

ELEMENTO DE SEGURANÇA, MATERIAL IMPRESSO E MÉTODO PARA INSPECIONAR AUTENTICIDADE DE TAL MATERIAL

Campo da invenção

[001] A presente invenção refere-se a um elemento de segurança, bem como a um método para verificar a autenticidade de uma impressão disposta sobre um substrato de impressão. Seu campo de aplicação cai no domínio de proteção de materiais impressos produzidos por máquinas de impressão ou documentos gerados com impressoras jato de tinta e/ou impressoras a laser, contra falsificação.

Fundamentos da invenção

[002] Por enquanto, tecnologias de fotocópia e impressão a laser passaram por uma enorme melhoria. Como resultado, reprodução de alta qualidade de vários materiais impressos tornou-se significativamente simplificada usando essas técnicas. Ao mesmo tempo, infelizmente, falsificação de materiais impressos valiosos ou personalizados tornou-se mais fácil também. Assim, a proteção desses documentos contra a falsificação veio à tona. Qualquer documento fornecido com uma portadora de dados, tal como, por exemplo, uma escrita ou desenho produzido por, por exemplo, uma máquina de impressão ou uma impressora jato de tinta e/ou uma laser, pode constituir um material impresso que requer proteção. Tais materiais impressos são, por exemplo, os vários rótulos de embalagens (por exemplo, para medicamentos, capas de CD), bilhetes de entrada valiosos, certificações, notas de banco, cheques, identificadores pessoais, vários vouchers, etc., só para citar apenas alguns exemplos. Para evitar (ou minimizar) uso indevido, referidos materiais impressos são geralmente fornecidos

pelos elementos de segurança apropriados. Em geral, os elementos de segurança aplicados e/ou suas combinações são bastante complicados.

[003] Um grande número de soluções existe no domínio da proteção de impressão. Em uma classe das mesmas, o elemento de segurança fornecendo proteção é escondido na própria imagem impressa. Panfleto de Pedido de Patente Internacional No. W099/35819 e Patente No. US 1996/019310 divulgam soluções baseadas em apenas este conceito. De acordo com as soluções ensinadas, uma imagem secundária não visível a olho nu, mas visível a um dispositivo de decodificação específico é escondida dentro de uma imagem principal que é visível a olho nu. Os parâmetros físicos das técnicas utilizadas para criar referida imagem secundária podem ser escolhidos de tal maneira que a imagem secundária desaparece simplesmente mediante cópia do substrato (o documento) material impresso em cima com a imagem combinada. Ou seja, esta informação não pode ser reconstruída a partir de uma cópia da impressão. Para implementar as soluções em questão, no entanto, uma máquina de impressão de alta precisão (com uma resolução de pelo menos 8000 dpi) é necessária, e para inspecionar autenticidade da impressão, há uma necessidade também para uma lente de decodificação. Devido a estes inconvenientes, a aplicação de referidas soluções não faz/faria tornar-se bem espalhado na prática cotidiana, onde - como consequência dos avanços alcançados em impressão digital - a proteção dos materiais impressos com impressões produzidas por máquinas em geral com resolução muito menor (tipicamente de 600 dpi) tem de ser salvaguardada.

[004] O elemento de segurança divulgado em Patente RU No. 2.430.836 é um elemento de segurança forte que pode ser inspecionado a olho nu e dá uma experiência estética extraordinária. No entanto, a aplicação do elemento de segurança obtido sobre um substrato de impressão requer o uso de um máquina de impressão específica (intaglio). Tais máquinas de impressão são tipicamente propriedade de impressoras de notas, e, assim, o acesso a tais máquinas é bastante limitado.

[005] Em uma outra classe de proteção de cópia, é a tinta de impressão usada para aplicar a impressão e/ou o substrato de impressão em si que é feito específico, e é tentado conseguir a natureza não copiável desta forma. Tais soluções são divulgadas, por exemplo, em Patente EP Nos. 2.004.414; 1.858.605; 1.827.864 e 1.779.335. A maior desvantagem das soluções em causa é devido às tintas específicas e, portanto, relativamente caras (por exemplo, tintas de impressão com pigmentos opticamente variáveis) ou o uso de substratos de impressão específicos que podem ser produzidos a custos relativamente elevados, também.

[006] Em uma ainda outra classe de proteção de impressão, a impressão compreende um ou mais identificadores que associam a impressão com uma base de dados. Patente US No. 6.952.485 ensina uma tal marca d’água eletrônica como o identificador. Aqui, um ruído incorporado na imagem e não é visível a olho nu transporta a informação. A marca d'água eletrônica pode ser reconstruída a partir da cópia preparado pela reprodução sem alterações, o que é referida marca d'água eletrônica é sempre transferida por cópia. Um campo de aplicação para as

referidas marcas d'água eletrônicas é a proteção de notas contra a cópia. Em particular, uma tal marca d'água eletrônica é incluída nas notas de Euro como elemento de segurança. Esta marca d'água é reconhecida pelo acionador de cada máquina de impressão única vendida hoje em dia, e depois simplesmente recusa a imprimir a imagem compreendendo a marca d'água eletrônica. Uma desvantagem desta técnica reside no fato que é necessário um amplo acordo entre os fabricantes de impressora e scanner como para a marca d'água eletrônica usada para proteção contra cópias. Isso significa que este tipo de proteção de impressão pode ser usado apenas em materiais impressos altamente excepcionais. Além disso, a marca d'água proibida tem que ser "ensinada" a cada acionador de impressora/scanner. Uma outra desvantagem desta técnica origina apenas a partir do último: dispositivos de impressão fabricados antes do acordo ter sido feito simplesmente não reconhecem a marca d'água proibida, e, assim, eles imprimem o material impresso protegido pela referida marca d'água.

