REPÚBLICA FEDERATIVA DO BRASIL

Ministério do Desenvolvimento, Indústria e Comércio Exterior
Instituto Nacional da Propriedade Industrial

CARTA PATENTE N.º PI 0008900-1

Patente de Invenção

O INSTITUTO NACIONAL DA PROPRIEDADE INDUSTRIAL concede a presente PATENTE, que outorga ao seu titular a propriedade da invenção caracterizada neste título, em todo o território nacional, garantindo os direitos dela decorrentes, previstos na legislação em vigor.

(21) Número do Depósito : PI 0008900-1

(22) Data do Depósito : 17/01/2000

(43) Data da Publicação do Pedido : 20/07/2000

(51) Classificação Internacional : G06F 21/20; G06T 7/00; G07F 19/00

(30) Prioridade Unionista : 18/01/1999 US 09/232,538

(54) Título : APARELHO PARA COLETAR E TRANSMITIR DADOS BIOMÉTRICOS ATRAVÉS DE UMA REDE E MÉTODO PARA COLETAR E TRANSMITIR DADOS BIOMÉTRICOS ATRAVÉS DE UMA REDE.

(73) Titular : IRIDIAN TECHNOLOGIES, INC., Sociedade Norte Americana. Endereço: 121 Whittendale Drive, Moorestown, New Jersey 08057, Estados Unidos (US).

(72) Inventor : RANDAL GLASS, Norte Americano(a). Endereço: 441 Briar Creek Drive, Hockessin, Delaware 19707, Estados Unidos. Cidadania: Norte Americana.; MARCOS SALGANICOFF, Norte Americano(a). Endereço: 70 North 26th Street, Philadelphia, PA 19130, Estados Unidos. Cidadania: Norte Americana.; ULF CAHN VON SEELEN. Endereço: 2130 Spruce Street, Apt A2 Philadelphia, PA 19103, Estados Unidos. Cidadania: Alemã.

Prazo de Validade : 10 (dez) anos contados a partir de 07/10/2014, observadas as condições legais.

Expedida em : 7 de Outubro de 2014.

Assinado digitalmente por
Júlio César Castelo Branco Reis Moreira
Diretor de Patentes

"APARELHO PARA COLETAR E TRANSMITIR DADOS BIOMÉTRICOS ATRAVÉS DE UMA REDE E MÉTODO PARA COLETAR E TRANSMITIR DADOS BIOMÉTRICOS ATRAVÉS DE UMA REDE"

Campo da Invenção

A presente invenção se relaciona a dados biométricos não processados a partir de uma câmara ou de um outro sensor para um servidor remoto através de uma rede de maneira segura.

Histórico da Invenção

Ocorrem muitas situações onde é necessário identificar a pessoa que tenta entrar em um site de segurança, usar um sistema de computador, ou realizar uma transação financeira ou uma outra transação onde se requer que esta pessoa seja autorizada a realizar tal tarefa. Há diversos métodos, que são conhecidos como biométricos, para reconhecer ou identificar uma pessoa. Estes métodos incluem analisar assinatura, obter e analisar a imagem de uma impressão digital e formar e analisar imagem dos padrões vasculares da retina de um olho humano. Recentemente, a técnica usava a íris do olho que contém um padrão altamente detalhado e que é único para cada pessoa e estável por muitos anos como um elemento biométrico não-obstrusivo e de não-contato. Esta técnica se encontra descrita na patente U.S. N° 4.641.349 depositada para Flom e associados e N° 5.291.561 para Daugman. Sistemas de identificação biométricos captam a imagem da pessoa a ser identificada no instante em que a pessoa pretende realizar uma tarefa. Esta imagem será então processada para extrair certos aspectos particulares. O resultado deste processamento é um código de íris no caso da patente N° 5.291.560, ou em termos mais gerais, é um modelo biométrico. Este modelo biométrico recém-computado então será comparado a um modelo biométrico previamente armazenado para identificar e daí autorizar ou não que a pessoa realize tal tarefa. Verificação de identificação ou identidade de uma pessoa através de dispositivos biométricos automatizados, tais como sistemas de reconhecimento de íris e sistemas de

impressão digital, se baseiam em uma tecnologia de formação de imagem digital. Os dados biométricos brutos das pessoas, presumivelmente características individuais únicas, são obtidos por sistemas consistindo de elementos ópticos, câmara, e componentes eletrônicos que capturam e digitalizam a imagem apresentada para a câmara. A representação digital da imagem (isto é, dados de imagem brutos e não processados) então pode ser processada por um algoritmo que converte os dados de imagem para uma particular representação denominada "modelo biométrico". O modelo biométrico é adequado para ser comparado contra um modelo previamente armazenado para verificar a identidade da pessoa ou contra múltiplos modelos para identificar uma pessoa. Este método está ilustrado no fluxograma da figura 1. Freqüentemente, a conversão do modelo biométrico e a subseqüente comparação é realizada por um computador localizado remotamente em relação à câmara ou sensor, que coleta os dados biométricos. Esta conversão e comparação remota são feitas de modo que a integridade do algoritmo de computação de modelo biométrico seja mantida não se transferindo para localizações não seguras, tal como um microcomputador doméstico. Assim, os dados biométricos digitalizados não-protegidos devem ser transmitidos da câmara para o computador remoto. Tal transmissão pode ocorrer através de uma linha de transmissão direta e dedicada, ou através de uma linha pública, por exemplo, sistema telefônico, ou mesmo através da Internet.

Qualquer sistema biométrico pode ser fraudado se um intruso puder substituir os dados de imagem brutos antes de sua conversão para um modelo biométrico e subseqüente comparação. Por exemplo, se Mallory deseja se passar por Bob, ele precisa primeiro capturar os dados de imagem brutos de Bob e armazená-los; então poderá enganar o sistema alvo injetando artificialmente os dados de imagem falsos no instante e local corretos, de modo que a conversão e comparação do modelo resulta ser Bob de fato

na frente da câmara. O potencial para tal ataque aumenta, quando o processo de aquisição de imagem puder ser separado do processo de conversão e comparação de modelo, tal como em um caso onde o terminal remoto equipado com sistema formador de imagem (cliente) envia uma imagem através de uma rede interna ou Internet, para um servidor central que realiza conversão e comparação. A corrupção da imagem pode ocorrer em qualquer ponto entre a câmara e um sistema servidor "seguro". O próprio sistema servidor também poderá ser atacado, mas a probabilidade de um ataque bem sucedido contra este sistema será muito pequeno sem um "auxílio interno".

