República Federativa do Brasil
Ministério da Indústria, Comércio Exterior
e Serviços
Instituto Nacional da Propriedade Industrial

(11) **PI 0507408-8 B1**

(22) Data do Depósito: 07/02/2005

(45) Data de Concessão: 20/03/2018

(54) Título: PROCESSOS DE LEITURA E DE PROTEÇÃO DE INFORMAÇÕES SENSÍVEIS, DE CODIFICAÇÃO DE CHAVES ASSIMÉTRICAS E DE AUMENTO DE SEGURANÇA DE INFORMAÇÕES SENSÍVEIS, SUPORTE PORTADOR DE DADOS E DISPOSITIVO ADAPTADO PARA A EXECUÇÃO DO PROCESSO DE LEITURA

(51) Int.Cl.: G06K 19/073

(30) Prioridade Unionista: 06/02/2004 FR 0401171

(73) Titular(es): SIGNOPTIC TECHNOLOGIES

(72) Inventor(es): YANN BOUTANT; DAVID LABELLE; HERVÉ SEUX

“PROCESSOS DE LEITURA E DE PROTEÇÃO DE INFORMAÇÕES SENSÍVEIS, DE CODIFICAÇÃO DE CHAVES ASSIMÉTRICAS E DE AUMENTO DE SEGURANÇA DE INFORMAÇÕES SENSÍVEIS, SUPORTE PORTADOR DE DADOS E DISPOSITIVO ADAPTADO PARA A EXECUÇÃO DO PROCESSO DE LEITURA”

[0001] A presente invenção se refere ao domínio técnico da proteção e da segurança de informações. Em especial, a invenção tem como objeto a utilização de uma ou várias assinaturas digitais de um elemento material de estrutura complexa, caótica, única e estável, para proteger da leitura direta informações sensíveis, um suporte portador de tais informações protegidas e um processo de leitura dessas informações protegidas.

[0002] O advento da era digital trouxe novas possibilidades de desenvolvimento às organizações e aos indivíduos. Se o mundo digital permitiu o acesso muito mais rápido, fácil e pertinente à informação e à comunicação sob todas as suas formas, se ele revolucionou as funções de estocagem e transmissão da informação, é possível considerar também que, intrinsecamente, as plataformas digitais, em geral, em redes, permitem a reprodução, o envio e a captura infinita das informações, e com frequência de maneira incontrolável.

[0003] O mundo digital se encontra assim intrinsecamente inadaptado a preencher funções de autenticação, de proteção/segurança de informações (confidencialidade), de acompanhamento da informação (assinalamento e integridade), etc.

[0004] Partes inteiras de tecnologia foram desenvolvidas a fim de corrigir esses defeitos originais (antivírus, firewall, criptografia, esteganografia, controle de acesso, ...). As respostas se apóiam essencialmente em princípios algorítmicos ou de programação para trazer essas novas dimensões contranaturais ao mundo digital.

[0005] Nesse contexto, a presente invenção tem como objetivo fornecer um novo processo geral de aumento de segurança de informações sensíveis, quer dizer das quais se deseja proteger, controlar o acesso direto ou verificar a integridade, assim como um processo de leitura das informações protegidas obtidas, que apresenta um

grau elevado de segurança. Esse processo apresenta a vantagem de não, geralmente, fazer repousar sua segurança em conjeturas matemáticas e/ou algorítmicas.

[0006] Esse processo tem o dever se ser adaptado à proteção de qualquer tipo de informações notadamente gráficas, digitais, estáticas, dinâmicas, analógicas.

[0007] A invenção também tem como objetivo fornecer um novo meio de gerar ao infinito sequências inteiramente aleatórias.

[0008] Esse novo processo tem o dever de trazer respostas novas, complementares e de alto desempenho em aplicações tão variadas quanto:

- o assinalamento de produtos e atividades com um nível de segurança elevado,

- a gestão documentária, entre as quais a determinação da hora (datação) e a geolocalização (GPS)

- os documentos de segurança, (fiduciária, valor numerário, ID, medicais, patentes,...)

- o aumento de segurança dos dados e das trocas (comunicações),

- as etiquetas embarcadas ou não,

- as embalagens de todas as naturezas (entre as quais as inteligentes e RFID)

- a confidencialidade de documento físico ou informação digital,

- o controle de acesso (a locais, máquinas, atividades, dinheiro e informações) e cartões multifunções

- o voto eletrônico

- os jogos de azar

- a luta contra a contrafação de produtos manufaturados ou de obras intelectuais e artísticas

- a certificação de origem de documento em papel ou eletrônico (assinatura eletrônica),

- o pagamento eletrônico (entre os quais o «e-ticketing» e a franquia postal)

- a proteção de chave(s) de criptografia em protocolos clássicos.

[0009] A invenção tem portanto como objeto a utilização de pelo menos uma assinatura digital obtida a partir de pelo menos uma características estrutural de um elemento material escolhido entre a totalidade ou parte de um material fibroso, plástico, metálico, feito de couro, feito de madeira, compósito, feito de vidro, feito de mineral, feito de estrutura cristalina, para proteger da leitura direta informações sensíveis sob a forma digital, submetendo para isso as informações sensíveis a um tratamento digital que emprega a ou as assinaturas digitais.

[0010] Um outro objeto da invenção é a utilização de elementos materiais escolhidos entre a totalidade ou parte de um material fibroso, plástico, metálico, feito de couro, feito de madeira, compósito, feito de vidro, feito de mineral, feito de estrutura cristalina, para gerar sequências aleatórias ou chaves de codificação aleatórias, sob a forma de assinaturas digitais obtidas a partir de pelo menos uma característica estrutural do elemento material do qual ela é extraída.

[0011] A invenção também tem como objeto um processo de leitura de informações sensíveis protegidas, a leitura sendo realizada submetendo-se as informações sensíveis protegidas sob a forma digital a um tratamento digital que emprega uma ou várias assinaturas digitais de um elemento material obtida(s) a partir de pelo menos uma característica estrutural de um elemento material escolhido entre a totalidade ou parte de um material fibroso, plástico, metálico, feito de couro, feito de madeira, compósito, feito de vidro, feito de mineral, feito de estrutura cristalina.

[0012] A presente invenção também tem como objeto os processos e utilizações tais como descritos nas reivindicações.

[0013] A descrição abaixo, em referência às figuras anexas, permite compreender melhor o objeto da invenção.

[0014] A FIG. 1 representa um esquema geral que inclui um processo de proteção e um processo de leitura de acordo com a invenção.

[0015] A FIG. 2 ilustra variantes de obtenção de assinaturas digitais a partir de diferentes elementos materiais.

[0016] As FIG. 3 e 4 ilustram um exemplo de execução dos processos de proteção e de leitura da invenção e de suporte.

[0017] Os processos e utilizações da invenção utilizam assinaturas digitais obtidas a partir de pelo menos uma característica estrutural de um elemento material, selecionado por suas características estruturais. Em consequência disso, todos os processos e utilizações de acordo com a invenção compreendem uma etapa de obtenção de pelo menos uma assinatura digital a partir de um elemento material, mais precisamente uma etapa de detecção de pelo menos uma característica estrutural do elemento material, a fim de gerar pelo menos uma assinatura digital. O elemento material utilizado apresenta uma estrutura complexa, caótica, única e estável. De acordo com sua significação clássica, uma «assinatura digital» de um elemento material designa uma representação, uma caracterização digital que é própria ao elemento material. De acordo com a invenção, uma assinatura digital é extraída da estrutura do elemento material, ela é obtida a partir de pelo menos uma característica do elemento material que informa sobre sua estrutura. De modo vantajoso, a assinatura digital apresenta um caráter aleatório. Notadamente, as assinaturas digitais podem se apresentar sob a forma de uma imagem digital da estrutura do elemento material, como ilustrado na FIG. 2.

[0018] A presente invenção utiliza o mundo físico, analógico e material que possui, sob múltiplas formas, elementos únicos, em geral resultado de um processo de criação caótico e/ou estocástico. De fato, certos elementos materiais contêm características amplamente caóticas e apresentam uma extrema complexidade estrutural intrínseca, dando uma riqueza informacional considerável a quem sabe lê-la.

[0019] Em geral, os elementos materiais selecionados para executar a invenção reunirão características ao mesmo tempo deterministas e ao mesmo tempo aleatórias. No âmbito da invenção, é especialmente vantajoso extrair dos mesmos do melhor modo possível a parte aleatória. Esses elementos materiais, serão também em geral não copiáveis/não reprodutíveis.

[0020] Além disso, certos elementos materiais têm uma quase invariância

estrutural em um tempo dado, o que permite conservar e utilizar os mesmos durante esse tempo. A presente invenção utiliza elementos materiais dos quais a estrutura é ao mesmo tempo complexa, única, caótica e quase invariante no tempo. Convêm, em geral, no sentido da invenção, os materiais fibrosos, os plásticos, os metais, os couros, as madeiras, os materiais compósitos, o vidro, os minerais, as estruturas cristalinas, que podem ter sofrido modificações ou transformações. Eles podem, por exemplo, ser impressos e/ou gravados e/ou perfurados. Uma combinação de vários materiais pode também servir de elemento material no sentido da invenção. Os materiais fibrosos, à base de fibras sintéticas ou naturais, e em especial a totalidade ou parte de um papel, papelão ou não tecido são preferidos. A invenção recorre portanto, vantajosamente a materiais manufaturados. É possível também considerar que o elemento material faça parte de um papel, papelão ou não tecido, sobre o qual ele é assinalado por um material transparente ao modo de detecção utilizado para extrair a ou as características estruturais, estável no tempo e que assegura sua proteção, por exemplo, um revestimento plástico ou uma resina.

[0021] O elemento material utilizado na presente invenção pode ser pré-existente, ou fabricado, e eventualmente modificado, unicamente para ser empregado no processo de acordo com a invenção.

[0022] De modo preferido, será utilizado o papel como elemento material na origem da ou das assinatura(s) digital(ais) utilizada(s) para assegurar a proteção das informações sensíveis, de acordo com a invenção. De fato, o papel é um material poroso extremamente complexo constituído essencialmente de fibras celulósicas e de cargas minerais. Ele é anisotrópico e heterogêneo. As fibras são orientadas e reunidas em agregados: flocos.

[0023] A instabilidade «natural» do processo físico-químico de fabricação, a variabilidade intrínseca da matéria prima utilizada explicam a forte componente caótica da estrutura do papel. A formação da estrutura desse material se realiza consolidando-se um fluxo de pasta de papel em uma peneira (uma tela de fabricação). Seu fator de formação é apreciável a olho nu em transvisão em luz natural: ele é chamado de «formação de folha ». O papel é geralmente produzido em

tira contínua e é conformado tipicamente em folha. Ele pode ser escrutado de múltiplas maneiras e por exemplo, características estruturais que mostram seu estado de superfície, sua porosidade interna, sua organização em volume da rede fibrosa microscópica ou macroscópica (flocos) em diferentes escalas, podem ser detectadas.

[0024] O papel reúne as propriedades genéricas exigidas para ser utilizado como elemento material gerador de assinaturas digitais aleatórias, a saber a alta complexidade de sua estrutura, aspecto caótico (imprevisível) em diferentes escalas, a unicidade de cada local de um papel, e sua quase invariância no tempo (envelhecimento muito lento em especial de sua estrutura, permitindo conservar papéis durante decênios, e mesmo séculos...).

[0025] Todo o valor da invenção se revela quando é utilizado um elemento material que entre outras propriedades, possui a propriedade da quase invariância. Quer dizer que naturalmente, ele não se modifica ou se modifica pouco no tempo, e que se são medidas certas características estruturais a um momento dado, é-se capaz de encontrar senão intactas, muito similares essas mesmas características a um outro momento ulterior. Ele pode portanto ser qualificado de estável. Essa estabilidade pode ser obtida protegendo-se o elemento material de eventuais agressões exteriores (arranhões, perfurações, deteriorações ópticas,...). Essa proteção pode ser realizada inserindo-se o elemento material de maneira definitiva em um invólucro externo, que não impede em nada o acesso às características interessantes do elemento material. Ela pode também ser realizada conservando-se o elemento material longe de qualquer agressão em atmosfera condicionada e/ou fisicamente protegida, quer dizer em lugar seguro. O tipo de proteção a trazer ao elemento material é função da aplicação escolhida (recurso frequente ao elemento material ou não, sensibilidade da aplicação, ...).