[007] De acordo com a solução revelada no Pedido de Patente Internacional No. PCT/EP2009/061073, um identificador primário visível e um único elemento de imagem de interferência aleatório (informação secundária) que não é visível a olho nu são dispostos sobre um artigo a ser protegido durante fabricação. O referido identificador primário e o elemento de imagem, também referidos como informação secundária, são armazenados em uma base de dados através da Internet em forma digitalizada. Quando autenticidade de um artigo é inspecionada, com base na

informação primária, a imagem armazenada no banco de dados é procurada e, em seguida, é comparada com uma foto do artigo inspecionado tomada no local. Uma desvantagem da solução é em que para realizar a inspeção, um acesso ao banco de dados remoto é necessário em todos os casos que necessitam a disponibilidade de uma conexão de comunicação de dados com uma largura de banda adequada.

[008] Em uma ainda outra classe de proteção de impressão, para inspecionar autenticidade de uma impressão, interferência do dispositivo de impressão e o suporte de impressão durante impressão é explorado. Pedido de Patente No. US 2002/0037093 se refere a uma solução em que uma máquina de fotocópia ou uma impressora laser "falha" o substrato de impressão (papel) que passa por ela aleatoriamente com toner ou micropontos de tinta não visíveis a olho nu quando a cópia é preparada. Ou seja, através da análise de uma imagem digital de alta definição de um documento, se toner ou micropontos de tinta são procurados especialmente em partes do referido documento que transportam nenhuma impressão, pode-se inequivocamente decidir se ou não o documento é gerado por cópia. Uma desvantagem desta técnica reside em que para a realização do estudo, um meio de digitalização de alta resolução é necessário.

[009] Pedido de Patente Japonês No. 2009/034921 A descreve um material impresso fornecido com um meio antifraude compreendendo uma Figura latente modelada de linha, que é uma informação secundária. Em pelo menos uma borda lateral de cada linha constituinte de referida Figura latente, é formada uma pluralidade de regiões de projeção

estendidas cobertas de tinta salientes ao longo da direção de largura de linha, muito próximas uma da outra. Quando esse documento é copiado, as lacunas entre as respectivas regiões de projeção estendidas ficam enterradas por tinta em harmonia com as características de reprodução da máquina copiadora. Por conseguinte, a largura de linha de cada constituinte de linha de referido padrão de linha expande que praticamente resulta no "desenvolvimento"/aparecimento da imagem latente, assim como da informação secundária.

[0010] Por enquanto, códigos de barra, códigos Matriz de Dados, vários códigos QR, códigos móveis e outros códigos similares (a partir de agora, códigos de ponto, em geral) se tornaram meios de portadora de informação bem espalhados. Sua popularidade deve-se principalmente ao espalhamento rápido de telefones celulares, especialmente de telefones inteligentes. Sua desvantagem reside no fato que, em geral, não contêm qualquer proteção de cópia e, portanto, sua aplicação como elementos de segurança é altamente limitada.

[0011] Em face do exposto, é evidente que apesar de uma pluralidade de tecnologias de proteção de impressão ser disponível para proteger impressões a serem equipadas com proteção de cópia e imprimir substratos/documentos com essas impressões, as tecnologias são muito caras ou exigem um conjunto específico de dispositivos para sua criação e/ou inspeção.

[0012] É uma demanda natural, no entanto, que a autenticidade de um documento seja determinada simplesmente e rapidamente por qualquer pessoa em qualquer lugar essencialmente sem a necessidade de competência adicional e

equipamentos técnicos.

[0013] Em face do exposto, um objetivo primário da presente invenção consiste em fornecer um elemento de segurança aplicado a um substrato de impressão por meio de impressão que, por um lado, contém dados de identificação associados com o próprio material impresso como informação primária e, por outro lado, também fornece uma proteção confiável para copiar o material impresso via informação secundária latente.

[0014] Um outro objetivo da presente invenção é fornecer uma técnica de proteção de impressão, especialmente um método para inspecionar/determinar autenticidade de impressão que permite verificação de autenticidade de um material impresso com um elemento de segurança de acordo com a invenção para qualquer um e sem qualificação em segurança de informação imediatamente e no local por meio de dispositivos de pelo menos resolução média (ou seja, de 300 a 1200 dpi) que estão disponíveis no uso cotidiano, como por exemplo, celulares, tablets, telefones inteligentes (smartphones), câmeras de internet, etc..

[0015] Nossos estudos nos levaram à conclusão que um elemento de segurança realizando o objetivo da invenção pode ser realizado através da combinação de um código convenientemente escolhido transportando informação primária com uma parte de informação secundária, em que a informação secundária não pode ser reconstruída a partir da própria impressão (ou suas cópias), mas fornece uma característica inerente que pode ser analisada por métodos estatísticos. Uma estrutura portando tal informação

secundária pode ser gerada sob a forma de áreas incorporadas (preferencialmente pelo fabricante) no código portando informação primária de acordo com um conceito/algoritmo de codificação predefinido, e não impressa em cima diretamente. Devido a distorções/incertezas de impressão, tais como por exemplo, a deformação do substrato de impressão e/ou a placa de impressão por contacto entre si ou o umedecimento de tinta inevitável da tinta de impressão aplicada sobre o substrato de impressão, surgindo quando a impressão é executada, as áreas deixadas fora a partir de impressão direta tornam-se mais ou menos cobertas por tinta. De acordo com os nossos estudos, uma condição para referida área (s) deixada para fora ser indetectável a olho nu na impressão do elemento de segurança é que a maior dimensão da referida área (s) deixada para fora no interior da impressão ao longo de pelo menos uma direção é 2 a 40 µm, dependendo da tecnologia de impressão aplicada e a qualidade do substrato de impressão. Embora, devido às incertezas de impressão, a informação secundária em causa não será toda detectável a olho nu na impressão do elemento de segurança, nem sua natureza ordenada é reconhecível por uma lupa (em uma ampliação de 2-20x), verificou-se que a incorporação da referida informação secundária altera o valor de escala de cinza da referida porção da representação digital da impressão em que, na verdade, tinha sido incorporada. Através da alteração do valor de escala de cinza, referida informação secundária atribui o elemento de segurança inventivo com uma característica inerente de que pode ser analisada por métodos estatísticos, em que o resultado da análise é

característico do próprio elemento de segurança e, assim, pode ser utilizado como um elemento de proteção de cópia para o elemento de segurança, bem como para o substrato de impressão tendo um tal elemento de segurança.