Há muitos locais chave onde um intruso pode realizar esta substituição de imagem. Um intruso pode substituir a câmara por um sistema que simula a funcionalidade de câmara, daí provendo uma imagem previamente armazenada para o resto do sistema. Um intruso pode ganhar acesso ao lado de dentro do hospedeiro do sistema cliente e substituir o conteúdo de memória ou depósito de quadros contendo os dados de imagem "verdadeiros" com a representação de memória de uma imagem previamente armazenada. Finalmente, o intruso pode ganhar acesso em algum lugar ao longo da trajetória de comunicação entre o sistema de cliente e o sistema servidor e substituir a imagem enquanto a mesma está sendo transmitida. Assim, há necessidade de um método ou dispositivo que possa transmitir dados biométricos ao mesmo tempo em que impede substituição ou corrupção de imagem.

Reconhecemos que podem ser feitos ataques usando uma cena artificial ou planejada. Por exemplo, um intruso pode apresentar um olho falso para um sistema que de outra forma não seria molestado. Estes são tipos de ataque completamente diferentes. A tecnologia para enfrentar tais tipos de ataques existem, e ataques deste tipo não são relevantes para a presente discussão. Ao invés, a presente invenção pretende manter a integridade de uma imagem contendo dados biométricos e impedir corrupção ou

substituição de imagem.

Foram desenvolvidas uma variedade de técnicas para detectar corrupção de imagem ou dados e cópias não autorizadas. Muito deste esforço tem sido direcionado para impedir e detectar infrações e falsificações em direitos autorais. As técnicas mais amplamente usadas aplicam marcas d´água e sinais de código incorporados à imagem. As patentes U.S. N^{os} 5.768.426, 5.809.139 e 5.822.432 divulgam métodos para marcar sinais de vídeo digitais adicionando informação do sinal ou arquivo de imagem de um modo pré-determinado de modo que os dados aparecem como ruído para um observador comum, mas pode ser detectado contra uma marca d´água ou código pelo proprietário do sinal ou arquivo de imagem. A patente U.S N° 5.613.004 divulga um método e um dispositivo esteganográficos que codifica o fluxo de dados digitalizados com chaves especiais. A patente também ensina que códigos ou outras informações podem ser pré-anexadas ou anexadas ao fluxo de dados. Uma outra técnica conhecida para se aplicar marcas d´água às imagens é alterar o brilho em pixéis selecionados em um padrão pré-determinado. Este método se encontra divulgado na patente U.S. N° 5.825.892. No entanto, nenhuma destas referências trata de assegurar que os dados biométricos não sejam comprometidos para impedir um acesso não-autorizado a sistemas ou sites seguros.

É imperativo que dados de imagem biométricos brutos sejam seguros de tal modo que uma substituição ou corrupção não-detectável da imagem antes da conversão do modelo biométrico seja extremamente difícil de realizar. Adicionalmente, pode ser desejável que dados de imagem sejam codificados de modo que as imagens tenham uma duração pré-determinada. Então, uma imagem codificada não pode ser usada para identificar um usuário mais que uma vez, (ou n vezes), e/ou as imagens sejam válidas somente dentro de um período pré-determinado de tempo além do qual não serão processadas pelo algoritmo biométrico, por

serem consideradas inválidas pelo sistema ou servidor de autenticação. Ademais, é desejável que um servidor de autenticação biométrico seja provido de um único ID do sistema formador de imagem que provê os dados de imagem para o mesmo. Deste modo, um servidor de autorização pode determinar que Bob está na frente da câmara ID #xyz para fazer uma transação ID #pdq, que a captura ocorreu no intervalo t_2-t_1, e que a imagem não foi alterada, nem reutilizada, a partir de outra transação.

Por exemplo, para aplicações comerciais, para cada transação corresponderá exatamente uma imagem associada. Também, se o cliente não prover a imagem para o servidor dentro de uma janela de tempo, a transação não será autorizada. Isto provê níveis adicionais de proteção impedindo uma posterior substituição de imagens previamente válidas e forçando um intruso a desenvolver métodos que funcionem dentro de um prazo de validade, que adiciona considerável dificuldade a um intruso.

Para prover uma segurança adequada, o segredo deve ser compartilhado somente por emitente (câmara) e recipiente (sistema que realiza autenticação da imagem). Este segredo deve permanecer em segurança, ou a segurança de todo o sistema será comprometida. O segredo compartilhado entre câmara e servidor de autenticação se encontra na forma de chave digital ou em alguns casos, um par de chaves. O pacote reativo/ resistente a corrupção da câmara protege chave secreta incorporada ao seu interior. A chave do servidor deve ser protegida por medidas de segurança, tais como, firewall, controle de acesso físico, etc. para se prover altos níveis de segurança aos dados sensíveis.

Recentemente tem aumentado o uso de microcomputadores tanto no escritório quanto em casa. Inicialmente, estes microcomputadores eram usados quase exclusivamente para processamento de texto e aplicações de banco de dados. Hoje, os microcomputadores estão sendo usados para uma variedade de atividades de comunicação que se estendem de

correio eletrônico e transferência de arquivos a operações bancárias (home_banking) e transações comerciais através de rede. Assim, é necessário um sistema que possa ser conectado a um microcomputador para garantir transmissão e recepção de dados biométricos de modo seguro através de uma rede não segura, daí permitindo ao usuário, com identidade certificada remotamente, ser autorizado a realizar transferências financeiras ou transação solicitada.

Sumário da Invenção

Provemos um sistema e uma metodologia que possam prover uma transmissão segura e uma subseqüente autenticação para os dados biométricos a serem usados no esquema cliente servidor, no qual os dados biométricos são transferidos de um computador para outro computador através de rede não segura para identificar ou verificar identidade de um usuário. Preferimos prover uma câmara que funciona como sensor para coletar dados biométricos. Os dados são digitalizados para um arquivo de dados biométricos. Um código é aplicado a este arquivo. Então, o arquivo com código será transmitido para uma rede para ser transferido para um sistema servidor de autenticação. O sistema servidor de autenticação valida os dados recomputando os códigos a partir de seu conhecimento dos dados de entrada necessários para gerar um código. Se os dados forem autênticos, o servidor retifica o arquivo de dados biométricos para um modelo biométrico a ser usado para verificar a identidade do usuário.

Adicionalmente, preferimos prover um gerador de marcações (token) no servidor de autenticação que envia uma marcação para a câmara ou para um outro sensor. Esta marcação é aplicada ao arquivo digital antes de ser transferida para o servidor de autenticação. A marcação define uma única transação e conecta os dados biométricos à transação assim evitando o uso posterior de dados biométricos ou estabelecendo um prazo além do qual os dados se tornam inválidos.