[0026] As assinaturas digitais de um elemento material tal como precedentemente definido, são obtidas como se segue. Seleciona-se um elemento físico no sentido da invenção e extrai-se dele uma ou várias características de sua estrutura quase invariantes no tempo. Vantajosamente, essas características

informam sobre sua estrutura caótica, complexa, única e estável. Em outros termos, uma ou várias características complexas e caóticas da estrutura única do elemento material são extraídas. Essas características vão servir para gerar, depois de digitalização conjuntamente, ou não, com outros tratamentos de tipo conformação/condicionamento e/ou codificação, uma assinatura digital. Essa assinatura digital, que ela própria informa sobre a estrutura caótica, complexa, única e estável do elemento material selecionado, vai, então, ser empregada para assegurar a proteção, o aumento de segurança, de qualquer tipo de informações sensíveis sob a forma digital, quer dizer para impedir a leitura direta das mesmas. Será portanto às vezes necessário digitalizar, previamente, as informações sensíveis a proteger, se elas já não estiverem sob a forma digital. De modo clássico, por digital, entende-se uma representação de informações ou de grandezas físicas sob a forma de qualquer tipo de sinais (entre os quais imagens reais ou complexas, componentes amplitude e/ou fase) de valores discretos, por exemplo sob a forma de algarismos (em qualquer base que seja: binária, decimal, hexadecimal, ...) ou sob a forma de um conjunto qualquer de símbolos (alfabeto, gramática predefinida, ...). Os sistemas digitais recorrem com frequência aos conversores analógico-digital ou digital-analógico.

[0027] A FIG. 1 ilustra de modo geral um processo de proteção e um processo de leitura de acordo com a invenção. O processo compreende as seguintes etapas:

1. Um elemento físico no sentido da invenção é selecionado.

2. A aquisição e a conformação/condicionamento e mesmo a digitalização de uma ou várias características do elemento material é realizada graças a um ou vários sensores com ou sem contato com o elemento material. Esses sensores são classicamente seguidos por uma unidade de tratamento analógica (óptica ou eletrônica por exemplo) ou digital (cartão de aquisição ligado a uma plataforma qualquer informática ou automática).

3. Uma ou várias assinatura(s) digital(ais) são geradas a partir das características extraídas e conformadas/condicionadas na etapa 2. Uma codificação (sob a forma analógica e/ou digital) pode ser realizada seguida ou precedida por

uma digitalização se as características extraídas na etapa 2 já não estiverem sob a forma digital, a natureza desses tratamentos pode variar em função do tipo de elemento material escolhido e da aplicação para a qual o processo é empregado.

4. A ou as assinaturas digitais são associada, de maneira direta (por operações matemáticas elementares) ou indireta (utilizando-se algoritmos sofisticados de codificação e/ou de esteganografia por exemplo), com informações digitais sensíveis, a fim de assegurar a proteção das mesmas.

[0028] A invenção emprega, para a proteção de informação sob a forma digital, um tratamento digital que utiliza pelo menos uma assinatura digital proveniente de um elemento material, o que permite tornar as informações sensíveis originais não diretamente acessíveis, legíveis, audíveis... Em outros termos, compreende-se que as informações sensíveis têm sua segurança aumentada, sua leitura ou compreensão necessitando empregar um processo de leitura ulterior que constitui um outro dos aspectos da invenção.

[0029] De modo opcional, as informações sensíveis na totalidade ou em parte podem estar ligadas fisicamente ao elemento material que foi empregado na etapa 1: elas podem, por exemplo, ser impressas em um documento do qual é proveniente o elemento material.

[0030] As informações com segurança aumentada na etapa 4, são estocadas (etapa 6) em um suporte de dados (digital, óptico, magnético, eletrônico, papel, notadamente, por gravura, impressão, gravação...). A estocagem pode ser uma gravação temporária ou permanente. O elemento material que foi empregado na etapa 1, pode constituir uma parte desse suporte. Por outro lado, de acordo com a etapa 7, a totalidade ou parte das informações protegidas na etapa 4 pode ser transmitida, por intermédio de uma rede de telecomunicações (de fibras ópticas, de ondas de rádio, telefônica, por satélite, ...) ou de um transporte sob a forma material. As informações sensíveis sendo protegidas graças à, ou às assinaturas digitais extraídas do elemento material, elas não podem ser acessíveis ulteriormente a quem não possua o elemento material inicial e os algoritmos de codificação para gerar as assinaturas digitais e/ou as ditas assinaturas digitais e os algoritmos de utilização

dessas últimas. As informações sensíveis, uma vez que elas estão protegidas, são pelo menos parcialmente ilegíveis. O processo de leitura será detalhado na sequência.

[0031] Existem diferentes meios de obter uma assinatura digital de um elemento material. As assinaturas digitais mais adaptadas aos processos e utilizações da invenção apresentam um caráter complexo e aleatório que reflete a estrutura do material do qual elas são extraídas. Essa assinatura é, vantajosamente, obtida por detecção, com o auxílio de um ou vários sensores, de uma ou várias características estruturais quase invariantes no tempo desse elemento que informam sobre sua estrutura complexa, caótica, única e estável, seguida eventualmente por uma conformação/por um condicionamento, por uma digitalização, de uma codificação de acordo com um ou vários algoritmos dessa ou dessas características estruturais. Por algoritmo, entende-se um encadeamento determinado de regras operatórias ou de etapas de tratamentos elementares para obter um resultado a partir de dados ou de sinais iniciais, tais como algoritmos informáticos (sentido digital do termo) (por exemplo) ou operações elementares eletrônicas ou ópticas (sentido analógico do termo).

[0032] Por outro lado, a aquisição da característica estrutural pode ser realizada sob a forma analógica ou digital. Se a aquisição é realizada sob a forma analógica, é possível ou digitalizar e depois codificar sob a forma digital para obter a assinatura digital, ou codificar sob a forma analógica e depois digitalizar, para obter a assinatura digital. A digitalização pode portanto intervir mais cedo, na etapa 2 da FIG. 1 ou então ser a última operação realizada na etapa 3 da FIG. 1. É possível portanto, por exemplo utilizar os encadeamentos seguintes:

a – Sensor / Unidade de tratamento digital (cartão de aquisição ligado à plataforma informática) / Codificador Digital

b - Sensor / Unidade de tratamento analógica (Condicionamento do sinal) / Conversor Analógico-Digital / Codificar Digital

c – Sensor / Unidade de tratamento analógica (conformação / condicionamento do sinal e Codificação) / Conversor analógico-Digital.

[0033] Também é possível utilizar, nas etapas 2 2/ou 3, conversores Analógico/Digital ou Digital/Analógico, a fim de realizar certos tratamentos especiais sem sair do âmbito da invenção, o importante no final da etapa 3 sendo obter assinaturas digitais.

[0034] Por outro lado, de modo vantajoso, a característica estrutural, e portanto a assinatura digital, informam sobre a estrutura interna do elemento material, de modo que a característica estrutural é medida em um volume do suporte e no interior desse último.

[0035] A detecção pode ser feita de acordo com métodos sem contato (ópticos e/ou eletromagnéticos notadamente), nos quais é utilizada a interação (reflexão e/ou absorção e/ou transmissão e/ou difusão e/ou refração e/ou difração e/ou interferência) de uma onda ou radiação eletromagnética com o elemento material, e utilizando-se um sensor óptico/eletrônico para realizar a aquisição, e mesmo a digitalização. O ou os sensores empregados podem então ser colocados em qualquer posição em relação ao elemento material observado, e em relação à, ou às fontes de radiação. Tipicamente, as radiações utilizadas podem ser a luz visível e/ou infravermelha (IR) e/ou ultravioleta (UV) e/ou laser ou raios beta e/ou gama e/ou X. A escolha da ou das radiações e do ou dos sensores utilizados pode ser influenciada pela aplicação do processo, pelo tipo de elemento material selecionado, pela escala de medição escolhida, pelo custo da execução... O ou os sensores utilizados podem ser fixos em relação à fonte e/ou ao elemento material, ou estar em movimento relativo. Também é possível medir a interação entre a onda e o material de acordo com várias orientações.

[0036] De modo vantajoso, os processos e utilizações de acordo com a invenção empregam a assinatura digital de um elemento material, parte de um papel, papelão ou não tecido, obtida depois de detecção de sua interação com a luz visível, por transvisão, notadamente utilizando-se um sensor CCD ou CMOS.

[0037] A detecção pode também ser realizada de acordo com métodos com contato entre o elemento material e o, ou os sensores de medição. Um apalpador é, por exemplo, utilizado como sensor. Esse apalpador pode ou não integrar, além da

dimensão mecânica (acompanhamento da rugosidade de superfície), dimensões eletromagnéticas (comportamento magnético) ou outras. Nesse caso, um movimento relativo do apalpador e do elemento material é necessário.

[0038] Um outro exemplo de sensor com contato consiste em utilizar o elemento material como suporte de uma onda ultrassônica, por exemplo, ou qualquer outra solicitação aplicada (elétrica, térmica, química, biológica,...). Registra-se então, em diferentes orientações, o comportamento/a resposta do elemento material submetido a essa onda ou solicitação.

[0039] A extração de características estruturais do elemento material pode também ser feita a uma ou várias escalas, do nível microscópico ao nível macroscópico, determinando então a complexidade da característica estrutural medida. A complexidade da característica determina aquela da assinatura digital, escolhida no caso de uma proteção por combinação direta, em função do tamanho das informações sensíveis a proteger. Se é retomado o exemplo de um elemento material de tipo papel, é possível escrutar sua estrutura obtida por transvisão, ou a rugosidade de sua superfície, e isso ao nível das fibras (elementos de 100 μm a alguns mm de comprimento e cerca de 10 a 20 μm de largura), ou ao nível dos agregados de fibras (tipicamente da ordem de 1 a 10 mm).

[0040] A superfície de um metal pode ser, ela também, perfeitamente lisa ao olho e se tornar muito rugosa e portanto interessante como elemento material no âmbito dessa invenção quando ela é observada em escala micrométrica ou sub-micrométrica.

[0041] A madeira é um outro exemplo, visto que é possível acompanhar as nervuras do material a olho nu, mas a estrutura íntima desse material só é acessível a partir de uma escala de 10 a 100 μm. A FIG. 2 ilustra assinaturas digitais que podem ser obtidas a partir desses diferentes materiais, em função dos filtros aplicados.

[0042] A detecção, no elemento material, de uma característica estrutural que informa sobre sua estrutura complexa única, pode ser realizada escrutando-se para isso o elemento de acordo com uma linha (1D), de acordo com uma superfície (2D),

ou de acordo com um volume (3D Estereoscopia), de modo que depois de digitalização, a característica estrutural está sob a forma 1D, 2D ou 3D. De modo vantajoso, a(s) assinatura(s) digital(ais) utilizada(s) informa(m) sobre a estrutura interna do material fibroso e serão portanto obtidas por observação das características internas e eventualmente de superfície em um volume desse último. A detecção pode também ser feita independentemente do tempo ou «em tempo real». Nesse último caso, a característica estrutural é amostrada no tempo.

[0043] Do mesmo modo, é possível acrescentar dimensões a essa fase de detecção, observando-se o elemento material sob diferentes orientações ou iluminações, em cor, níveis de cinza, sob a forma binária... A imagem considerada pode também ser uma imagem discreta ou não, real ou complexa (amplitude e fase) no sentido do tratamento e da análise de imagem.

[0044] A ou as assinaturas digitais empregadas no processo da invenção corresponde a uma tal características estrutural digitalizada, submetida eventualmente a uma codificação (antes ou depois de digitalização) de acordo com um ou vários algoritmos. Igualmente, uma tal assinatura digital se apresenta, por exemplo, sob uma forma binária, sob a forma de uma ou várias imagens em cor ou em níveis de cinza, de uma ou várias imagens discretas, reais ou complexas (amplitude e fase).