[0016] O objetivo visando do fornecimento de um elemento de segurança é conseguido através do elemento de segurança de acordo com a reivindicação 1. Possíveis outras modalidades preferidas do elemento de segurança inventivo são definidas pelas reivindicações 2 a 6. O objetivo visando do fornecimento de um método para inspecionar a autenticidade de uma impressão é conseguido pelo método de acordo com a reivindicação 8. Outras variantes preferidas do método da invenção são definidas nas reivindicações 9 a 11.

Breve descrição das figuras

[0017] De modo que a invenção possa ser descrita mais claramente, modalidades serão agora descritas em maior detalhe com referência aos desenhos anexos, em que:

- a Figura 1A mostra o diagrama de blocos de um método para gerar um elemento de segurança de acordo com a invenção e para aplicá-lo sobre um substrato de impressão;

- a Figura 1B mostra o diagrama de blocos de um método de inspeção de autenticidade com base na aplicação de um elemento de segurança de acordo com a invenção;

- a Figura 2 mostra esquematicamente o modo de geração de um código combinado, que constitui o elemento de segurança, a partir de códigos portando informação primária e secundária;

- a Figura 3 mostra uma porção do código combinado da Figura 2 em vista ampliada;

- a Figura 4 ilustra a decomposição da porção de código combinado ilustrado na Figura 3 em classes em termos da informação secundária, realizada em conjunto com um conceito de codificação estabelecido pelo fabricante;

- a Figura 5 mostra uma célula de código generalizada aplicável quando a informação secundária é introduzida em um ponto de código;

- a Figura 6 ilustra um par de possíveis modalidades preferidas da área (s) deixada de fora (pixels) que representam informação secundária que são aplicáveis em um elemento de segurança de acordo com a invenção;

- a Figura 7 mostra diversos exemplos de códigos de ponto (visíveis a olho nu) transportando informação primária que tem a maior dimensão superior a 50 µm;

- a Figura 8 ilustra a aparência teórica (como formada em uma placa de impressão) e a aparência real (como pode ser vista depois de ser impressa sobre um substrato de impressão) de uma porção do elemento de segurança fornecido pelo código combinado; e

- as Figuras 9A e 9B ilustram uma parte de informação secundária (latente) que tem uma dimensão de no máximo 50 µm ao longo de pelo menos uma direção, escondida em um desenho tipo ponto e tipo linha, respectivamente, antes e depois da impressão.

Descrição detalhada da invenção

[0018] Um método geral para gerar um elemento de segurança de acordo com a invenção formado por um código combinado é mostrado na Figura 1A. De acordo com este, um código que transporta informação é escolhido (passo 100) que é formado por um sinal de código bem conhecido (por

exemplo, um código de barras, um código QR, um código de Matriz de Dados, um código de celular) ou uma linha codificada de forma única ou código de ponto. De acordo com ainda uma outra possibilidade, o código portando informação primária também pode ser formado por um código de ponto ou linha escondido dentro de uma ilustração gráfica ornamental da impressão. Além disso, o código portando informação primária pode ser a própria informação primária, material impresso simplesmente sobre o substrato de impressão de forma não codificada. O substrato de impressão pode ser qualquer documento ou a superfície de um objetivo a ser protegido; em particular, por exemplo, notas, títulos, faturas, embalagens de produtos, cartões/etiquetas de identidade, capas, bilhetes de entrada, certificados, documentos pessoais, comprovantes ou quaisquer outros documentos similares. A informação primária significa uma parte de informação que se relaciona com o documento a ser protegido, em geral, os dados identificando o próprio documento. É importante que o código portando informação primária possa ser segmentado, isto é, possa ser coberto por uma malha de células de um dado tamanho e normalmente de forma regular (em particular, forma retangular), sendo, opcionalmente, rodado com um certo ângulo em relação ao código portando informação primária. Devido ao desenho de construção, este último requisito é automaticamente cumprido para os sinais de código bem conhecidos acima mencionados.

[0019] Depois de selecionar o código portando informação primária, um código que carrega informação secundária é gerado (passo 110). Este passo é realizado em

harmonia com um conceito/algoritmo de codificação predefinido de uma forma discutida para um exemplo específico no que segue com referência às Figuras 2-4 em mais detalhe. Em particular, a informação secundária é carregada pelas áreas deixadas para fora da impressão do código portando informação primária. Devido ao seu tamanho, o código portando informação secundária é uma parte de informação latente, ou seja, não é visível quando inspecionado a olho nu. Tal informação secundária exemplar definida pelas áreas deixadas para fora é ilustrada nas Figuras 3 e 6. A informação secundária resulta preferencialmente a partir da informação primária, por exemplo, a partir de um elemento/dados da mesma.

[0020] Depois de gerar o código portando informação secundária, os códigos portando informação primária e secundária são combinados (passo 120), como um resultado de que um código combinado que corresponde ao elemento de segurança inventivo é obtido.

[0021] Finalmente, o material impresso com o elemento de segurança é produzido através da aplicação do elemento de segurança assim obtido sobre o substrato de impressão através da tecnologia de impressão selecionada (passo 130).

[0022] O elemento de segurança do material impresso produzido pelo método mostrado na Figura 1A, por um lado, contém dados que podem ser utilizados para identificar referido material impresso (informação primária) e, por outro lado, é adequado para proteger referido material de impressão contra cópia, enquanto a informação secundária é uma informação latente que não é visível a olho nu e

desaparece ou fica distorcida em uma forma detectável quando sendo impressa/copiada.