O código que é aplicado à imagem para transferência é computado em função de imagem, marcação, e uma chave secreta associada à câmara. A chave secreta assegura que um intruso tendo conhecimento de imagem, marcação, e algoritmo para geração de marcações e código ainda não possa criar um código válido para uma imagem falsa. A chave secreta pode ser um número de série, ou um outro número de identificação único para câmara ou sensor que coleta os dados biométricos. Se for usado tal código podemos prover uma autoridade separada para certificação de câmara que contenha uma lista das câmaras autorizadas. O servidor de autenticação consulta a autoridade de certificação a cada vez que uma nova imagem é recebida, de modo que o servidor tenha conhecimento da chave secreta correspondente à câmara que gera o sinal de imagem. A autoridade para certificação de câmara pode ser um simples banco de dados localizado dentro do servidor de autenticação ou em um computador separado. Uma autoridade de certificação separada é útil quando houver dois ou mais servidores conectados à rede.

Outros objetivos e vantagens da invenção se tornarão aparentes a partir da descrição de certas configurações presentemente preferidas mostradas nos desenhos.

Descrição Resumida dos Desenhos

A figura 1 é um fluxograma das etapas básicas para realizar identificação biométrica, como tem sido feito na técnica anterior.

A figura 2 é um diagrama de blocos de um sistema de identificação biométrica que transfere dados através de uma rede e contendo nosso sistema de segurança.

A figura 3 é um diagrama de blocos funcional do sistema formador de imagens presentemente preferido que é usado para o sistema de identificação mostrado na figura 2.

As figuras 4 e 5 são diagramas ilustrando processo de marca d´água.

A figura 6 é um diagrama de uma configuração da rede de servidor cliente, de acordo com a presente invenção.

A figura 7 é um diagrama ilustrando uma transação operacional conduzida usando nosso método.

A figura 8 é um diagrama ilustrando um segundo exemplo de uma transação operacional conduzida usando nosso método.

Descrição das Configurações Preferidas

A presente configuração preferida de nosso sistema é empregada em um sistema de servidor cliente mostrado na figura 2. O sistema cliente 1 consiste em um microcomputador 2 denominado computador hospedeiro (Host_Computer) no diagrama. O computador hospedeiro 2 pode ser qualquer microcomputador comercialmente disponível, ou um processador incorporado com suficiente memória para guardar um arquivo de imagens biométricas, e um modem ou hardware para comunicação em rede para permitir que o arquivo de imagens biométricas seja transferido para o servidor de autenticação. Há ainda um sistema formador de imagens separado 4 que é conectado ao computador hospedeiro. O sistema formador de imagem contém uma câmara 6 com elementos ópticos ou outros sensores associados para coletar dados biométricos de um usuário. Tipicamente, os dados biométricos são uma representação analógica de uma imagem e digitalizados e armazenados para posterior transferência. Preferimos prover um digitalizador e memória ou depósito de quadros que digitaliza a imagem e então armazena a mesma no sistema formador de imagem 4 para um posterior processamento e transferência. Para guardar os dados de imagem brutos, um hardware eletrônico adicional e um software são incluídos em quer um pacote de câmara digital ou em um sistema formador de imagem. Estes componentes adicionais incorporam informação aos dados de imagem antes que saiam da câmara ou do sistema formador de imagem, de tal modo que os dados de imagem possam ser subseqüentemente autenticados e validados como não-corrompidos por um outro elemento para processamento de dados externo posterior à câmara, tal como, o servidor de autenticação biométrica 10. Uma representação digital da

imagem que foi apropriadamente codificada para segurança é transmitida a partir do sistema formador de imagem para o computador hospedeiro 2 para ser transferida através da rede 9 para o servidor de autenticação 10. Antes de entrar no servidor de autenticação, os dados devem passar por um firewall 11. O firewal deve ser usado sempre que for usada uma rede Internet ou uma outra rede pública. Um firewall poderá não ser necessário se o sistema cliente for conectado ao servidor de autenticação através de uma linha de transmissão privada.

O pacote inteiro que contém o sistema formador de imagem 4, deve ser resistente a corrupção de modo a ser extremamente difícil acessar os elementos internos do pacote sem detecção ou destruição do dispositivo. É essencial assegurar que a integridade de imagens e códigos adquiridos a serem transmitidos através da rede não tenha sido comprometida. Isto é especialmente importante em aplicações onde ocorrem transações de grandes valores. Assim, em nossa configuração preferida, o sistema formador de imagem 4 será compreendido em um pacote resistente a corrupção 50 que será usado para detectar qualquer intrusão indesejada que torne o sistema inútil. O pacote resistente a intrusão pode ser passivo pelo fato de qualquer abertura para o dispositivo provocar sua destruição. Alternativamente, o pacote pode utilizar pelo menos um detector de intrusão de chassis ou chave 51, mostrado na figura 3. A chave 51 vai sinalizar a lógica de controle 44 (que pode ser implementada por um micro-controlador) para retornar para um estado de não-funcionamento similar àquele encontrado durante montagem. Este estado de não-funcionamento essencialmente vai deletar rotinas de software de chave relacionadas aos dados biométricos. Pode também deletar tabelas especiais suportadas por baterias de reserva (back-up) que incluem informações de segurança e codificação. Assim, se um intruso tiver acesso ao sistema, ele não poderá injetar vídeo nem obter dados, ou mesmo operar software, ou

software incorporado, do sistema daí tornando tais intrusões inúteis. Por conseguinte, qualquer substituição ou corrupção nos dados de imagem depois de transmitidos a partir de uma câmara segura será detectável através do processamento de dados que se segue, e a substituição ou corrupção dos dados de imagem antes da aplicação da informação de segurança sendo extremamente difícil ou mesmo impossível.

A função de segurança será efetiva somente depois de o software do sistema ser carregado e habilitado. A função de segurança permanecerá ativa até ser detectada uma intrusão ou o software do sistema ser recarregado usando um protocolo especial.