[0045] Está bem claro que todo o valor da invenção se revela utilizando-se para isso uma ou várias assinaturas digitais que conservam um caráter aleatório e complexo característico da estrutura única e estável do material, apesar do tratamento aplicado às características estruturais utilizadas para gerar a assinatura digital.

[0046] Para gerar a partir das características uma ou várias assinaturas digitais, numerosos métodos podem ser, eles também, considerados, e não é razoável querer citá-los todos. As técnicas dadas abaixo não constituem de nenhuma forma uma lista exaustiva.

[0047] Os métodos conhecidos em tratamento e análise do sinal ou da imagem, da eletrônica ou da óptica são bem naturalmente diretamente mobilizáveis. Os

tratamentos utilizados então se apóiam, sob a forma analógica ou digital, sobre fibras espaciais e/ou frequências (passa-altas, passa-baixas, passa-banda,...), e/ou a transformada de Fourier, e/ou as transformadas ditas por pequenas ondas, e/ou descritores, e mais geralmente, qualquer tipo de algoritmo que permite analisar, e/ou transformar e/ou reorganizar e/ou classificar e/ou limitar os dados brutos (portanto sinais e imagens) extraídos da ou das características estruturais. As operações de convolução/desconvolução, assim como as operações lógicas e aritméticas entre imagens e/ou sinais podem ser empregadas para a obtenção das ditas assinaturas. A título ilustrativo, a transformada de Fourier de um sinal-imagem poderá ser empregada, ou com o auxílio de um algoritmo de transformada de Fourier rápida (“FFT”) se o sinal é de natureza discreta, ou com o auxílio de uma lente de Fourier se o sinale de natureza óptica.

[0048] É possível também aplicar à ou às características estruturais extraídas do elemento material algoritmos mais elaborados, tais como aqueles evocados acima de tal modo que a ou as assinaturas digitais finais se apresentem sob a forma de um sinal, de uma imagem, ou de qualquer tipo de arquivo que seja possível codificar sob a forma alfanumérica ou digital em base decimal, binária, octal, hexadecimal, ou outra.

[0049] A fase de proteção pode empregar uma ou várias assinaturas digitais provenientes de um mesmo elemento material ou de vários elementos materiais.

[0050] A fase de proteção das informações sensíveis sob a forma digital, com o auxílio da ou das assinaturas digitais assim geradas, pode ser realizada, como explicado precedentemente, de maneira direta por operações matemáticas elementares, ou indireta recorrendo-se a algoritmos elaborados existentes, por exemplo de criptografia e/ou esteganografia, com ou sem compressão de dados previamente.

[0051] Na via direta, a proteção das informações sensíveis sob a forma digital é realizada por combinação com pelo menos uma assinatura digital de um elemento material, que torna pelo menos parcialmente ilegíveis, ao mesmo tempo as informações sensíveis sob a forma digital e a assinatura digital.

[0052] A título de exemplo, é possível citar a combinação de uma assinatura digital que se apresenta sob a forma binária (sequência de “0” e de “1” imagem da estrutura caótica do elemento material), com as informações sensíveis sob a forma digital codificadas elas também sob a forma binária, efetuando-se uma operação lógica (XOR (adição módulo 2) por exemplo) entre as duas sequências binárias bit a bit. As duas sequências binárias sendo idealmente de mesmo tamanho. A assinatura digital e as informações digitais a proteger podem também ser combinadas somando-se, octeto por octeto, as duas cadeias digitais. Aqui ainda, um grande número de combinações são possíveis permanecendo-se no âmbito da invenção. A combinação pode ser realizada, a partir da forma binária, hexadecimal, ASCII ou alfabética, das informações sensíveis sob a forma digital e da ou das assinaturas digitais do elemento material, por aplicação conjuntamente ou não dos princípios de permutação, transposição, substituição, iteração, máscara (operadores lógicos XOR, adição, subtração, bit a bit (em cadeia), ou bloco a bloco...) ou propriedades matemáticas de álgebra modular (módulo n), de teoria dos números.

[0053] Uma forma mais elaborada de combinação utiliza o princípio de máscara descartável (“One Time Pad”). A assinatura digital utilizada é uma sequência perfeitamente aleatória, do mesmo tamanho que as informações sensíveis sob a forma digital (em número de bits, por exemplo) e só serve de máscara uma só vez. Por extensão, é possível também considerar utilizar uma assinatura digital de tamanho superior ou igual àquele das informações sensíveis. Deve ser notado, além disso, que é possível combinar qualquer tipo de informação sensível, qualquer que seja seu tamanho, visto a reserva quase inesgotável que os elementos materiais elegíveis constituem.

[0054] A proteção de somente uma parte das informações sensíveis pode ser absolutamente considerada, basta selecionar, no seio das informações digitais, as zonas a combinar com a assinatura digital.

[0055] A via indireta de aumento de segurança da informação digital emprega a ou as assinaturas digitais do elemento material e dos algoritmos de criptografia (de chave privada e/ou de chave pública) e/ou esteganografia. As assinaturas digitais

desempenham o papel de chaves de codificação, de esteganografia, palavra de senha, frase de senha, arquivo de senha, grão aleatório, chaves de codificação aleatórias, ou podem simplesmente ser empregadas como «invólucro digital» de uma informação digital comprimida, codificada e/ou esteganografiada. Tem-se então um processo de proteção mais complexo: as informações sensíveis podem ser protegidas de acordo com métodos conhecidos (combinação, algoritmo de criptografia), e depois submetidas ao processo de proteção de acordo com a invenção ou inversamente. Quando a proteção de acordo com a invenção intervém na etapa final, é possível considerar que a assinatura digital desempenha o papel de invólucro digital.

[0056] Se as aplicações com chave(s) secreta(s) são naturalmente exploráveis com o processo da presente invenção, é possível em uma versão mais elaborada da invenção utilizar protocolos existentes de chaves assimétricas (pública/privada) utilizando-se para isso uma ou várias assinaturas digitais extraídas do elemento material como chaves de criptografia. A título de exemplo, é possível extrair do elemento material dois grandes números primos (extração intrinsecamente aleatória mas fixada no elemento material portanto reprodutível para quem possui a chave física) que servirão para executar um processo de tipo RSA (Rivest-Shamir-Adleman), ou utilizar por exemplo uma extração aleatória extraída do elemento material em um protocolo criptográfico qualquer. É possível assim mais geralmente a partir de um elemento material pertinente no sentido da invenção extrair uma chave pública e uma chave privada, a chave pública sendo por exemplo transmitida a um destinatário, a chave privada permanecendo por exemplo sob a forma física no elemento material, e sendo chamada unicamente temporariamente quando é preciso decifrar uma mensagem cifrada com a chave pública. É possível também extrair uma chave (privada por exemplo) de um elemento material pertinente no sentido da invenção e utilizar uma outra chave (pública por exemplo) gerada por qualquer outro meio. Outras adaptações da invenção a processos ou protocolos criptográficos existentes podem ser naturalmente consideradas. Em especial é possível facilmente assegurar as funções de autenticação, de certificação, de identificação, de não

repúdio, de confidencialidade, de controle de integridade, de prova de divulgação nula, de assinatura, de troca de chaves, de datação, de geração, depósito e gestão de chaves, etc... hoje cobertas pelos ditos protocolos existentes.

[0057] Que seja utilizada a via direta, ou indireta de proteção descrita acima, é possível submeter a montante, quer dizer antes da utilização da combinação ou do algoritmo de codificação e/ou esteganografia, a assinatura e as informações digitais a um algoritmo de compressão dos dados, ou a qualquer outro tratamento.

[0058] A proteção por via direta e a proteção por via indireta permitem ambas, se for necessário, só proteger uma parte das informações sensíveis, e colocar no lugar vários níveis de acesso às informações sensíveis originais. Também se revela interessante que a proteção empregue várias assinaturas digitais provenientes de um mesmo ou de diferentes materiais, permitindo ulteriormente dar acessos de leitura distintos às informações sensíveis, e notadamente somente a certas partes dessas informações sensíveis. A utilização de várias assinaturas digitais sucessivamente e/ou de maneira sequencial permite um aumento de segurança da informação digital a múltiplos níveis de acesso. As assinaturas digitais são em seguida geradas na fase de leitura ulterior, em função do nível de autorização de acesso do operador.

[0059] Um dispositivo adaptado para a execução da proteção de informações sensíveis, utilizável no âmbito da invenção, compreende meios para assinalar um elemento material selecionado e detectar nesse último, uma ou várias de suas características estruturais, em especial informando sobre sua natureza complexa, caótica, única e estável, ligados a uma unidade de estocagem e de tratamento que assegura:

a1) a aquisição, a conformação/o condicionamento, a digitalização e eventualmente a codificação de acordo com um ou vários algoritmos da ou das características estruturais detectadas para gerar um (ou várias) assinatura(s) digital(ais), que informam vantajosamente sobre o caráter complexo, caótico, único e estável da estrutura do elemento material,

b1) a associação da (ou das) assinatura(s) digital(ais) gerada(s) a

informações sensíveis sob a forma digital para assegurar a proteção das mesmas, gerando assim informações sensíveis protegidas.

[0060] Um sensor óptico será, de preferência, utilizado para a detecção. O dispositivo pode ser ligado a meios de transmissão à distância das informações sensíveis protegidas (mesmo em um canal não seguro tal como a Internet) e/ou da assinatura digital e/ou das características estruturais.

[0061] Um aspecto importante da presente invenção é que ela é aplicável, tanto a informações de tamanho definido e invariável no tempo, quanto a informações «tempo real» de tipo sinal digital que varia no tempo. Se o primeiro modo de aplicação é facilmente perceptível, visto que se combina uma porção delimitada e invariável de informações (assinatura digital) proveniente de um elemento material com uma porção de informações digitais a proteger, ela também delimitada e invariante, o segundo modo de aplicação merece mais precisões.

[0062] No caso em que o processo de acordo com a invenção é executado para proteger informações sensíveis dinâmicas, tais como uma seqüência sonora e/ou de vídeo, é necessário utilizar uma assinatura digital «dinâmica». A assinatura digital «dinâmica» pode ser obtida por repetição de uma assinatura digital estática ou por detecção repetida, com o auxílio de um ou vários sensores, de uma ou várias características estruturais de um elemento material estático que informa sobre sua estrutura complexa única.

[0063] Uma outra variante consiste em obter uma assinatura digital «dinâmica» por detecção de modo contínuo, com o auxílio de um ou vários sensores, de uma ou várias características estruturais de um elemento material em movimento relativo em relação ao(s) sensor(es). O elemento material «desfila» diante do ou dos sensores, de maneira sincrônica ou não com o sinal digital a aumentar a segurança. O deslocamento relativo do elemento material e do ou dos sensores pode também ser obtido com o movimento somente do ou dos sensores ou o movimento combinado do(s) sensor(es) e do elemento material, em direções e/ou em velocidades diferentes. Nessa última variante, o elemento material é, por exemplo, uma bobina de papel, papelão ou não tecido, em deslocamento, ou papel em decorrer de

fabricação em máquina de papel. Pode ser mesmo considerado combinar instantaneamente, o sinal digital a proteger com as assinaturas «dinâmicas» obtidas.

[0064] Em todo processo de proteção/aumento de segurança de informações, é preciso em seguida ser capaz de ler as informações que foram protegidas. O termo «ler» deve ser interpretado no sentido amplo, ele inclui qualquer tipo de decodificação, decifração..., tornando as informações sensíveis originais, pelo menos em parte, acessíveis, compreensíveis, legíveis.

[0065] A presente invenção tem portanto como objeto um processo de aumento de segurança de informações sensíveis que compreende:

a) uma etapa de proteção tal como definida acima, que leva a informações sensíveis sob a forma segura,

b) uma etapa de leitura das informações seguras obtidas na etapa a), que permite reencontrar as informações sensíveis.

[0066] Em geral, entre a etapa de proteção e a etapa de leitura, o processo de aumento de segurança compreende uma etapa de registro das informações seguras em um suporte de dados.

[0067] A etapa de leitura vai agora ser descrita.