[0023] As Figuras 2-4 ilustram os passos de combinar os códigos portando informação primária e secundária em um caso específico, em que o código portando informação primária é fornecido por um código de ponto (ver Figura 2) formado por pontos de tinta 20 e representando um valor "0" impresso na resolução de 600 dpi, em que segmentação é realizada por meio de uma malha 30 de células em forma de quadrado 34 (ver Figura 3). Aqui, o tamanho de cada célula 34 é, pelo menos, 300 µm ao longo de ambas as direções X e Y. Verificou-se que o tamanho de 300 µm é suficiente para assegurar que cada ponto de tinta individual 20 caia em uma célula separada 34 e longe das fronteiras da referida célula 34 (isto é, praticamente no centro da célula 34). Além disso, cada célula 34 é dividida em sete por sete pixels 40 (neste caso específico), os pixels 40 formando unidades da referida divisão são os "blocos de construção" para as áreas deixadas de fora 32, 42 codificando informação secundária. É evidente para um perito na arte que segmentação pode ser realizada com diferentes tamanhos de células e/ou com diferentes números de pixels ao longo das direções X, Y por células para um tipo diferente de sinal de código. Uma malha retangular comum 50 e 52 e sua (i,j)-ésima célula 52 aplicável para segmentar são mostradas na Figura 5. Também é notado aqui que se maior resolução é usada, o número de pixels ao longo de cada uma das direções deve ser aumentado proporcionalmente.

[0024] Tendo segmentado o código que carrega

informação primária, introdução do código que carrega informação secundária é realizada. Para este fim, as células 34 do código portando informação primária obtida pela segmentação e contendo um ponto de tinta, são ordenadas em várias classes. Aqui, o número de diferentes classes é escolhido para cair entre quatro e seis, no entanto, qualquer outro número de classes pode ser igualmente utilizado. Uma vez que após a impressão do elemento de segurança inventivo, a informação secundária conduz a uma característica que pode ser analisada por técnicas estatísticas, de preferência existem pelo menos dez células 34 em cada classe. A referida ordenação pode realizar-se em uma base regular ou de uma maneira aleatória, no entanto, ela sempre resulta a partir do código portando informação primária. No presente exemplo, classificação é feita em termos do número de pixels que formam a área deixada para fora dentro de cada célula. Aqui, o número inscrito em uma dada célula corresponde ao tamanho da área deixada para fora dentro da célula, expresso em pixels. O tamanho da área deixada para fora muda de classe para classe de forma estritamente crescente. Por conseguinte, por exemplo, a primeira classe permanece inalterada (isto é, não existe área deixada para fora nela), a segunda classe terá uma área deixada para fora de um pixel, a terceira classe terá uma área deixada para fora, pelo menos, dois pixels, a classe adiante terá uma área deixada para fora de pelo menos três pixels, e assim por diante.

[0025] O tamanho da área deixada para fora em cada célula 34 depende da tecnologia de impressão a ser

aplicada: o tamanho/dimensão da área deixada para fora é sempre escolhido de tal maneira que a tecnologia de impressão aplicada seja simplesmente inadequada para imprimir referida área deixada para fora bruscamente. Consequentemente, devido à incerteza de impressão das áreas deixadas para fora, referidas áreas não serão nada visíveis no elemento de segurança impresso quando inspecionado a olho nu. Além disso, a natureza ordenada da informação secundária não é reconhecível por uma lupa (em uma ampliação de 2-20x) também.

[0026] Vários exemplos de várias formas possíveis das áreas deixadas para fora formadas por pixels são mostrados na Figura 6. Forma e dimensão da área deixada para fora não podem ser arbitrárias, a última é limitada pela tecnologia de impressão a ser aplicada, tal como discutido acima. Na Tabela 1 abaixo, um par de larguras de linha de capacidade de impressão de branco proposto para a preparação do elemento de segurança inventivo, obtido empiricamente por meio de experimentos de umedecimento de tinta sobre um substrato de impressão é coletado para diferentes tecnologias de impressão. As medições de umedecimento da tinta foram realizadas com as tintas de impressão adaptadas para diferentes tecnologias de impressão, isto é, por exemplo, com uma tinta de impressão preta a partir de Hewlett Packard, com uma tinta de impressão preta de MEMJET, com a tinta de preta de pressão KODAK Prosper e uma tinta de impressão preta da Epson, em que papel fibroso usado normalmente para impressão de segurança foi aplicado como substrato de impressão na temperatura de 18-22°C (temperatura ambiente) e em 101 kPa

de pressão ambiente. Note aqui que os valores listados na Tabela 1 são válidos para os outros tipos de papel também, ainda que a resolução necessária geralmente mude. Em particular, se o substrato de impressão é, por exemplo, um papel lustroso, a impressão tem de ser realizada na resolução de pelo menos 600-1200 dpi em vez de 300-600 dpi.

[0027] Em consonância com o acima, quando uma tecnologia de impressão nova torna-se disponível, o umedecimento da tinta pode ser determinado em uma impressão piloto e, em seguida, uma largura de linha de capacidade de impressão de branco proposta para a área deixada de fora expressa em número de pixels pode ser derivada para a nova tecnologia. Para esse fim, as seguintes equações empíricas também podem ser utilizadas:

largura da linha [µm] = 1,2 * umedecimento de tinta [µm];

largura da linha [pix] = o maior inteiro de {(1,2 * umedecimento de tinta [µm] * resolução [dpi] /25,4) / 1000+0,5}, mas pelo menos 1.