A configuração presentemente preferida de nosso sistema formador de imagem 4 está mostrada na figura 3 onde as trajetórias de dados são mostradas por linhas cheias e as trajetórias de sinais de controle são indicadas por linhas tracejadas. Elementos ópticos 41 direcionam a luz a partir da cena para um formador de imagem que pode ser uma câmara CCD, um dispositivo CMOS ou um formador de imagem bidimensional que cria uma imagem digital. Conseqüentemente, identificamos este componente 42 como Formador de Imagem & Digitalizador. A imagem digital é enviada para um multiplexador 45 e/ou uma memória para depósito de quadros 43. A unidade lógica de controle 44 determina para onde a imagem é enviada. A imagem no depósito de quadros 43 é enviada através de um debulhador 46 e compressor 47 para criar uma imagem secdcionada e comprimida que é enviada para um gerador de códigos 48 que gera um código que é aplicado à imagem. As operações de cortar e comprimir a imagem podem ser opcionais para certas aplicações, mas apresentam a vantagem de reduzir a quantidade de dados que precisa ser transmitida através da rede, daí acelerando a transmissão. Uma técnica de criptográfica é empregada para criar uma assinatura digital para cada quadro dos dados de imagem adquirido pela câmara ou elementos ópticos. Este processo de

criptografia é implementado pelos elementos de processamento acima mencionados. A assinatura digital preferivelmente deve ser uma função de mistura (hash_function) segura que considera os seguintes elementos: cada bite dos dados de imagem no quadro; uma "chave secreta" que é armazenada e que permanece oculta dentro da câmara; e opcionalmente, uma marcação digital introduzida nos elementos eletrônicos da câmara pelo hospedeiro. Alternativamente, a marcação pode ser provida pelo servidor de autenticação. A chave "oculta" ou "secreta" é requerida, uma vez que um intruso, tendo uma imagem, mais a marcação, mais o conhecimento do algoritmo de assinatura digital, poderia, sem esta chave secreta, simular a funcionalidade de autenticação da câmara.

A "chave" da câmara pode ser um pequeno bloco de dados contido dentro da câmara que é usada no algoritmo de assinatura digital. Opcionalmente, a chave poderia ser o único identificador para a câmara. Dependendo do tipo de esquema usado, a chave da câmara pode simplesmente assumir um valor arbitrário designado para cada câmara, um identificador para uma lista de câmaras, um identificador único de câmara, uma única chave para um algoritmo para assinatura simétrica, ou uma metade de um par de chaves para um algoritmo de assinatura assimétrica. O servidor de autenticação 10 deve ter *a priori* conhecimento da chave secreta (ou no caso de algoritmo assimétrico, conhecimento da chave pública complementar). Assim, para uma dada câmara, esta chave não se altera entre transações, no entanto, diferentes câmaras podem ter diferentes chaves. Também é possível haver um esquema onde as chaves de câmaras podem se alterar com base em um dado período de tempo, tal como, mensal, semanal, etc.. Neste caso, o servidor de autenticação, ou uma outra autoridade, poderá enviar uma nova chave codificada para o cliente codificado usando chave corrente na câmara. O cliente envia esta chave codificada para o sistema formador de imagem 4 que recebe

novos dados através da interface de comunicação 49. Estes dados então são enviados para o gerador de códigos 48 que decodifica a nova chave usando a chave corrente e armazena a nova chave para uso posterior.

A marcação (token) é um bloco de dados gerado para cada e para toda transação. Cada marcação é única e nunca mais será usada. As marcações assim podem ser usadas para identificar qualquer transação em particular. Qualquer função para a qual seja garantida geração de um único resultado, pode ser usada para gerar marcações. O uso de uma marcação provê um nível adicional de segurança pelo fato de acoplar os dados de imagem a uma transação específica.

A assinatura digital acima mencionada pode ser implementada como uma função de mistura O resultado da função de mistura é um bloco de dados menor que seus elementos de entrada. Uma importante característica de uma função de mistura é que sendo dadas as mesmas entradas, a reaplicação da função de mistura produzirá o mesmo resultado. Adicionalmente, funções de mistura de alta segurança se caracterizam pelo fato de qualquer mudança nos elementos de entrada resultar em uma mudança importante no bloco de dados resultante. Em particular, se a função de mistura for computada com os dados de imagem, qualquer mudança introduzida nos dados de imagem provocará em um diferente resultado para a função de mistura. A assinatura digital dos dados pode ser enviada para um outro sistema (isto é, para o servidor de autenticação) junto com os dados originais; e o sistema de recepção pode, com a mesma marcação ou com uma marcação complementar, computar a assinatura dos dados originais e verificá-la contra a assinatura enviada com os dados. Se as assinaturas combinarem, pode-se assumir que os dados não foram alterados com nível de confiança extremamente alto. Assim, se uma função DS (x, y, z), onde x representa dados de imagem, y uma marcação, e z chave secreta, produz resultado Q, então dado x, e Q

através de meios para troca de dados e sabendo ambos valores originais y, z, assim como a função de mistura DS (_), um recipiente poderá computar Q'= DS (x, y, z). Se Q= Q', então x, y, z não foram alterados, e caso contrário, um ou mais itens dos dados foram alterados. Na prática, a função de mistura será computada com respeito a combinação dos dados de imagem, marcação opcional, e chave secreta. Para segurança adicional, função DS pode operar como algoritmo assimétrico, onde um ou mais parâmetros funcionais podem ser diferentes (mas complementares) para ambos os lados, enviar e receber.

Há uma variedade de modos pelos quais a assinatura digital computada pela câmara pode ser enviada de volta para o sistema de autenticação. O método mais direto é anexar (ou pré-anexar) a assinatura aos dados e enviar pacote completo de volta para o sistema de autenticação. Uma outra técnica é usar uma técnica de marca d´água para incorporar a informação de assinatura diretamente aos dados de imagem originais. Isto pode ser realizado de um modo no qual a assinatura incorporada desaparece na imagem, e não podendo ser distinguida do ruído randômico. O sistema de recepção pode determinar a seqüência de decodificação da assinatura incorporada para separar a mesma da imagem, e então realizar autenticação, acima mencionada. As figuras 4 e 5 ilustram a técnica de marca d´água. Cada imagem 20 é compreendida de uma série de linhas de quadro (raster_lines). Cada uma das linhas de quadro é adicionalmente dividida em elementos denominados pixéis. Cada pixel é representado por um certo número de bits. Assim, cada linha contém uma série de pixéis, cada com vários bits. Uma marca d´água é aplicada a alguns destes bits, tipicamente a um ou mais bits menos significativos. Como indicado na figura 4, a imagem digitalizada passa através de um gerador de marcas d´água 28. Este dispositivo pode ser considerado o gerador de códigos 48 mostrado na figura 3. O gerador de marcas d´água cria n bits de dados de marca d´água 26 que são

aplicados à imagem de acordo com um plano pré-determinado. Este plano está ilustrado na figura 5, onde um bit 27 da marca d´água substitui um bit 25 de conjuntos selecionados de bits de imagem original 24. Deve ser notado, que se a técnica de marca d´água for usada para autenticar a imagem, qualquer processamento de imagem que altere os dados depois de edição da marca d´água (e.g., compressão de perda (lossy_compression)), não proporcionará certeza ao processo de autenticação, que é indesejável para aplicações de alta segurança.