[0068] Igualmente, a presente invenção tem também como objeto um processo de leitura de informações protegidas no qual, a leitura das informações protegidas é realizada sob a forma digital, por aplicação de um tratamento digital, que emprega pelo menos uma assinatura digital obtida a partir de pelo menos uma característica estrutural de um elemento material escolhido entre a totalidade ou parte de um material fibroso, plástico, metálico, feito de couro, feito de madeira, compósito, feito de vidro, feito de minério, feito de estrutura cristalina.

[0069] Tudo o que foi dito precedentemente na parte relativa à proteção das informações sensíveis, em especial, no que diz respeito à escolha do elemento material, à obtenção das características estruturais, das assinaturas digitais, se aplica à leitura.

[0070] De modo esquemático, a leitura das informações protegidas vai ser efetuada graças a um tratamento digital que corresponde sensivelmente ao

tratamento digital inverso daquele utilizado para a proteção das mesmas, utilizando-se para isso uma ou várias assinaturas digitais do elemento material que serviram para sua proteção, como chave(s) de leitura.

[0071] Um dos problemas é conservar e transmitir as informações necessárias a essa leitura. Essas informações incluem, naturalmente, a ou as assinaturas digitais que serviram para a proteção das informações sensíveis. A conservação pode ser feita em vários níveis. Primeiramente, é possível registrar, sob a forma digital por exemplo, ou a ou as características estruturais que serviram para gera a (ou as) assinatura(s) digital(ais), ou a (ou as) própria(s) assinatura(s) digital(ais). Nesse caso, há desmaterialização do elemento material que não precisa mais ser conservado e pode ser destruído. É no entanto necessário gerir perfeitamente a segurança dos dados digitais conservados. Nesse caso, a(s) assinatura(s) digital(ais) utilizada(s) para a leitura correspondem exatamente àquela(s) utilizada(s) para a proteção.

[0072] Em seguida, é também possível conservar o elemento material que serviu para gerar a assinatura digital, o que implica determinar e proteger o elemento material para sua reutilização posterior. Nesse último caso, será preciso ser capaz geralmente de reproduzir todas as etapas executadas para obter a assinatura digital utilizada para a proteção. Quer dizer que é preciso:

- retomar o elemento material que serviu para aumentar a segurança das informações sensíveis. Esse elemento material terá podido ser indexado a essas últimas, através de uma base de dados, ou então ser ligado a uma parte das informações sensíveis originais (impressão de um código por exemplo),

- extrair, adquirir uma ou várias características estruturais desse elemento material através de um ou vários sensores com ou sem contato com o elemento material, seguido(s) em geral de uma unidade de tratamento analógica (óptica ou eletrônica por exemplo) ou digital (cartão de aquisição ligado a uma plataforma qualquer informática ou automática). Uma ou várias assinatura(s) digital(ais) são assim geradas, eventualmente depois de codificação das características estruturais, por aplicação de um ou vários algoritmos, cuja natureza pode variar em função do

tipo de elemento material escolhido e da aplicação visada.

[0073] As etapas de execução no processo de leitura utilizam, de preferência, as mesmas condições operatórias que aquelas empregadas no processo de proteção das informações. A capacidade de reencontrar ou de reproduzir perfeitamente uma ou várias assinaturas digitais dadas a partir de um elemento material é geralmente indispensável, para bem executar o processo de leitura. O fator de escala, a sensibilidade do sensor (filtragem), o posicionamento do elemento... são parâmetros que devem ser bem levados em consideração por ocasião da seleção da características estrutural a detectar no elemento material. É entretanto possível considerar recorrer a chaves de controle ou a códigos corretores de erros, mais geralmente técnicas de detecção e de correção de erros, que permitem corrigir erros de leitura. É possível também autorizar a recuperação das informações sensíveis digitais originais de acordo com o êxito em um teste de dependência estatística entre a ou as assinaturas digitais extraídas no momento da leitura e aquelas que serviram para o aumento de segurança, por exemplo estocadas em uma base de dados. Em consequência disso, no caso em que por ocasião da leitura, as assinaturas digitais são reencontradas a partir do elemento material, essas últimas poderão ser ligeiramente diferentes daquelas utilizadas para a proteção e portanto ser submetidas a chaves de controle, de códigos corretores de erros, ou a um teste de dependência estatística.

[0074] É possível ainda utilizar outros meios que permitem recuperar a informação digital original, apesar de uma reprodução imperfeita da assinatura digital do elemento material por ocasião da fase de leitura. Por exemplo, a introdução de redundância nas informações sensíveis originais antes da fase de proteção das informações pelo processo objeto da invenção, dá a solidez ao processo de leitura.

[0075] Deve ser notado, além disso, que em certos casos, é mesmo possível utilizar uma ou várias assinaturas digitais ligeiramente diferentes daquelas que serviram para a proteção dos dados originais mas que provêm do mesmo elemento material original, e apesar de tudo reencontrar senão intactas as informações originais, pelo menos seu significado. Por exemplo, uma foto de identidade

ligeiramente embaçada ou com defeitos menores não impede em nada que se reconheça a pessoa...

[0076] No que diz respeito ao transporte das informações necessárias para a leitura, que incluem notadamente o elemento material, a característica estrutural sob a forma digital ou a assinatura digital, a invenção também apresenta um interesse especial: o elemento gerador da assinatura digital é de origem física e pode ser transportado fisicamente por um canal totalmente distinto dos canais digitais. Se há um acordo sobre um outro segredo (algoritmos de gerações de assinaturas digitais, números de assinaturas digitais úteis em um conjunto maior, ordem de utilização dessas chaves,...), as informações digitais podem ser transmitidas diretamente, e mesmo ser elas mesmas protegidas por uma outra variante da invenção, por ocasião de sua transmissão.

[0077] Antes da execução do processo de proteção, o operador tem em sua posse informações sensíveis sob a forma digital a tornar seguras e um elemento material. Depois de sua execução, o operador tem em sua posse as informações sensíveis seguras registradas em um suporte de dados, o elemento material e as informações sensíveis originais. Essas últimas podem ser, ou estocadas em segurança para verificar posteriormente a integridade das informações seguras, por exemplo, ou destruídas. Só resta, então, o elemento material e o suporte portador das informações sensíveis seguras. As informações sensíveis seguras só poderão ser lidas por aquele que possuirá o elemento material e o conhecimento detalhado dos meios de execução para gerar a assinatura digital, e depois assegurar a proteção das informações. A segurança do sistema é duplamente assegurada pela segurança de conservação do elemento material, e a segurança do segredo dos detalhes do processo. Quando uma informação digital foi tornada segura a partir da análise da textura de um papel, e que somente uma zona ou zonas bem definidas desse papel constituem o elemento material, então a segurança do processo está assegurada pela preservação do papel e pelo conhecimento das zonas ativas desse elemento material. Esse exemplo ilustra a força desse gênero de proteção da informação digital, que permite conservar por um lado o elemento material que foi

empregado (sem por outro lado ter que revelar a natureza do mesmo) e poder, em toda segurança, transmitir ou estocar a informação segura. Uma parte do sistema é conservada materialmente, uma parte é imaterial e digital.

[0078] Naturalmente, uma alternativa mencionada precedentemente é a de conservar não o elemento material mas sim sua assinatura digital ou as características, sob a forma digital por exemplo, informando sobre sua estrutura complexa, caótica, única e estável. Essa últimas são então salvaguardadas de maneira durável e segura e poderão ser utilizadas diretamente para a leitura, o elemento material original podendo eventualmente ser destruído. O interesse aqui é obter o aumento de segurança se apoiando para isso nas propriedades estruturais complexas, caóticas e únicas do elemento material, e conservando imagens digitais dessas últimas (desmaterializadas) para facilitar a execução da fase de leitura. A segurança de estocagem das características digitalizadas e/ou das assinaturas digitais é então crítica. Elas podem bem evidentemente ser tornadas seguras por todos os meios clássicos do tipo criptografia, esteganografia, chave material USB (Universal Serial Bus) cartão com chip ou outro.

[0079] O processo de leitura de acordo com a invenção é aplicado nas informações protegidas sob a forma digital, às quais é feito um tratamento digital inverso àquele utilizado para sua proteção. Ele deve, na maior parte das vezes, reproduzir ao inverso o algoritmo, tratamento, ou combinação utilizada para a proteção, a assinatura utilizada para a proteção desempenhando então o papel de chave de leitura, no sentido amplo do termo, de modo que as informações sensíveis originais se tornem de novo pelo menos parcialmente legíveis. A título de exemplo, será utilizado um algoritmo de reconstrução, um ou vários algoritmos de decifração inverso daqueles empregados para a proteção, a ou as assinaturas digitais servindo de chaves de decifração.

[0080] No caso em que a fase de leitura utiliza o elemento material para reencontrar a assinatura digital necessária, será utilizado um dispositivo que compreende meios para assinalar um elemento material selecionado e detectar nesse último, uma ou várias de suas características estruturais, em especial

informando sobre sua estrutura complexa, caótica, única e estável, ligados a uma unidade de estocagem e de tratamento que assegura:

a2) a aquisição, a conformação/o condicionamento, a digitalização e eventualmente a codificação de acordo com um ou vários algoritmos da ou das características estruturais detectadas para gerar um (ou várias) assinatura(s) digital(ais), que informam vantajosamente sobre o caráter complexo, caótico, único e estável da estrutura do elemento material,

b2) a leitura das informações sensíveis protegidas por execução de um tratamento digital que utiliza a ou as assinaturas digitais geradas na etapa a2, como chave(s) de leitura, e que corresponde vantajosamente ao tratamento digital sensivelmente inverso àquele utilizado para a associação da (ou das) assinatura(s) digital(ais) às informações sensíveis originais, por ocasião da proteção das mesmas.

[0081] Em especial, a unidade de estocagem e de tratamento assegura:

a2) a digitalização e eventualmente a codificação de acordo com um ou vários algoritmos da ou das características estruturais detectadas para gerar uma (ou várias) assinatura(s) digital(ais),

b2) a leitura das informações sensíveis protegidas por execução de um tratamento digital que utiliza a ou as assinaturas digitais geradas na etapa a2, como chave(s) de leitura, e que corresponde ao tratamento digital sensivelmente inverso àquele utilizado para a associação da (ou das) assinatura(s) digital(ais) às informações sensíveis originais, por ocasião da proteção das mesmas.

[0082] Compreende-se bem que o processo de proteção e o processo de leitura podem ser executados por um mesmo dispositivo.

[0083] A proteção de acordo com a invenção é, por exemplo, utilizada para proteger informações sensíveis digitais (telecomunicações, música, vídeo, multimídia,...), tendo em vista o transporte das mesmas em redes pouco seguras e/ou tendo em vista controlar/garantir a utilização ulterior das mesmas. Nesse gênero de aplicações, a desmaterialização do elemento material como chave de segurança aumentada pode ter todo seu interesse. De fato, se é desejado realizar um aumento de segurança de um sinal digital a fim de transportá-lo em redes pouco

seguras e/ou controlar o mesmo e/ou garantir sua utilização ulterior, e além disso que essa fase de leitura deva ocorrer geograficamente e/ou em um prazo que torna impossível o transporte do elemento material, é possível imaginar, por exemplo, emitir simultaneamente ou ligeiramente em defasagem o sinal digital tornado seguro e as características estruturais digitalizadas do elemento material e/ou as assinaturas digitais associadas. A segurança da operação é, então, assegurada pelo aspecto algorítmico a empregar no processo de leitura e pela natureza intrinsecamente caótica, portanto imprevisível, do elemento material que é encontrada em suas características estruturais digitalizadas e/ou nas assinaturas digitais associadas. Também é possível imaginar dois tipos distintos de canais de transmissão do sinal digital tornado seguro por um lado, e das características digitalizadas do elemento material e/ou das assinaturas digitais associadas por outro lado.