Tecnologia	Resolução típica [dpi]	Umedecimento de tinta [µm] (dependente de papel)	Largura de linha de capacidade de impressão de branco (de uma área deixada de fora de impressão direta	
			[µm]	[pix]
Impressão de jato de tinta	600	10-50	12-60	1-2

Impressão a laser	720	30-40	36-48	2-3
Impressão de deslocamento	800	10-20	12-24	4-8

Tabela 1. Largura de linha de áreas deixadas de fora portando informação secundária

[0028] Embora as áreas deixadas de fora da impressão direta não sejam visíveis a olho nu na impressão do elemento de segurança, devido às incertezas de impressão elas mudam a escala de cinza da célula definida pela expressão de valor de escala de cinza = (número de pixels pretos na célula)/(número de pixels totais na célula); aqui, a alteração é inversamente proporcional ao aumento do número de pixels da área deixada para fora dentro da classe considerada. Assim, o elemento de segurança inventivo fornecido pelo código combinado discutido acima exibe uma característica inerente na forma dos valores de escala de cinza refinados acima que podem ser associados com a informação secundária latente; após a impressão do elemento de segurança e geração de uma representação digital da impressão obtida referida característica inerente pode ser analisada estatisticamente.

[0029] Decodificar o elemento de segurança inventivo aplicado sobre um substrato de impressão e, como um resultado disto, decidir sobre a autenticidade do material impresso em causa é realizado em conformidade com o esquema mostrado na Figura 1B. De acordo com isto, em um primeiro passo uma representação digital do sinal de código portando informação primária do referido elemento de segurança é gerada (passo 160) em luz visível caindo na

gama de comprimentos de onda de 380-750 nm, ou por meio da utilização de uma fonte de luz fornecendo iluminação que espectralmente corresponde à luz natural caindo dentro da referida gama de comprimentos de onda por meio de um meio de formação de imagem digital adequado, como um telefone celular, um telefone inteligente, um scanner (mão), uma câmera de internet, opcionalmente uma câmera, tendo normalmente uma resolução média.

[0030] Após este passo, pré-processamento da imagem do sinal de código é realizado (passo 170), em que, em primeiro lugar, a qualidade da imagem é inspecionada: no caso de uma imagem com qualidade insuficiente (por exemplo, devido à iluminação insuficiente), a imagem do sinal de código é desconsiderada e uma nova imagem de sinal de código é gravada. Se referido sinal de código é escondido em uma ilustração ornamental, separar a imagem do sinal de código a partir da ilustração ornamental também é realizado durante o pré-processamento. A forma de execução da separação depende do modo de ocultação; a este respeito, Panfleto de Publicação Internacional No. W099/35819, mencionado anteriormente, revela uma possível solução exemplar em detalhe. Outros métodos de separação são conhecidos por um perito na arte e, por conseguinte, não são aqui discutidos em mais detalhe. Como um passo de finalização do pré-processamento, a imagem do sinal de código é convertida em uma imagem sombreada de cinza e a imagem de escala de cinza assim obtida é, em seguida, armazenada para posterior análise.

[0031] Após concluir os passos de pré-processamento acima em boa ordem, uma verificação da informação

secundária introduzida no código portando informação primária no momento de gerar o elemento de segurança aplicado ao material impresso é realizada (passo 180). Para este fim, a classificação de pontos com base no código portando informação primária é realizada de novo. Depois de completada a classificação, uma análise estatística dos valores de escala de cinza das classes obtidas é realizada. Para a imagem tirada de uma verdadeira impressão, os valores de escala de cinza das classes têm que diminuir continuamente. A análise estatística é necessária por causa da distorção de câmera. Aqui, o teste-*t* de duas amostras é um método adequado com a hipótese de meio1 = meio2 contra a hipótese alternativa de meio1 < meio2 com um nível de significância p = 0,05. Para uma pessoa especialista na técnica é claro que, em vez de teste-*t*, outros testes estatísticos são igualmente aplicáveis neste caso.

[0032] Após cópia, as ilhas de pixel formando a pequena área deixada de fora se fecharam, e, portanto, um aumento dos valores médios de escala de cinza das classes não mais se mantém. O fechamento é causado pelos passos durante a cópia. Na medida em que se diz respeito a esse processo, o número de pixels formando a área deixada de fora e a disposição dos referidos pixels são de grande importância. A referida área deixada de fora tem de apresentar uma largura, ao longo de pelo menos uma das suas dimensões, que corresponde à largura de linha de capacidade de impressão de branco dada na Tabela 1 a fim que o scanner ou máquina fotocopiadora utilizado poderia remover os elementos de da área deixada para fora com certeza. Em tal caso, o material impresso inspecionado é considerado uma

"falsificação". Se, como um resultado da análise estatística, pode afirmar-se que o aumento dos valores médios de escala de cinza das classes se mantém, o material impresso inspecionado fornecido com o elemento de segurança inventivo é considerado como sendo "genuíno".

[0033] A Figura 7 ilustra um par de códigos de ponto exemplares portando informação primária (visível a olho nu), em particular, da esquerda para a direita, um código de barras, um código QR, um código de Matriz de Dados e um chamado código de desenho, em que cada um deles apresenta uma maior dimensão superior a 50 µm. Para gerar o elemento de segurança de acordo com a invenção, cada um deles pode ser utilizado.

[0034] O fechamento de ilhas brancas portando informação secundária de uma impressão produzida por uma impressora de jato de tinta mostrada na Figura 8 tomada por um microscópio de campo em uma ampliação de 50x. Embora a área deixada para fora da placa de impressão no lado esquerdo apresente fronteiras nítidas, as áreas deixadas de fora podem ser dificilmente detectadas na impressão no lado direito. Além disso, após cópia, esses locais incertos são fechados pela máquina de fotocópia, e a fotocópia fica preta em 100%.

[0035] As Figuras 9A e 9B ilustram alguns exemplos para uma parte de informação secundária escondida em desenhos.