Se um esquema de marcação for usado, a marcação é gerada pelo servidor 10 e transmitida ao sistema cliente 1 logo antes da captura de imagem. A marcação é transmitida à câmara 6 onde é incluída no algoritmo para autenticação de imagem, de tal modo que a marcação, ou uma marcação complementar mantida somente pelo servidor em adição à chave secreta, será requerida na autenticação da imagem. Assim, para uma imagem ser reconhecida pelo servidor como válida, a imagem não pode ser alterada de nenhuma forma depois de deixar a câmara, e a imagem deve incluir dentro da assinatura digital, a marcação válida da transação.

Devido à marcação ser gerada e conhecida pelo servidor, e uma vez que cada transação possui uma única marcação associada e incorporada, imagens são asseguradas somente para uma única transação e não poderão ser reutilizadas. Também, uma vez que o servidor gera uma marcação e inicia captura de imagem, o servidor pode estabelecer um prazo além do qual as marcações expiram. Na verdade, o esquema de prazo, não precisa de marcações; uma vez que a transação é temporizada e há uma janela de tempo para o cliente enviar a imagem de volta para o servidor, então alguma proteção é provida. A marcação meramente torna a substituição de dados mais difícil, uma vez que fica mais fácil acompanhar imagens e transações. Uma vez que o servidor é o único sistema de computador a gerar marcações, iniciar comando de captura, e manter prazo, não há necessidade de sincronismo entre os sistemas

cliente e servidor. No entanto, uma marca de tempo pode ser incluída nos algoritmos para gerar marcação, ou a marcação por si mesma pode incluir alguma representação de tempo. A despeito do algoritmo, a unicidade de cada marcação deve ser mantida ou a segurança poderá vir a ser comprometida em alguns casos.

Um outra variação possível da implementação do esquema de marcação envolve gerar valores únicos que funcionam como chaves para um algoritmo de assinatura digital usando uma chave ou diversas chaves. Isto é ligeiramente diferente de uma implementação na qual o gerador de marcações gera blocos únicos de dados, uma vez que o gerador de marcações deve gerar chaves únicas, porém válidas. Isto oferece a capacidade de usar algoritmos de assinatura digital assimétricos. No caso de algoritmos simétricos, somente uma marcação, ou chave, é usada para ambos, assinatura de cliente e verificação de servidor. No caso de algoritmos assimétricos, são geradas duas marcações ou chaves. A primeira chave é enviada para a câmara, e a segunda chave, ou chave complementar, é mantida no servidor. Este último método provê maior segurança, uma vez que a chave nunca sai do servidor seguro.

Um dispositivo de aquisição, que inclui uma autenticação de imagem segura, pode ser melhorada incluindo chaves individualizadas no software/ software incorporado/ hardware do sistema. Um esquema possível seria incorporar pares de chaves assimétricas à câmara junto com o número de série único da câmara. Cada par de chaves seriam únicos, e seriam gerados e incorporados à câmara no instante de sua fabricação dentro de uma facilidade segura. Este tipo de sistema está mostrado pelo diagrama da figura 8.

A figura 6 mostra como sistemas cliente e servidor se conectam. Na figura 6 há vários sistemas cliente 1a, 1b, até 1n. Cada sistema cliente possui um computador hospedeiro 2, e um sistema formador de imagem 4 associado que inclui uma câmara. Os sistemas cliente podem ser

conectados a um dentre muitos sistemas servidores de autenticação 10a, 10b até 10n. Estes servidores podem ser associados a outros sistemas de computador que realizam transações bancárias em rede. Outros servidores de autenticação podem ser associados a fornecedores cujos serviços podem ser comprados através da rede 9. Esta rede muito provavelmente é a Internet, mas também poderia ser uma outra rede pública, tal como um sistema telefônico ou um sistema de transmissão por satélite. Quando o servidor selecionado recebe uma solicitação de acesso a partir de um cliente, envia uma consulta de uma das chaves, chave pública, para uma autoridade de certificação de câmara 30, que contém todas as chaves públicas de todas as câmaras. A consulta contém o número de série reportado pela câmara. A chave pública pode ser usada para determinar se uma câmara em particular "assinou" a imagem recebida pelo servidor usando a mesma chave privada interna da câmara. Uma vez que a imagem tenha sido assinada na câmara usando a chave privada, o servidor de autenticação é capaz de usar a chave pública para determinar irrefutavelmente que uma dada câmara produziu a imagem em questão. Adicionalmente, usando "Autoridade de Certificação" de câmara, câmaras individuais poderão ser temporariamente ou permanentemente desabilitadas, ativando ou alterando uma particular chave pública armazenada na câmara. Desta maneira, se for considerado que uma certa câmara tenha sido comprometida, a mesma poderá ser marcada como não válida pela autoridade de certificação e o certificado revogado. Daí, o servidor de autenticação não terá capacidade de validar quaisquer imagens "assinadas" a partir desta câmara em particular, ou seja, para todos os efeitos, desabilita a mesma.

Dois cenários entre servidor e cliente estão ilustrados nas figuras 7 e 8.

O primeiro cenário operacional, mostrado na figura 7, é uma transação na qual o servidor de autenticação funciona como "porteiro". O servidor de autenticação permite

acesso aos dados ou a serviços somente a pessoas autorizadas. Por exemplo, aplicações bancárias (banking) em rede (on_line), que requerem identificação biométrica para prover identificação positiva e funcionalidade de transferência para altos valores monetários, experimentaria tal intercâmbio. Esta solução ilustra o uso de um método que implementa um protocolo de câmbio baseado em marcações únicas por transação. Neste exemplo, a chave secreta incorporada em cada câmara é a mesma chave para todas as câmaras, e esta chave secreta é conhecida pelo servidor de autenticação.

O segundo cenário operacional, mostrado na figura 8, é uma transação similar à primeira; entretanto, cada câmara possui uma chave secreta única e um número de série único. Para cada chave incorporada na câmara, há uma chave pública complementar armazenada em um banco de dados central seguro que atua como "Autoridade de Certificação" de câmara que permite ao sistema identificar a fonte de cada imagem.

Referindo-se à figura 7, a transação começa quando o sistema cliente 1 pede acesso a um recurso protegido pelo computador servidor 10. Por exemplo, uma pessoa deseja usar seu computador 2 para acessar telas de transferência de valores que permite a pessoa deslocar fundos de seu banco para outras contas. Pode se tratar de transferência da conta de aplicação para conta corrente ou pagamento de contas, transferindo fundos para a conta de um de seus fornecedores. O servidor de autenticação 10 tem um operador de solicitações 12 que recebe a consulta. Quando recebe o pedido, o computador servidor de autenticação 10 inicia uma transação de segurança para no fim prover acesso ao recurso protegido. O servidor, como parte da transação, gera uma marcação única, ou conjunto de marcações únicas, uma das quais é enviada de volta para o cliente. As marcações são criadas por um gerador de marcações 13 e podem ser geradas em conseqüência de um gerador de números randômicos, um gerador de chaves

randômicas, um número de transação único, uma marca de tempo, ou uma combinação dos mesmos.