[0084] O suporte de dados sobre o qual as informações protegidas podem ser estocadas constitui também um aspecto importante. Esse suporte vai também servir na maior parte das vezes para a transmissão ou para o transporte ulterior das informações protegidas. A estocagem pode intervir de modo permanente ou temporário. Esse suporte é portador das informações protegidas: essas informações podem ser impressas em um suporte físico, feito de papel, por exemplo, ou registradas em um suporte eletrônico, magnético, óptico. Naturalmente, o suporte pode ser portador de outras informações. A título de exemplos ilustrativos, as informações digitais protegidas de acordo com o processo da invenção podem ser registradas sobre disco rígido magnético, fita magnética, sob a forma óptica, memória holográfica, gravadas em um CD ou DVD, em uma chave USB, memória flash ou outra, sob a forma eletrônica em um cartão com chip, mas também sob a forma impressa ou gravada em um material ou documento. As informações tornadas seguras podem também ser estocadas sob a forma de uma base de dados, facilmente consultável, ou diretamente, ou por uma rede de telecomunicações (Internet por exemplo).

[0085] A informação tornada segura pode portanto ser transmitida e recebida

pela via de uma rede de telecomunicações ou por um transporte sob a forma material.

[0086] A suporte pode além disso integrar meios de transmissão da informação ou integrar um ou múltiplos elementos empregados em uma transmissão de informação, em especial elementos sensíveis às radiofrequências (antenas ativas ou passivas por exemplo) empregados em uma transmissão sem contato e à distância de informação. De acordo com uma variante de realização, o suporte é um documento em papel, um papelão ou um não tecido. Pode se tratar em especial de um papel dito de segurança (nota de dinheiro, cheque, ato autêntico, distribuidor automático de bilhetes,...) que reúne a totalidade ou parte das seguintes seguranças: elementos embarcados (fios de segurança, pequenas pranchas,...) filigranas, hologramas, micro perfurações, micro impressões, diferentes tipos de impressão, reagentes químicos anti-contrafação,...

[0087] Esse suporte pode se apresentar sob a forma de um documento em papel ou papelão ou não tecido, do qual a totalidade ou parte corresponde ao elemento material do qual é proveniente a ou as assinatura(s) digital(ais) que serviram para a proteção das informações sensíveis, em parte ou totalmente protegido por um invólucro transparente externo (por exemplo plastificação ou revestimento ou extrusão ou outro) de um outro material que desempenha um papel protetor contra as agressões exteriores normais de utilização mas também que impede a separação do documento e de seu invólucro sem destruição do primeiro. Um tratamento de superfície com uma resina transparente pode também assegurar a proteção do mesmo.

[0088] As informações sensíveis protegidas são portanto registradas sobre esse suporte, por exemplo por impressão. De acordo com uma variante, as informações sensíveis protegidas aparecerão sob a forma de um código de barras.

[0089] Esse suporte pode também se apresentar sob a forma de papel, papelão ondulado ou plano ou não tecido por exemplo transformado em invólucro, em papelão de embalagem, em etiqueta, em vestuário descartável,...

[0090] Certas formas possíveis de suporte de informações tornadas seguras

acima listadas, podem além disso integrar intimamente a totalidade ou parte do elemento material que serviu para a proteção das informações sensíveis e/ou a totalidade ou parte das informações sensíveis originais sob qualquer forma que seja, impressas ou estocadas sob a forma digital. O elemento material será de preferência localizado e protegido.

[0091] Nas aplicações cartões com chip e/ou com tira magnética, isso é especialmente interessante visto que se coloca «inteligência» no suporte e se junta de maneira biunívoca o elemento material/suporte e as informações tornadas seguras. As informações originais só são então acessíveis ao possuidor do elemento material. Esse acoplamento das informações originais e do elemento material permite além disso uma verificação implícita da autenticidade do cartão. As informações sensíveis digitais presente em claro no suporte permitem também verificar a integridade dessas informações e/ou das informações tornadas seguras por simples comparação.

[0092] O suporte físico pode, de maneira análoga, integrar intimamente a totalidade ou parte do elemento material que serviu para a execução da proteção e/ou a totalidade ou parte da ou das características estruturais extraídas do elemento material sob qualquer forma que seja, e/ou a totalidade ou parte da ou das assinaturas digitais do elemento material sob qualquer forma que seja. No entanto, ele integra pelo menos uma assinatura digital obtida a partir de uma característica quase invariante de um elemento material que informa sobre sua estrutura complexa única, de preferência, sob a forma codificada.

[0093] A título de outros exemplos de suporte, dos quais é possível verificar a autenticidade, podem ser citados:

- um cartão feito de papel sobre o qual são impressos, por um lado, as informações sensíveis originais, por outro lado, as informações sensíveis protegidas e do qual uma parte corresponde ao elemento material papel que serviu para gerar a assinatura eletrônica, esse elemento sendo protegido e localizado por um filme plástico,

- um suporte de papel do qual uma parte corresponde ao elemento

material, preso no seio de um CD no qual são gravadas, as informações protegidas graças a uma assinatura digital gerada com o elemento material papel.

[0094] Em consequência disso, se o processo de leitura autoriza a leitura com êxito das informações sensíveis, ele valida também o caráter autêntico da ou das assinaturas digitais utilizadas, e/ou do elemento material do qual elas são provenientes, e/ou do suporte portador das informações sensíveis protegidas.

[0095] Além disso, uma etapa suplementar, no processo de leitura, que compara as informações lidas com as informações sensíveis conhecidas pelo usuário permite validar o caráter autêntico da ou das assinaturas digitais empregadas, do elemento material do qual elas são provenientes e das informações sensíveis. Esse aspecto é especialmente vantajoso, quando o suporte serve para a realização de documentos de identidade, de cartão de acesso...

[0096] Os processos de proteção e de leitura de acordo com a invenção podem, naturalmente, ser integrados a montante ou a jusante de um processo aplicativo mais geral. Em especial, eles poderão ser utilizados, sozinhos ou em combinação, com outros processos, para o assinalamento de produtos e serviços, a gestão documentária, a fabricação de documentos de segurança, de atos autênticos, de etiquetas embarcadas ou não, a confidencialidade de correio físico ou eletrônico, a certificação de origem de documento em papel ou eletrônico, o pagamento eletrônico, a assinatura eletrônica, para gerar códigos de barras, carta recomendada com aviso de recebimento, acompanhamento de correio ou de pacotes, envelopes, tatuagem digital,...

[0097] As FIGs 3 e 4 ilustram um exemplo de execução dos processos de proteção e de leitura de acordo com a invenção. Nesse exemplo, o elemento material considerado é um cartão feito de papel/papelão, e mesmo um cartão plástico que integra um elemento material papel/papelão, do qual a estrutura caótica do material é acessível por transvisão.

[0098] A fase de escrita ilustrada na FIG. 3 emprega o processo de proteção de acordo com a invenção, a partir de um conjunto de cartões originais virgens, que integram cada um deles um elemento material gerador de uma assinatura digital, do

tipo acima descrito, arquivos digitais que contêm dois tipos de informação (nível 1 que será impresso em um cartão e nível 2 que será tornado seguro com o nível 1 por exemplo), um PC com cartão de aquisição, uma impressora munida de um módulo de leitura óptica das características que informam sobre a estrutura complexa única do elemento material, ou em uma outra configuração um módulo de leitura óptica dissociado da impressora. As informações digitais (nível 1 e nível 2) que serão ligadas aos cartões podem ser em parte similares. No momento da passagem de um cartão na impressora ou no módulo externo de leitura óptica, é impressa nele uma informação de nível 1, e extrai-se a ou as características estruturais sob a forma digital do elemento material presente, gera-se as assinaturas digitais associadas, que são estocadas temporariamente no PC, a fim de realizar uma combinação (direta ou indireta) da informação digital (nível 1 e nível 2) com as ditas assinaturas. No final da fase de escrita, os cartões são impressos com uma parte da informação tornada segura sob a forma inteligível, e arquivos que contêm as informações digitais (nível 1 e nível 2) codificadas com as assinaturas digitais extraídas dos elementos materiais sucessivos, são estocados de maneira durável em uma base de dados de referência (com ou sem índice cartão/arquivo tornado seguro). Esses arquivos codificados poderão ser transmitidos por ligação local ou rede de telecomunicação.

[0099] A fase de leitura ilustrada na FIG. 4 emprega, no que lhe diz respeito, o processo de leitura de acordo com a invenção. O jogo de cartões originais impressos, obtidos na fase de escrita é analisado por passagem em um leitor óptico, um cartão de aquisição e um PC, as assinaturas digitais são geradas e estocadas de maneira temporária na memória do PC, a fim de poder experimentar as ditas assinaturas nos arquivos tornados seguros presentes na base de dados de referência. Se o cartão testado permite o acesso às informações digitais de nível 1 e de nível 2 contidas em um arquivo codificado, tem-se então várias informações conjuntamente: por um lado que o cartão (chave) é autêntico, por outro lado, comparando-se a informação de nível 1 compreendida no arquivo codificado e a informação de nível 1 impressa no cartão, que se há identidade então o arquivo

codificado e/ou a informação presente no cartão são íntegras, quer dizer que eles não foram modificados depois da criação do cartão.

REIVINDICAÇÕES

1. Processo de leitura de informações sensíveis protegidas caracterizado pelo fato de que a leitura é realizada submetendo-se as informações sensíveis protegidas sob a forma digital a um tratamento digital que emprega uma ou várias assinaturas digitais obtida(s) a partir de pelo menos uma característica estrutural de um elemento material escolhido entre a totalidade ou parte de um material fibroso, plástico, metálico, feito de couro, feito de madeira, compósito, feito de vidro, feito de mineral ou feito de uma estrutura cristalina, a uma ou várias assinaturas digitais sendo usadas como chave de leitura.

2. Processo de acordo com a reivindicação 1 caracterizado pelo fato de que a proteção das informações sensíveis empregou as informações sensíveis sob a forma digital e pelo menos uma assinatura digital obtida a partir de pelo menos uma características estrutural de um elemento material escolhido entre a totalidade ou parte de um material fibroso, plástico, metálico, feito de couro, feito de madeira, compósito, feito de vidro, feito de mineral ou feito de uma estrutura cristalina, e pelo fato de que, a leitura é realizada submetendo-se as informações sensíveis protegidas sob a forma digital a um tratamento digital inverso daquele utilizado para a proteção das mesmas e que emprega uma ou várias assinaturas digitais do elemento material que serviu para a proteção das mesmas.

3. Processo de acordo com a reivindicação 1 ou 2 caracterizado pelo fato de que ele utiliza pelo menos uma assinatura digital obtida a partir de pelo menos uma características estrutural de um elemento material que informa sobre sua estrutura complexa, caótica, única e estável.

4. Processo de acordo com qualquer uma das reivindicações 1 a 3 caracterizado pelo fato de que a(s) assinatura(s) digital(ais) é (são) aleatória(s).

5. Processo de acordo com qualquer uma das reivindicações 1 a 4 caracterizado pelo fato de que o elemento material é escolhido entre a totalidade ou parte de um papel, papelão ou não tecido.

6. Processo de acordo com a reivindicação 5 caracterizado pelo fato de que o elemento material é uma parte de um papel, papelão ou não tecido, sobre o

qual ele é assinalado por um material transparente, estável no tempo e que assegura sua proteção, por exemplo, um revestimento plástico ou uma resina.

7. Processo de acordo com qualquer uma das reivindicações 2 a 6 caracterizado pelo fato de que a ou as assinaturas digitais utilizadas por ocasião da leitura correspondem àquelas utilizadas por ocasião da proteção.

8. Processo de acordo com a reivindicação 7 caracterizado pelo fato de que a ou as características estruturais digitais e/ou a ou as assinaturas digitais empregadas pro ocasião da proteção são salvaguardadas de maneira durável e segura, enquanto o elemento material é destruído, e são utilizadas por ocasião da leitura.

9. Processo de acordo com qualquer uma das reivindicações 2 a 5 caracterizado pelo fato de que a ou as assinaturas digitais utilizadas por ocasião da leitura são submetidas a chaves de controle, de código corretores de erros ou a um teste de dependência estatística.

10. Processo de acordo com qualquer uma das reivindicações 1 a 9 caracterizado pelo fato de que, se sua execução autoriza a leitura com êxito das informações sensíveis, ele valida também o caráter autêntico da ou das assinaturas digitais utilizadas, e/ou do elemento material do qual elas são provenientes.