[0036] Resumidamente: para conseguir a presente invenção em prática, um dispositivo de inspeção específico não é absolutamente necessário; para este fim, uma foto tirada por, por exemplo, um telefone inteligente simples e

um software de decodificação e de análise com base no método ilustrado na Figura 1B instalado no telefone são suficientes. (No entanto, a foto ou a representação digital do elemento de segurança pode ser tomada por qualquer outra câmera também, e o software de análise pode ser executado por qualquer computador com capacidade de computação apropriada.) O dispositivo de inspeção pode ser um dispositivo feito sob medida; deve conter uma unidade de leitor (CCD, CMOS), por exemplo, uma câmara digital, para gerar uma representação digital do elemento de segurança, uma unidade de processamento de dados, por exemplo, um microcontrolador ou um processador, de preferência uma unidade de memória, bem como o próprio software de decodificação. Aplicação do elemento de segurança inventivo em um substrato de impressão não necessita de uma máquina de impressão de alta precisão; para este fim uma impressora de jato de tinta com a resolução de até 600 dpi é apropriada. Isto permite uma ampla gama de aplicabilidade para a solução de acordo com a presente invenção.

[0037] À medida que a informação secundária, em geral, não é armazenada em uma base de dados, para inspecionar autenticidade de um material impresso com o elemento de segurança de acordo com a invenção, não há necessidade de um enlace de comunicação de dados. A informação latente (secundária) pode ser deduzida a partir da informação primária e, portanto, é apenas o dispositivo de inspeção que é realmente necessário para a verificação de autenticidade.

[0038] Para uma pessoa perita na arte é, no entanto, evidente que o conceito de codificação previamente

selecionado para a informação secundária (ou sua chave de geração) pode ser armazenado em uma base de dados remota. Em tal caso, no âmbito do método de inspeção de autenticidade, o dispositivo de inspeção estabelece uma conexão com o banco de dados através de um canal de comunicação de dados apropriado, interroga a chave de geração necessária, e, em seguida, realiza a verificação de autenticidade do material impresso desafiado. Uma outra vantagem de tal modalidade é que referido dispositivo de inspeção também pode fornecer informação precisa para o banco de dados sobre a localização geográfica da interrogação de chave como uma consequência da comunicação de dados estabelecida. Se o dispositivo de inspeção é um telefone celular ou um telefone inteligente, tal informação pode ser facilmente fornecida na forma de tanto os dados de base móvel ou coordenadas GPS.

[0039] Além disso, quando um elemento de segurança de acordo com a presente invenção deve ser aplicado, nem tinta de impressão cara (s) de composição específica nem substratos de impressão caros especificamente produzidos são necessários. Como também é evidente para um perito na arte, o elemento de segurança inventivo pode também ser formado em/dentro de uma superfície do objetivo a ser protegido por ablação a laser em vez da impressão de tinta. No caso de tais aplicações, o substrato baseado em papel é substituído por quaisquer materiais que podem ser maquinados por ablação a laser.

[0040] É também evidente para um perito na arte que o elemento de segurança de acordo com a presente invenção pode ser usado sozinho ou em combinação com outros

elementos de segurança como um elemento adicional ao mesmo.

[0041] Modificações dentro do escopo da invenção podem ser prontamente realizadas pelos técnicos no assunto. Isto deve ser entendido, portanto, que esta invenção não é limitada às modalidades particulares aqui descritas de modo exemplificativo.

[0042] Nas reivindicações a seguir e no Relatório Descritivo da presente invenção, exceto onde o contexto requeira o contrário devido a expressões de linguagem ou implicação necessária, o termo “compreende” ou suas variações como “compreendendo” ou “compreender”, é usado em de um modo inclusivo, que é, para especificar a presença das características descritas nas não para impedir a presença ou adição de características adicionais em várias modalidades da invenção.

REIVINDICAÇÕES

1. Elemento de segurança aplicado por uma tecnologia de impressão em um substrato de impressão, o elemento de segurança caracterizado por compreender um código (20) que porta informação primária e é detectável a olho nu em luz visível na gama de comprimentos de onda de 380 a 750 nm, bem como um código (32, 42) que porta informação secundária e que é indetectável a olho nu;

o código (32, 42) portando informação secundária sendo combinado com o código (20) portando informação primária;

em que a maior dimensão do código (32, 42) portando informação secundária em pelo menos uma direção planar é de 2 a 40 µm,

em que a maior dimensão do código (32, 42) portando informação secundária é escolhida baseada na resolução da tecnologia de impressão de tal forma que o código (32, 42) portando informação secundária é distorcido como um resultado da impressão no substrato para tornar o código (32, 42) portando informação secundária não reconstruível a partir da impressão e o código (32, 42) portando informação secundária atribui o elemento de segurança com uma característica predeterminada estatisticamente analisável.

2. Elemento de segurança, de acordo com a reivindicação 1, caracterizado pelo fato de que a característica estatisticamente analisável é fornecida por valores de escala de cinza de porções de uma representação digital da impressão do referido elemento de segurança tomada à luz visível dentro da gama de comprimentos de onda de 380 a 750 nm, as referidas porções sendo selecionadas de acordo com um conceito de codificação predefinido.

3. Elemento de segurança, de acordo com a reivindicação 1 ou 2, caracterizado pelo fato de que o código (20) portando informação primária é escolhido a partir do grupo consistindo de: códigos de barra, códigos QR, códigos de Matriz de Dados, e os códigos de ponto exclusivamente desenvolvidos com codificação não pública.

4. Elemento de segurança, de acordo com a reivindicação 1 ou 2, caracterizado pelo fato de que o substrato de impressão é fornecido com uma ilustração gráfica ornamental e o referido código (20) portando informação primária é escondido na referida ilustração.

5. Elemento de segurança, de acordo com qualquer uma das reivindicações 1 a 4, caracterizado pelo fato de que a informação secundária pode ser derivada a partir da informação primária.

6. Elemento de segurança, de acordo com qualquer uma das reivindicações 1 a 4, caracterizado pelo fato de que o código (32, 42) portando informação secundária é gerado por áreas do código (20) portando informação primária não impressa em cima diretamente.

7. Elemento de segurança, de acordo com qualquer uma das reivindicações 1 a 6, caracterizado pelo fato de que o substrato de impressão é escolhido do grupo consistindo de: notas de banco, títulos, faturas, embalagens de produto, cartões/rótulos de identidade, coberturas, bilhetes de entrada, certificados, documentos pessoais, comprovantes ou quaisquer outros documentos similares ou superfícies de objeto a serem equipadas com proteção de cópia.