O computador cliente recebe a marcação, e envia a mesma para o sistema formador de imagem 4 conectado ao computador de cliente 2. O sistema formador de imagem contém uma câmara 6, que tem uma chave secreta indicada pelo ícone de chave. A câmara então é instruída a gerar uma imagem segura. A câmara aceita a marcação, captura uma imagem, e usa um algoritmo de assinatura digital que utiliza imagem, marcação, e chave secreta da câmara como parâmetros para prover uma assinatura digital desta imagem em particular. A câmara transmite a imagem segura para o computador de cliente 2. O computador de cliente, o qual pode ou não proceder a algum processamento na imagem, e por fim envia a imagem ao servidor 10 através da rede 9. Transmitida junto com a imagem segue a assinatura digital, quer incorporada diretamente na imagem ou contígua à mesma no pacote de dados enviado para o servidor. O servidor verifica que a imagem não foi corrompida computando a mesma ou usando o algoritmo de assinatura digital complementar sobre os dados, usando conhecimento de marcação ou marcação complementar, respectivamente, junto com uma cópia do servidor da chave secreta. Isto é realizado pelo módulo de autenticação de imagem 15 no qual a assinatura digital computada é comparada à assinatura digital do cliente. O módulo de autenticação contém ou recebe a partir de um outro componente no sistema servidor de autenticação informação que permite reconhecer chave a partir da câmara segura indicada pelo símbolo de chave colocado na caixa 15. Se os resultados conferem, a imagem recebida será considerada válida e pertencente à esta particular transação. O servidor então poderá obter imagem e realizar identificação biométrica, como se mostra na caixa 16. Passando identificação biométrica, o cliente obtém acesso ao recurso seguro, o que se mostra na caixa 17. Um registro da transação pode ser anotado pelo

sistema servidor, que pode conter, entre outros, dados seguros da imagem original originalmente enviados pelo cliente. Estes dados podem prover evidência irrefutável da transação, se requeridos.

Preferimos anotar cada etapa da transação. Também preferimos prover um temporizador 18 que é usado para verificar dados com marca de tempo assim como para registrar o instante de cada transação.

O segundo exemplo de transação está diagramado na figura 8. Como no primeiro exemplo, um sistema cliente 1 é conectado a um sistema servidor de autenticação 10 através de uma rede 9. Durante fabricação da câmara, uma chave pública, uma chave privada, e um número de série são designados para cada câmara dentro de uma facilidade segura. A chave pública e o número de série são introduzidos em um banco de dados central acessível por um computador servidor que atua como autoridade de certificação de câmara 30. A chave privada e o número de série estão programados na câmara. Esta chave privada é a chave secreta para a câmara. Um sistema formador de imagens contendo a câmara é conectado a um computador cliente 2 e as transações podem prosseguir.

A transação começa quando o sistema cliente 2 pede acesso a um recurso protegido pelo computador servidor 10. Por exemplo, uma pessoa deseja acessar uma tela de transferência de valores em seu computador. O computador servidor de autenticação 10, recebendo a solicitação através do operador de pedidos, inicia transação de segurança para, finalmente, prover acesso ao recurso protegido. O servidor, como parte da transação, gera marcação, ou marcações, usando o gerador de marcações 13, uma das quais é enviada de volta para o sistema cliente 1. Como no exemplo anterior, as marcações podem ser geradas em conseqüência de um gerador de números randômicos, um gerador de chaves randômicas, um número de transação único, uma marca de tempo, ou uma combinação dos mesmos. O computador cliente recebe a marcação e

envia a mesma para a câmara que então é instruída a gerar uma imagem segura. A câmara aceita a marcação, captura uma imagem, e usa um algoritmo de assinatura digital que toma a imagem, a marcação, e a chave privada única como parâmetros para prover uma assinatura digital para aquela imagem em particular. A câmara transmite a imagem segura para o cliente, junto com o número de série da câmara. O cliente, que pode ou não introduzir algum processamento à imagem, envia a imagem ao servidor 10. Transmitido junto com a imagem segue a assinatura digital e o número de série único da câmara, quer incorporados à imagem ou contíguos à mesma no pacote de dados enviado ao servidor. O servidor de autenticação extrai o número de série da câmara do pacote de dados enviado pelo cliente, como indicado na caixa 14. E, então, envia o número de série à autoridade de certificação de câmara 30 que levanta a chave pública daquela câmara. A chave pública então é enviada de volta para o servidor de autenticação. Usando o módulo 15, o servidor verifica se a imagem não foi corrompida por computação ou através de um algoritmo de assinatura digital complementar sobre os dados usando a marcação ou uma marcação complementar, respectivamente junto com a chave pública provida pela "Autoridade de Certificação" de câmara 30. O resultado dos algoritmos é verificado contra assinatura digital do cliente, e se o resultado for compatível, a imagem recebida será considerada válida e pertencente àquela particular transação, e reconhecida ter sido gerada por uma câmara em particular identificada pelo número de série. O servidor pode então tomar a imagem e realizar identificação biométrica indicada pela caixa 16. Passando identificação biométrica, o cliente obtém acesso ao recurso seguro, o que se mostra na caixa 17. Um registro da transação pode ser anotado pelo sistema servidor, que pode conter, entre outras coisas, dados originais seguros de imagem originalmente enviados pelo cliente. Estes dados podem prover uma evidência irrefutável da

transação, se requerida.

Em algumas aplicações, um código anexado aos dados poderá ser considerado não suficientemente seguro, uma vez que os dados potencialmente podem ter sido vistos por pessoas ou organizações não autorizadas. Neste caso, é possível incluir um esquema de codificação de modo que depois de o código ter sido gerado ambos, dados e códigos são codificados em um pacote de dados antes de serem transmitidos, do cliente para o servidor. O servidor então decodifica o pacote de dados codificados antes de autenticar os dados com o código. Aqueles habilitados na técnica reconhecerão que há uma variedade de técnicas de codificação e decodificação válidas com vários níveis de segurança que pode ser usada para realizar esta tarefa.

Há também outras possíveis variações para os esquemas propostos acima, mas o princípio geral de usar um esquema de autenticação digital para imagens seguras usadas para verificações e identificações biométricas contra substituição e/ou corrupção é consistente para todos os esquemas.

Embora tenhamos mostrado certas configurações preferidas de nossos método e aparelho, deve ser entendido que nossa invenção não se limita a estas configurações, mas pode ser configurada de várias maneiras dentro do escopo das reivindicações que se seguem.