11. Processo de acordo com qualquer uma das reivindicações 1 a 10 caracterizado pelo fato de que ele compreende uma etapa suplementar de comparação das informações lidas com as informações sensíveis conhecidas pelo usuário, permitindo assim validar, o caráter autêntico da ou das assinaturas digitais utilizadas, do elemento material do qual elas são provenientes e das informações sensíveis.

12. Processo de acordo com qualquer uma das reivindicações 1 a 11 caracterizado pelo fato de que a assinatura digital do elemento material é obtida por detecção, com o auxílio de um ou vários sensores, de uma ou várias características estruturais desse elemento, seguida por uma digitalização, eventualmente acompanhada por uma codificação de acordo com um ou vários algoritmos, dessa ou dessas características.

13. Processo de acordo com a reivindicação 12 caracterizado pelo fato de que a(s) característica(s) estrutural(ais) detectada(s) informa(m) sobre a estrutura complexa, caótica, única e estável do elemento material.

14. Processo de acordo com a reivindicação 12 ou 13 caracterizado pelo fato de que a detecção é realizada graças a um sensor óptico ou eletrônico, depois de aplicação no elemento material de uma onda ou de uma radiação eletromagnética.

15. Processo de acordo com a reivindicação 12 ou 13 caracterizado pelo fato de que a detecção é realizada graças a um sensor com contato, o elemento material servindo de suporte de uma onda ultra-sônica, ou de uma solicitação do tipo elétrico, térmico, químico, biológico, o comportamento/a resposta do elemento material submetido a essa onda ou solicitação sendo registrado em diferentes orientações.

16. Processo de acordo com qualquer uma das reivindicações 1 a 15 caracterizado pelo fato de que a assinatura digital se apresenta sob uma forma binária ou sob a forma de uma imagem real ou complexa ou várias imagens em níveis de cinza.

17. Processo de acordo com qualquer uma das reivindicações 1 a 16 caracterizado pelo fato de que ele emprega a assinatura digital de um elemento material, parte de um papel, papelão ou não tecido, obtida depois de detecção de sua interação com a luz visível por transvisão, utilizando-se para isso um sensor CCD ou CMOS.

18. Processo de acordo com uma das reivindicações 1 a 17 caracterizado pelo fato de que a leitura utiliza um ou vários algoritmos de decodificação, a ou as assinaturas digitais servindo como chaves de decodificação.

19. Processo de acordo com qualquer uma das reivindicações 2 a 17 caracterizado pelo fato de que a proteção das informações sensíveis sob a forma digital é realizada com o auxílio de um algoritmo esteganográfico, a(s) assinatura(s) digital(ais) do elemento material desempenhando um papel de chaves de esteganografia.

20. Processo de acordo com qualquer uma das reivindicações 2 a 17 caracterizado pelo fato de que a proteção das informações sensíveis sob a forma digital é realizada por combinação com pelo menos uma assinatura digital de um elemento material, tornando pelo menos parcialmente ilegíveis, ao mesmo tempo as informações sensíveis sob a forma digital e a assinatura digital.

21. Processo de acordo com a reivindicação 20 caracterizado pelo fato de que a combinação é realizada a partir da forma binária, hexadecimal, ASCII ou alfabética, das informações sensíveis sob a forma digital e da ou das assinaturas digitais do elemento material, por aplicação conjuntamente ou não dos princípios de permutação, transposição, substituição, iteração, máscara (operadores lógicos entre os quais XOR, adição, subtração, bit a bit (em cadeia), ou bloco a bloco...) ou propriedades matemáticas de álgebra modular (módulo n), de teoria dos números.

22. Processo de acordo com a reivindicação 20 caracterizado pelo fato de que a combinação foi realizada por aplicação do princípio de máscara descartável.

23. Processo de acordo com qualquer uma das reivindicações 2 a 17 caracterizado pelo fato de que a proteção das informações sensíveis sob a forma digital foi realizada, utilizando-se para isso a(s) assinatura(s) digital(ais) como «invólucro digital» das informações digitais sensíveis sob a forma comprimida, codificada e/ou esteganografiada.

24. Processo de acordo com qualquer uma das reivindicações 1 a 23 caracterizado pelo fato de que a ou as características estruturais são digitalizadas, e depois amostradas no tempo.

25. Processo de acordo com qualquer uma das reivindicações 1 a 23 caracterizado pelo fato de que as informações sensíveis são dinâmicas, tais como uma seqüência sonora e/ou de vídeo.

26. Processo de acordo com a reivindicação 25 caracterizado pelo fato de que a proteção é realizada com o auxílio de uma assinatura digital dinâmica obtida por repetição de uma assinatura digital estática ou por detecção repetida, com o auxílio de um ou vários sensores, de uma ou várias características estruturais de um elemento material estático.

27. Processo de acordo com a reivindicação 25 caracterizado pelo fato de que a proteção é realizada com o auxílio de uma assinatura digital dinâmica obtida por detecção de modo contínuo, com o auxílio de um ou vários sensores, de uma ou várias características estruturais de um elemento material em movimento relativo em relação ao(s) sensor(es).

28. Processo de acordo com a reivindicação 27 caracterizado pelo fato de que o elemento material é uma bobina de papel, papelão ou não tecido, em deslocamento, ou papel em decorrer de fabricação em máquina de papel.

29. Processo de acordo com qualquer uma das reivindicações 2 a 28 caracterizado pelo fato de que a proteção emprega várias assinaturas digitais de um mesmo ou de diferentes elementos materiais, e pelo fato de que a leitura recorre a várias assinaturas digitais de um ou vários elementos materiais, autorizando níveis de acesso distintos a certas partes das informações sensíveis.

30. Processo de proteção de informações sensíveis que emprega as informações sensíveis sob a forma digital e pelo menos uma assinatura digital obtida a partir de pelo menos uma característica estrutural de um elemento material escolhido entre a totalidade ou parte de um material fibroso, plástico, metálico, feito de couro, feito de madeira, compósito, feito de vidro, feito de mineral ou feito de uma estrutura cristalina, caracterizado pelo fato de que a proteção das informações sensíveis sob a forma digital é realizada com o auxílio de um algoritmo criptográfico, a(s) assinatura(s) digital(ais) do elemento material desempenhando o papel de chave(s) de criptografia.

31. Processo de proteção de informações sensíveis que emprega as informações sensíveis sob a forma digital e pelo menos uma assinatura digital obtida a partir de pelo menos uma característica estrutural de um elemento material escolhido entre a totalidade ou parte de um material fibroso, plástico, metálico, feito de couro, feito de madeira, compósito, feito de vidro, feito de mineral ou feito de uma estrutura cristalina, caracterizado pelo fato de que a proteção das informações sensíveis sob a forma digital é realizada com o auxílio de um algoritmo esteganográfico, a(s) assinatura(s) digital(ais) do elemento material desempenhando

o papel de chave(s) de esteganografia.

32. Processo de proteção de informações sensíveis que emprega as informações sensíveis sob a forma digital e pelo menos uma assinatura digital obtida a partir de pelo menos uma característica estrutural de um elemento material escolhido entre a totalidade ou parte de um material fibroso, plástico, metálico, feito de couro, feito de madeira, compósito, feito de vidro, feito de mineral ou feito de uma estrutura cristalina, caracterizado pelo fato de que a proteção das informações sensíveis sob a forma digital é realizada por combinação com pelo menos uma assinatura digital de um elemento material, que torna pelo menos parcialmente ilegíveis, ao mesmo tempo as informações sensíveis sob a forma digital e a assinatura digital, a partir de sua forma binária, hexadecimal, ASCII ou alfabética, por aplicação conjuntamente ou não dos princípios de permutação, transposição, substituição, iteração, máscara (operadores lógicos entre os quais XOR, adição, subtração, bit a bit (em cadeia), ou bloco a bloco...) ou propriedades matemáticas de álgebra modular (módulo n), de teoria dos números.

33. Processo de proteção de acordo com a reivindicação 32 caracterizado pelo fato de que a combinação foi realizada por aplicação do princípio de máscara descartável.

34. Processo de proteção de informações sensíveis que emprega as informações sensíveis sob a forma digital e pelo menos uma assinatura digital obtida a partir de pelo menos uma característica estrutural de um elemento material escolhido entre a totalidade ou parte de um material fibroso, plástico, metálico, feito de couro, feito de madeira, compósito, feito de vidro, feito de mineral ou feito de uma estrutura cristalina, caracterizado pelo fato de que a proteção das informações sensíveis sob a forma digital foi realizada, utilizando-se para isso a(s) assinatura(s) digital(ais) como «invólucro digital» das informações digitais sensíveis sob a forma comprimida, codificada e/ou esteganografiada.

35. Processo de proteção de acordo com qualquer uma das reivindicações 30 a 34 caracterizado pelo fato de que é utilizada pelo menos uma assinatura digital obtida a partir de pelo menos uma característica estrutural de um

elemento material que informa sobre sua estrutura complexa, caótica, única e estável.

36. Processo de proteção de acordo com qualquer uma das reivindicações 30 a 35 caracterizado pelo fato de que o elemento material é escolhido entra a totalidade ou parte de um papel, papelão ou não tecido.

37. Processo de proteção acordo com a reivindicação 36 caracterizado pelo fato de que o elemento material é uma parte de um papel, papelão ou não tecido, sobre o qual ele é assinalado por um material transparente, estável no tempo e que assegura sua proteção, por exemplo, um revestimento plástico ou uma resina.

38. Processo de proteção acordo com qualquer uma das reivindicações 30 a 37 caracterizado pelo fato de que a assinatura digital do elemento material é obtida por detecção, com o auxílio de um ou vários sensores, de uma ou várias características estruturais desse elemento, seguida por uma digitalização e eventualmente acompanhada por uma codificação de acordo com um ou vários algoritmos dessa ou dessas características estruturais.

39. Processo de proteção acordo com a reivindicação 38 caracterizado pelo fato de que a(s) característica(s) estrutural(ais) informa(m) sobre sua estrutura complexa, caótica, única e estável.

40. Processo de proteção acordo com a reivindicação 38 ou 39 caracterizado pelo fato de que a detecção é realizada graças a um sensor óptico ou eletrônico, depois de aplicação sobre o elemento material de uma onda ou de uma radiação eletromagnética.

41. Processo de proteção acordo com a reivindicação 38 ou 39 caracterizado pelo fato de que a detecção é realizada graças a um sensor com contato, o elemento material servindo de suporte de uma onda ultra-sônica, ou de uma solicitação de tipo elétrico, térmico, químico, biológico, o comportamento/a resposta do elemento material submetido a essa onda ou solicitação sendo registrado em diferentes orientações.

42. Processo de proteção acordo com qualquer uma das reivindicações 30 a 41 caracterizado pelo fato de que a assinatura digital se apresenta sob uma

forma binária ou sob a forma de uma imagem ou várias imagens em níveis de cinza.

43. Processo de proteção acordo com qualquer uma das reivindicações 30 a 42 caracterizado pelo fato de que ele emprega a assinatura digital de um elemento material, parte de um papel, papelão ou não tecido, obtida depois de detecção de sua interação com a luz visível por transvisão, utilizando-se para isso um sensor CCD ou CMOS.

44. Processo de proteção de acordo com qualquer uma das reivindicações 30 a 43 caracterizado pelo fato de que a ou as características estruturais são digitalizadas, e depois amostradas no tempo.

45. Processo de proteção de acordo com qualquer uma das reivindicações 30 a 44 caracterizado pelo fato de que as informações sensíveis são dinâmicas, tais como uma seqüência sonora e/ou de vídeo.

46. Processo de proteção de acordo com a reivindicação 45 caracterizado pelo fato de que a proteção é realizada com o auxílio de uma assinatura digital dinâmica obtida por repetição de uma assinatura digital estática ou por detecção repetida, com o auxílio de um ou vários sensores, de uma ou várias características estruturais de um elemento material estático.

47. Processo de proteção de acordo com a reivindicação 46 caracterizado pelo fato de que a proteção é realizada com o auxílio de uma assinatura digital dinâmica obtida por detecção de modo contínuo, com o auxílio de um ou vários sensores, de uma ou várias características estruturais de um elemento material em movimento relativo em relação ao(s) sensor(es).