8. Material impresso, caracterizado pelo fato de que compreende um substrato de impressão e pelo menos um elemento

de segurança conforme definido em qualquer uma das reivindicações 1 a 7, aplicado sobre o substrato de impressão por impressão.

9. Método para inspecionar autenticidade de material impresso tendo um elemento de segurança conforme definido em qualquer uma das reivindicações 1 a 7, caracterizado pelo fato de que compreende:

gravar uma imagem do código (20) portando informação primária do elemento de segurança sobre iluminação por luz visível na gama de comprimentos de onda de 380 a 750 nm;

converter a imagem obtida em uma imagem de escala de cinza e armazenar a imagem de escala de cinza;

segmentar a imagem de escala de cinza armazenada;

ordenar segmentos da imagem de escala de cinza segmentada em um determinado número de classes baseado no número de pixels que formam uma área deixada para fora dentro de cada segmento;

atribuir um valor médio de escala de cinza como uma característica estatisticamente analisável para cada classe ao submeter as referidas classes uma após a outra à análise estatística;

gerar uma tendência a partir dos valores médios de escala de cinza obtidos mudando de classe para classe;

confirmar autenticidade do referido material impresso quando a referida tendência combina uma tendência predeterminada de aumento nos valores médios de escala de cinza; e

rejeitar autenticidade do referido material impresso quando a referida tendência não combina a tendência predeterminada de valores médios de escala de cinza.

10. Método, de acordo com a reivindicação 9, caracterizado pelo fato de que a referida imagem é gerada por um dispositivo de formação de imagem com uma resolução de 300 a 1200 dpi.

11. Método, de acordo com a reivindicação 9 ou 10, caracterizado pelo fato de que compreende ainda o passo de separar a imagem do código (20) portando informação primária a partir de uma ilustração ornamental se o referido código estiver escondido na ilustração ornamental antes de converter a referida imagem gravada do código na imagem de escala de cinza.

12. Método, de acordo com qualquer uma das reivindicações 9 a 11, caracterizado pelo fato de que a referida análise estatística das classes é realizada por um teste-*t* de duas.