REIVINDICAÇÕES

1- Aparelho para coletar e transmitir dados biométricos através de uma rede, compreendendo:

- um sensor (41) para coletar dados biométricos, sendo que este sensor possui um identificador único;

- um digitalizador (42) conectado ao sensor (41) para converter dados biométricos, coletados pelo sensor (41) para um arquivo digital;

- um meio combinante (48) para criar um pacote de dados que inclui o arquivo digital e a assinatura digital; e

- uma interface de saída (49) conectada ao meio combinante (48) e arranjada para transmitir um pacote de dados para uma rede, o citado aparelho sendo caracterizado pelo fato de compreender ainda:

- uma interface (49) arranjada para transmitir um pedido a um servidor de autenticação (10) e receber a marcação (token) do servidor de autenticação (10), em resposta ao pedido; e

- um gerador de códigos para criar uma assinatura digital usando o arquivo digital, o identificador único e a marcação como parâmetros.

2- Aparelho, de acordo com a reivindicação 1, caracterizado pelo fato de o arquivo digital ser uma memória ou um depósito de quadros (43).

3- Aparelho, de acordo com a reivindicação 1, caracterizado pelo fato de também compreender um compressor para comprimir a imagem.

4- Aparelho, de acordo com a reivindicação 1, caracterizado pelo fato de também compreender um debulhador (cropper)(46) conectado à memória (43) para reduzir o tamanho da imagem na memória antes da compressão.

5- Aparelho, de acordo com a reivindicação 1, caracterizado pelo fato de o sensor (41) ser uma câmara (30).

6- Aparelho, de acordo com a reivindicação 5, caracterizado pelo fato de a câmara(30) ser um

dispositivo formador de imagem bi-dimensional.

7- Aparelho, de acordo com a reivindicação 6, caracterizado pelo fato de o dispositivo formador de imagem ser um dispositivo CCD ou CMOS.

8- Aparelho, de acordo com a reivindicação 1, caracterizado pelo fato de o gerador de códigos criar um código que é selecionado a partir do grupo que consiste de marcas d´água, assinaturas digitais, chaves de codificação, códigos pré-existentes no arquivo digital, e códigos anexados ao arquivo digital.

9- Aparelho, de acordo com a reivindicação 1, caracterizado pelo fato de também compreender um pacote resistente a falsificação (50) no qual estão contidos sensor (41), gerador de códigos meio combinante (48), e interface de saída (49).

10- Aparelho, de acordo com a reivindicação 9, caracterizado pelo fato de também compreender um interruptor (51), que será ativado se o pacote resistente a falsificação (50) for aberto.

11- Aparelho, de acordo com a reivindicação 10, caracterizado pelo fato de a ativação do interruptor (51) conduzir o aparelho (1) para um estado de não-funcionamento.

12- Aparelho, de acordo com a reivindicação 1, caracterizado pelo fato de também compreender um microcomputador (2) conectado à interface de saída (49).

13- Aparelho, de acordo com a reivindicação 1, caracterizado pelo fato de também compreender um processador incorporado conectado à interface de saída (49).

14- Método para coletar e transmitir dados biométricos através de uma rede, para um servidor de autenticação, caracterizado pelo fato de compreender:

a) transmitir um pedido ao servidor de autenticação (10) e receber, em resposta ao pedido, uma marcação do servidor de autenticação;

b) adquirir informações biométricas de um sensor (41)

tendo um identificador único;

c) converter as informações biométricas para um arquivo digital biométrico;

d) criar uma assinatura digital usando o arquivo digital, o identificador único e a marcação como parâmetros;

e) combinar o arquivo digital e a assinatura digital em um pacote de dados;

f) transmitir o pacote de dados através de uma rede para um servidor de autenticação (10).

15- Método, de acordo com a reivindicação 14, caracterizado pelo fato de também converter o arquivo digital biométrico para um modelo biométrico.

16- Método, de acordo com a reivindicação 15, caracterizado pelo fato de também compreender, no servidor:

a) comparar o modelo biométrico a um modelo biométrico armazenado; e

b) permitir ou recusar acesso a um recurso seguro com base em tal comparação.

17- Método, de acordo com a reivindicação 14, caracterizado pelo fato de a rede (9) compreender Internet.

18- Método, de acordo com a reivindicação 14, caracterizado pelo fato de também compreender pelo menos uma das etapas de cortar o arquivo digital e comprimir o arquivo digital antes de transmiti-los.