48. Processo de proteção de acordo com a reivindicação 47 caracterizado pelo fato de que o elemento material é uma bobina de papel, papelão ou não tecido, em deslocamento, ou papel em decorrer de fabricação em máquina de papel.

49. Processo de proteção de acordo com qualquer uma das reivindicações 30 a 48 caracterizado pelo fato de que a proteção emprega várias assinaturas digitais de um mesmo ou de diferentes materiais, que permitem ulteriormente dar acesso a leituras parciais e/ou distintos às informações sensíveis.

50. Suporte portador de dados que compreende informações sensíveis

protegidas da leitura direta cuja proteção empregou as informações sensíveis sob a forma digital e pelo menos uma assinatura digital obtida a partir de pelo menos uma característica estrutural de um elemento material caracterizado pelo fato de que ele se apresenta sob a forma de um documento em papel, papelão ou não tecido, do qual a totalidade ou parte corresponde ao elemento material do qual é proveniente pelo menos uma assinatura digital que serviu para a proteção das informações sensíveis, que está sob uma forma localizada e protegida por um invólucro transparente externo que desempenha um papel protetor contra as agressões exteriores normais de utilização, do qual ele não pode ser separado sem destruição.

51. Suporte portador de dados de acordo com a reivindicação 50, caracterizado pelo fato de que compreende informações sensíveis protegidas da leitura direta cuja proteção empregou as informações sensíveis sob a forma digital e pelo menos uma assinatura digital obtida a partir de pelo menos uma característica estrutural de um elemento material que informa sobre sua estrutura complexa, caótica, única e estável.

52. Suporte de acordo com a reivindicação 50 ou 51 caracterizado pelo fato de que ele é portador da totalidade ou de parte das informações sensíveis originais.

53. Suporte de acordo com qualquer uma das reivindicações 50 a 52 caracterizado pelo fato de que ele integra pelo menos uma assinatura digital obtida a partir de uma característica estrutural de um elemento material que informa sobre sua estrutura complexa, caótica, única e estável.

54. Suporte de acordo com a reivindicação 53 caracterizado pelo fato de que a(s) assinatura(s) digital(ais) está (estão) sob a forma codificada.

55. Suporte de acordo com qualquer uma das reivindicações 50 a 54 caracterizado pelo fato de que a proteção foi realizada de acordo com um dos processos do tipo definido em qualquer uma das reivindicações 30 a 49.

56. Suporte de acordo com qualquer uma das reivindicações 50 a 55 caracterizado pelo fato de que as informações sensíveis protegidas são impressas sobre o dito suporte sob a forma de um código de barras.

57. Suporte de acordo com qualquer uma das reivindicações 50 a 56 caracterizado pelo fato de que ele integra um ou múltiplos elementos sensíveis às radiofreqüências empregados em uma transmissão sem contato e à distância de informação.

58. Suporte de acordo com qualquer uma das reivindicações 50 a 57 caracterizado pelo fato de que ele integra um chip no qual as informações sensíveis protegidas são registradas.

59. Dispositivo adaptado para a execução do processo de leitura do tipo definido em qualquer uma das reivindicações 1 a 29, caracterizado pelo fato de que ele compreende meios para assinalar um elemento material selecionado e detectar nesse último, uma ou várias de suas características estruturais, em especial que informam sobre sua estrutura complexa, caótica, única e estável, ligados a uma unidade de estocagem e de tratamento que assegura:

a2) a aquisição, a conformação/o condicionamento, a digitalização e eventualmente a codificação de acordo com um ou vários algoritmos da ou das características estruturais detectadas para gerar um (ou várias) assinatura(s) digital(ais), que informam vantajosamente sobre o caráter complexo, caótico, único e estável da estrutura do elemento material,

b2) a leitura das informações sensíveis protegidas por execução de um tratamento digital que utiliza a ou as assinaturas digitais geradas na etapa a2, como chave(s) de leitura, e que corresponde vantajosamente ao tratamento digital sensivelmente inverso àquele utilizado para a associação da (ou das) assinatura(s) digital(ais) às informações sensíveis originais, por ocasião da proteção das mesmas.

60. Dispositivo adaptado para a execução do processo de leitura do tipo definido em qualquer uma das reivindicações 1 a 29, caracterizado pelo fato de que ele compreende meios para assinalar um elemento material selecionado e detectar nesse último, uma ou várias de suas características estruturais, em especial que informam sobre sua estrutura complexa, caótica, única e estável, ligados a uma unidade de estocagem e de tratamento que assegura:

a2) a digitalização e eventualmente a codificação de acordo com um ou

vários algoritmos da ou das características estruturais detectadas para gerar uma (ou várias) assinatura(s) digital(ais),

b2) a leitura das informações sensíveis protegidas por execução de um tratamento digital que utiliza a ou as assinaturas digitais geradas na etapa a2, como chave(s) de leitura, e que corresponde ao tratamento digital sensivelmente inverso àquele utilizado para a associação da (ou das) assinatura(s) digital(ais) às informações sensíveis originais, por ocasião da proteção das mesmas.

61. Dispositivo de acordo com a reivindicação 59 ou 60 caracterizado pelo fato de que um sensor óptico é utilizado para detectar a ou as características estruturais do elemento material.

62. Dispositivo de acordo com qualquer uma das reivindicações 59 a 61 caracterizado pelo fato de que o sensor óptico é um sensor CCD ou CMOS que assegura a detecção da ou das características estruturais por transvisão.

63. Processo de codificação de chaves assimétricas, que utiliza uma chave pública e uma chave privada, caracterizado pelo fato de que a chave pública e/ou a chave privada são uma assinatura digital obtida a partir de pelo menos uma características estrutural de um elemento material escolhido entre a totalidade ou parte de um material fibroso, plástico, metálico, feito de couro, feito de madeira, compósito, feito de vidro, feito de mineral ou feito de uma estrutura cristalina.

64. Processo de codificação de acordo com a reivindicação 63 caracterizado pelo fato de que ele emprega uma assinatura digital obtida a partir de pelo menos uma característica estrutural do elemento material que informa sobre sua estrutura complexa, caótica, única e estável.

65. Processo de aumento de segurança de informações sensíveis caracterizado pelo fato de que compreende as seguintes etapas:

a) uma etapa de proteção da leitura direta das informações sensíveis que emprega um processo de proteção do tipo definido em qualquer uma das reivindicações 33 a 52, que permite obter as informações sensíveis sob formas protegidas,

b) uma etapa de leitura das informações protegidas na etapa a), que

permite reencontrar as informações sensíveis.

66. Processo de aumento de segurança de acordo com a reivindicação 65 caracterizado pelo fato de que a etapa de leitura emprega um processo de leitura correspondente do tipo definido em qualquer uma das reivindicações 1 a 29.

67. Processo de aumento de segurança de acordo com a reivindicação 65 ou 66 caracterizado pelo fato de que a etapa a) é seguida por uma etapa de registro das informações sensíveis sob a forma protegida em um suporte de dados.

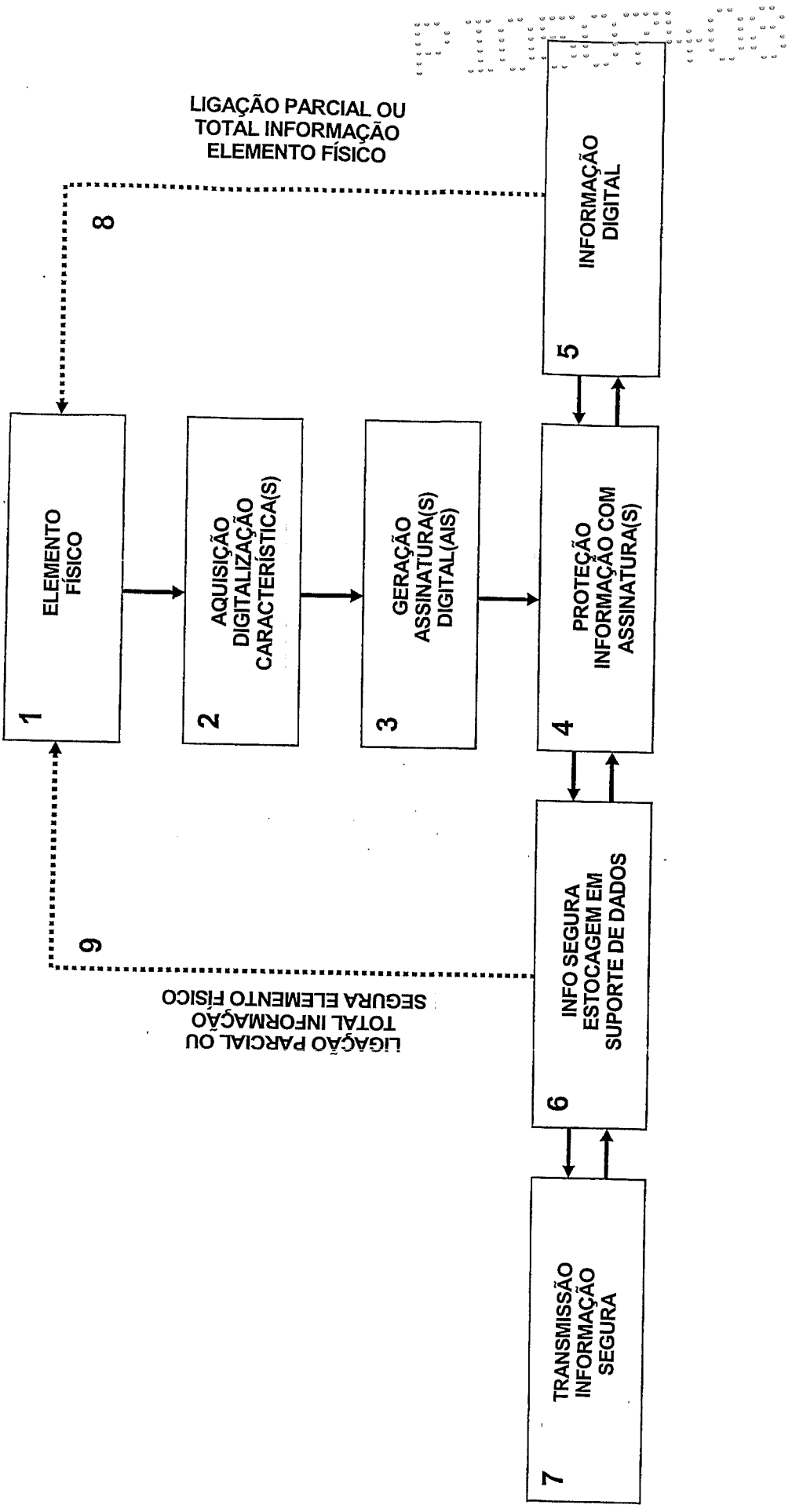
LIGAÇÃO PARCIAL OU
TOTAL INFORMAÇÃO
ELEMENTO FÍSICO
8
INFORMAÇÃO
DIGITAL
5
ELEMENTO
FÍSICO
1
AQUISIÇÃO
DIGITALIZAÇÃO
CARACTERÍSTICA(S)
2
GERAÇÃO
ASSINATURA(S)
DIGITAL(AIS)
3
PROTEÇÃO
INFORMAÇÃO COM
ASSINATURA(S)
4
9
INFO SEGURA
ESTOCAGEM EM
SUPORTE DE DADOS
6
TRANSMISSÃO
INFORMAÇÃO
SEGURA
7
LIGAÇÃO PARCIAL OU
TOTAL INFORMAÇÃO
SEGURA ELEMENTO FÍSICO