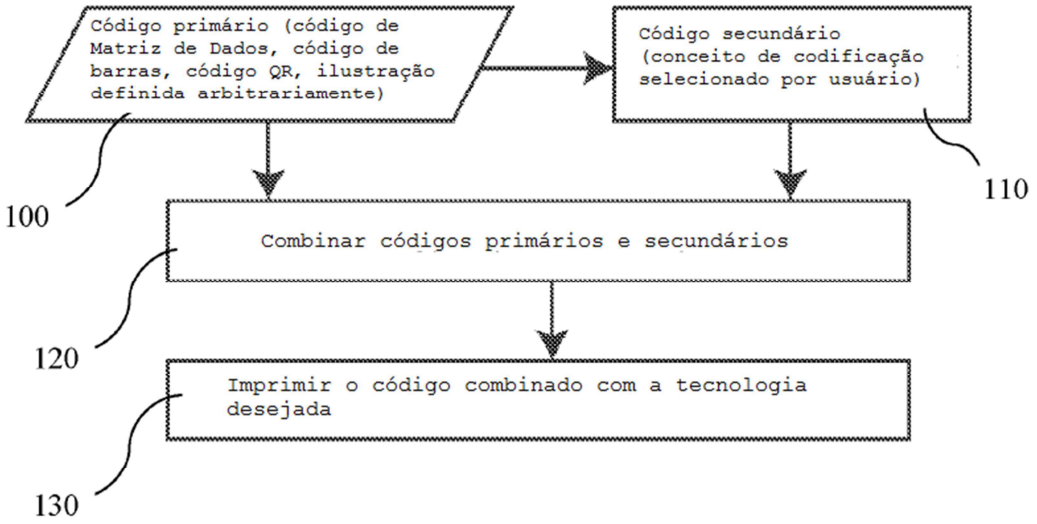

Figura 1A

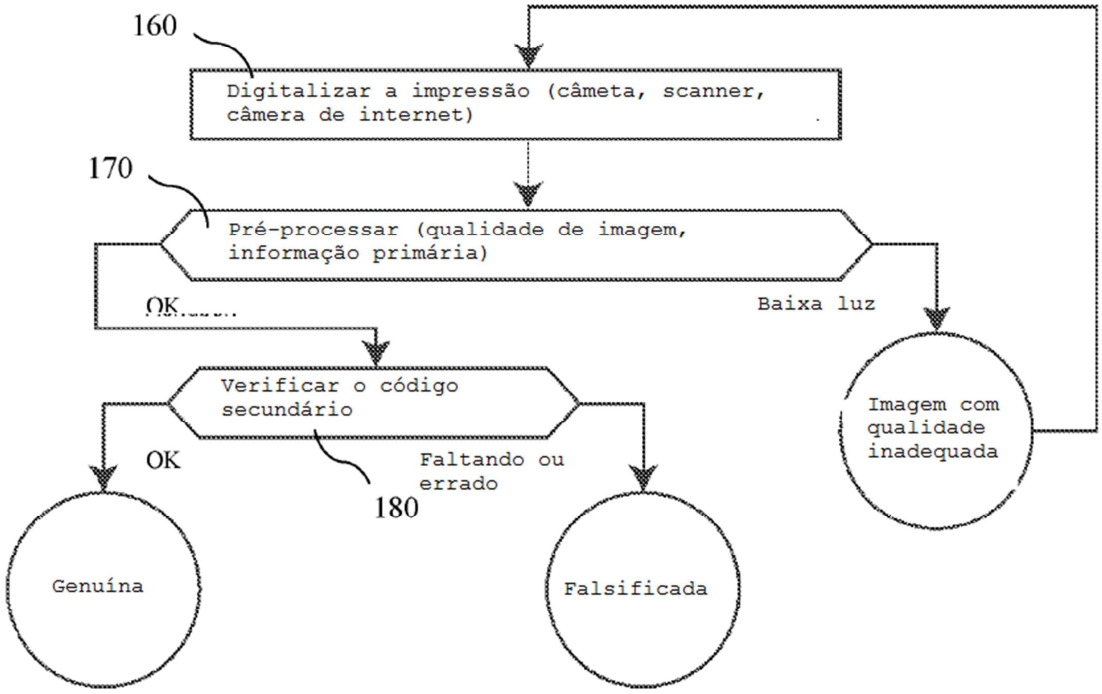

Figura 1B

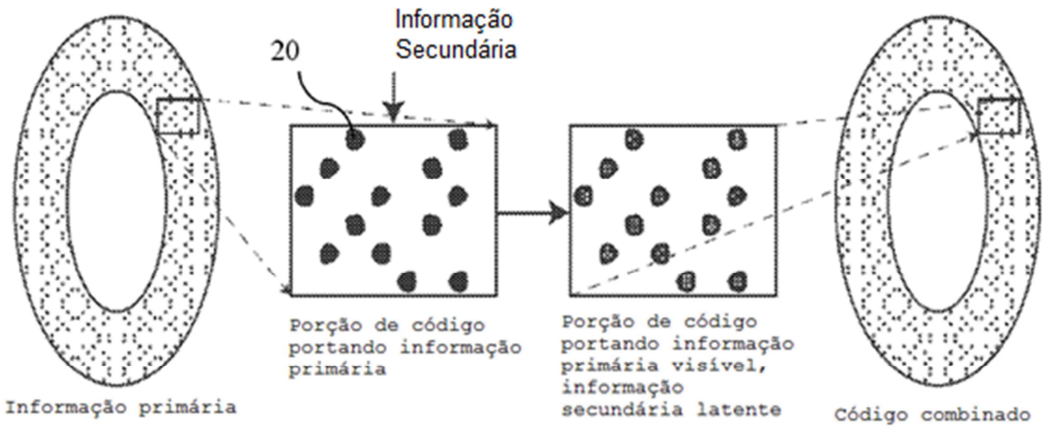

Figura 2

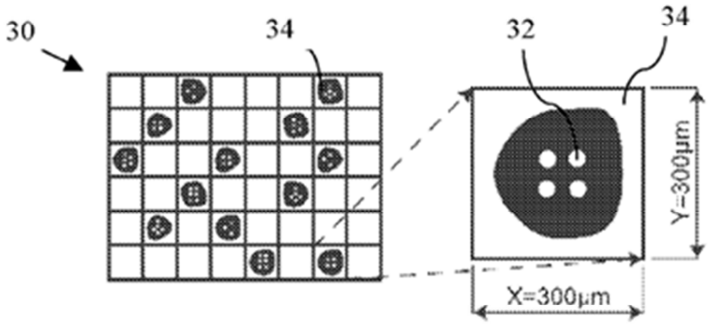

Figura 3

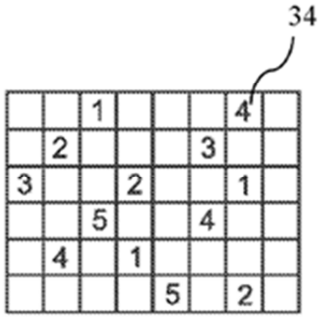

Figura 4

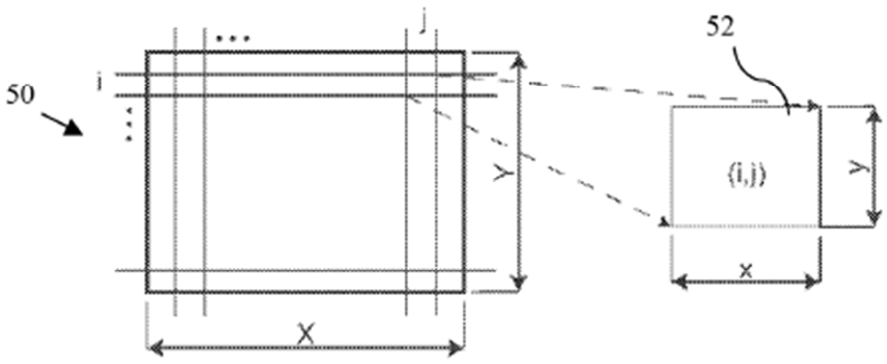

Figura 5

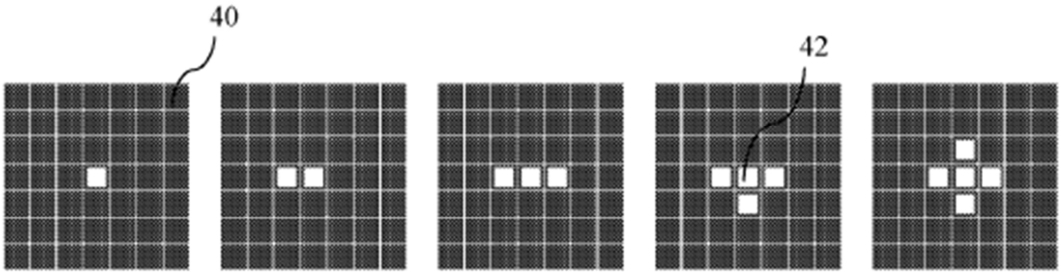

Figura 6

Figura 7

Figura 8

Figura 9A

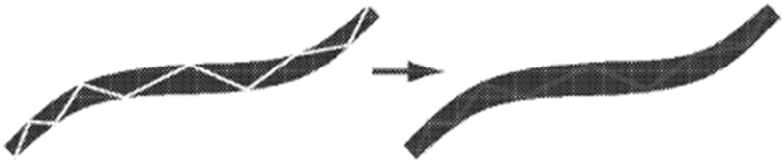

Figura 9B