FIG. 1

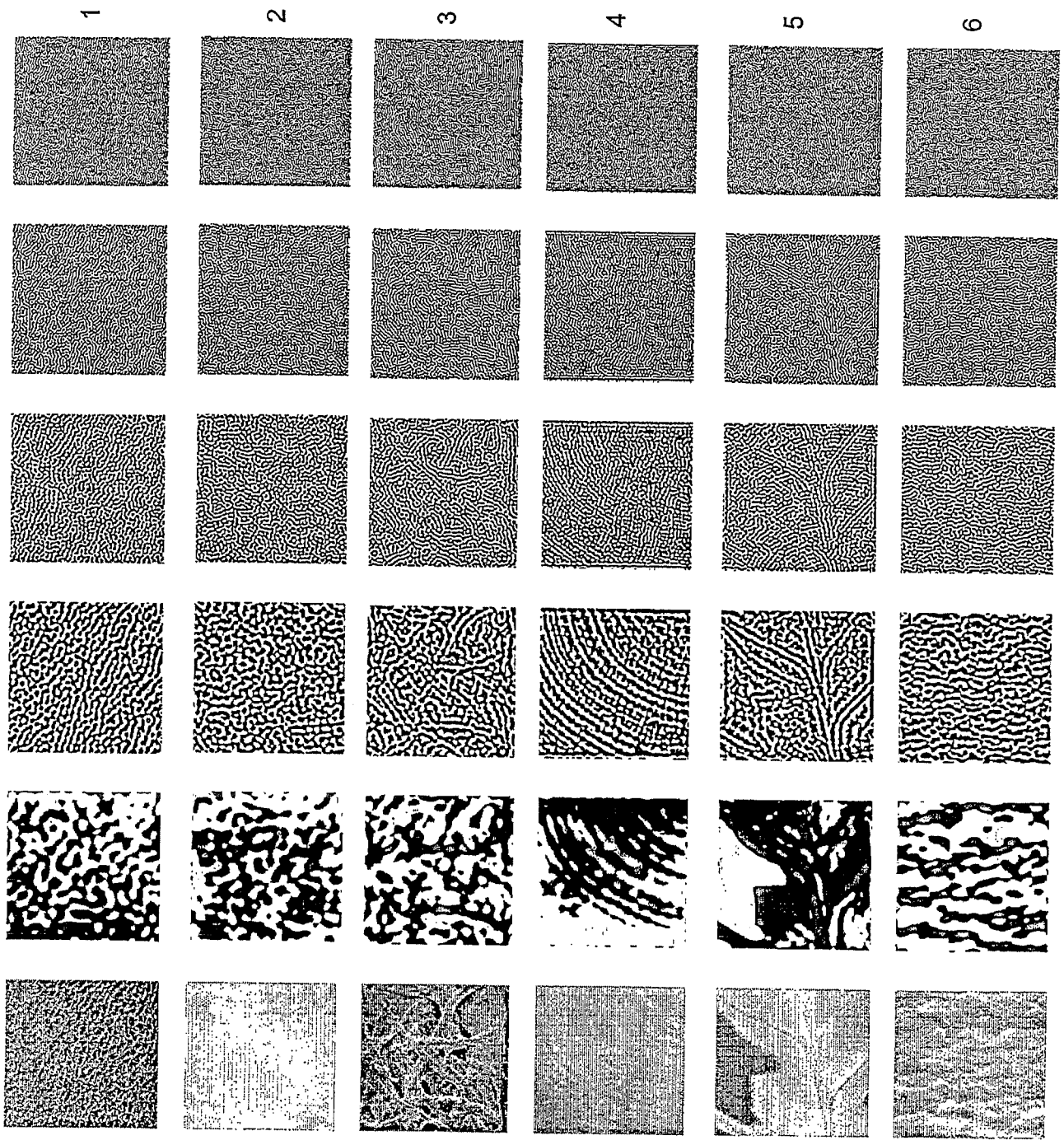

FIG. 2

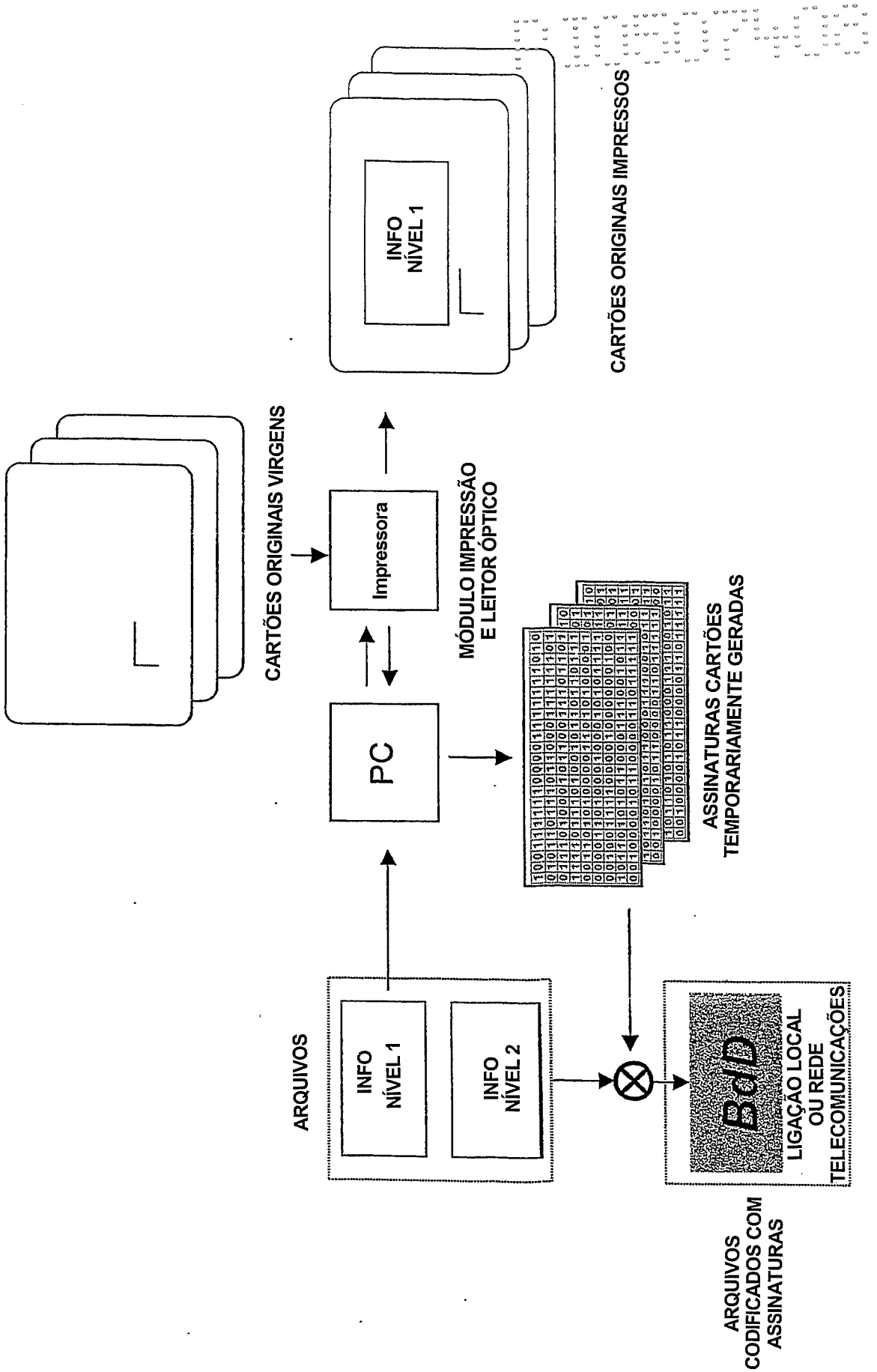
CARTÕES ORIGINAIS IMPRESSOS
INFO NÍVEL 1
CARTÕES ORIGINAIS VIRGENS
Impressora
MÓDULO IMPRESSÃO E LEITOR ÓPTICO
PC
ASSINATURAS CARTÕES TEMPORARIAMENTE GERADAS
ARQUIVOS
INFO NÍVEL 1
INFO NÍVEL 2
BdD
LIGAÇÃO LOCAL OU REDE TELECOMUNICAÇÕES
ARQUIVOS CODIFICADOS COM ASSINATURAS

FIG. 3

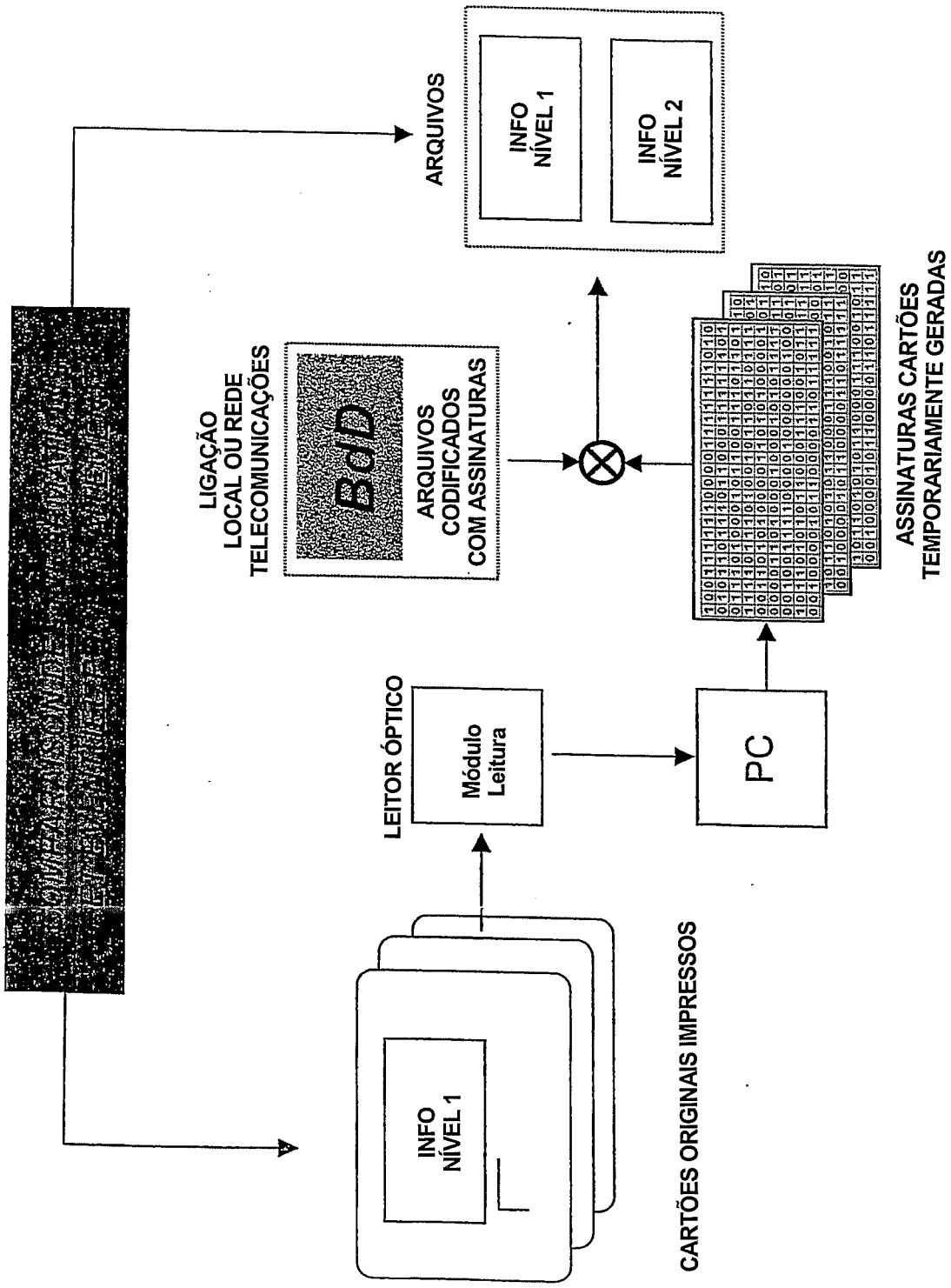
ARQUIVOS
INFO NÍVEL 1
INFO NÍVEL 2
LIGAÇÃO LOCAL OU REDE TELECOMUNICAÇÕES
BdD
ARQUIVOS CODIFICADOS COM ASSINATURAS
ASSINATURAS CARTÕES TEMPORARIAMENTE GERADAS
LEITOR ÓPTICO
Módulo Leitura
PC
INFO NÍVEL 1
CARTÕES ORIGINAIS IMPRESSOS

FIG. 4