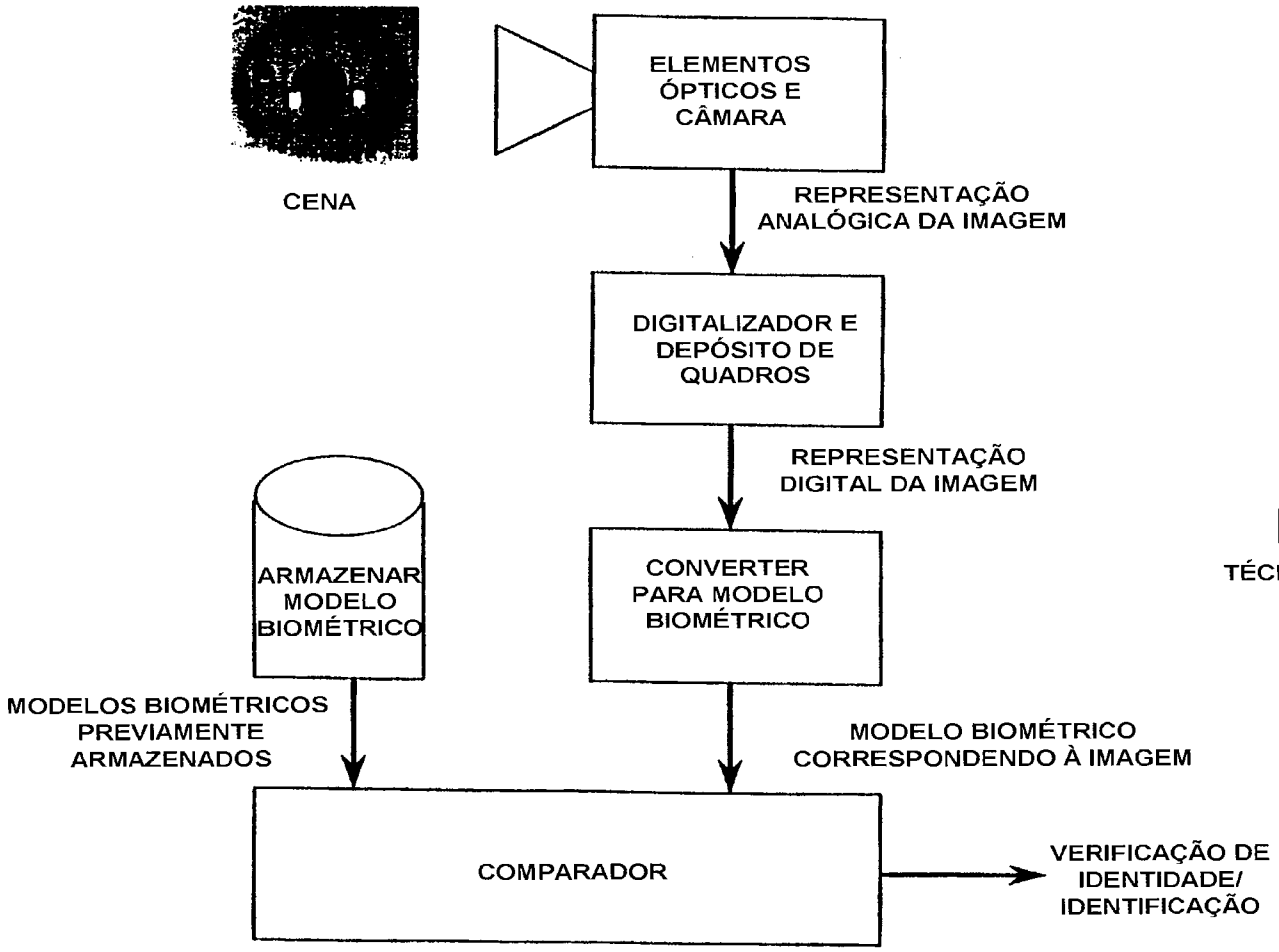


FIG.1
TÉCNICA ANTERIOR

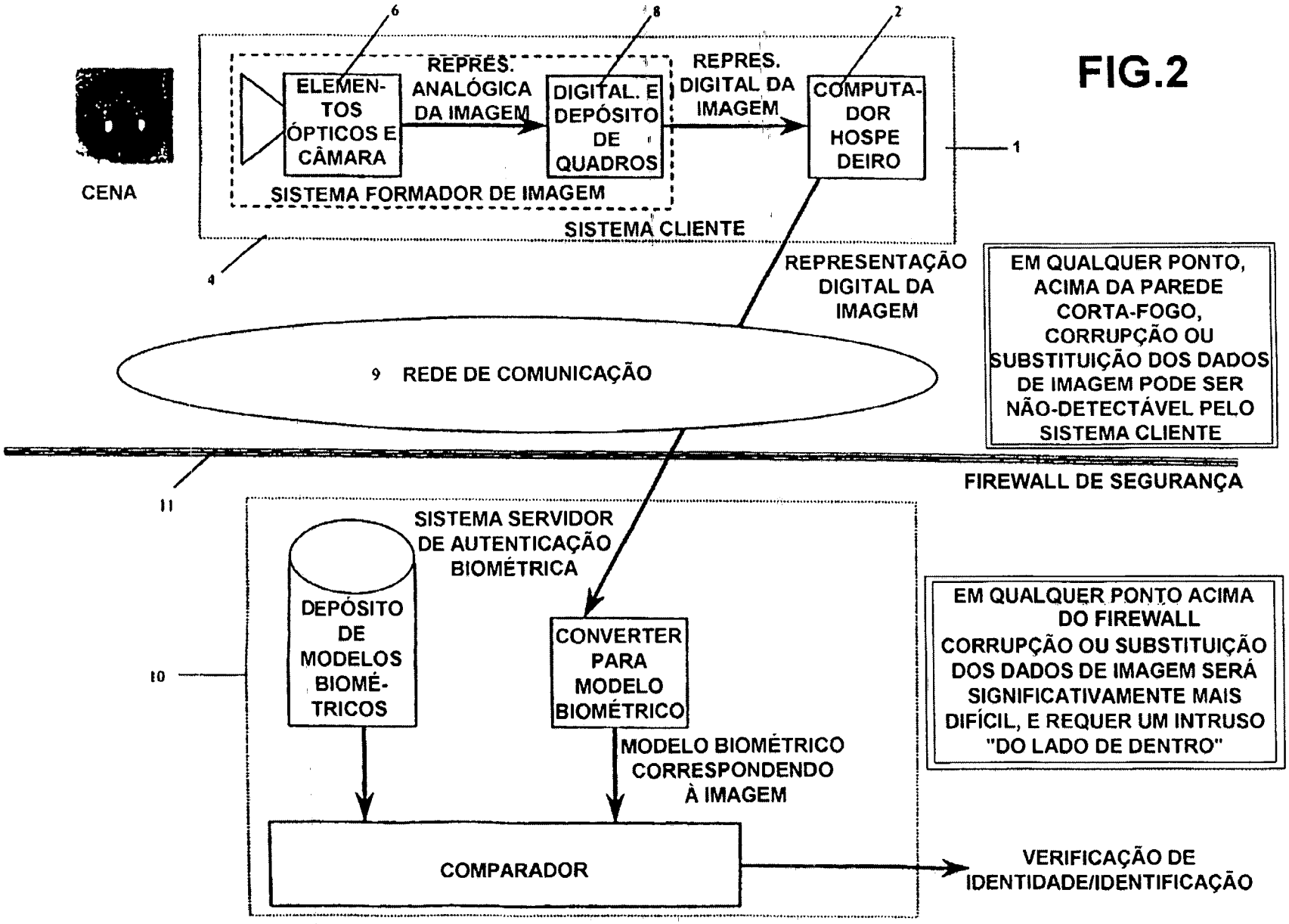

6
8
2
ELEMEN-
TOS
ÓPTICOS E
CÂMARA
REPRES.
ANALÓGICA
DA IMAGEM
DIGITAL. E
DEPÓSITO
DE
QUADROS
REPRES.
DIGITAL DA
IMAGEM
COMPUTA-
DOR
HOSPE
DEIRO
1
CENA
SISTEMA FORMADOR DE IMAGEM
SISTEMA CLIENTE
4
REPRESENTAÇÃO
DIGITAL DA
IMAGEM
EM QUALQUER PONTO,
ACIMA DA PAREDE
CORTA-FOGO,
CORRUPÇÃO OU
SUBSTITUIÇÃO DOS DADOS
DE IMAGEM PODE SER
NÃO-DETECTÁVEL PELO
SISTEMA CLIENTE
9 REDE DE COMUNICAÇÃO
FIREWALL DE SEGURANÇA
11
SISTEMA SERVIDOR
DE AUTENTICAÇÃO
BIOMÉTRICA
DEPÓSITO
DE
MODELOS
BIOMÉ-
TRICOS
CONVERTER
PARA
MODELO
BIOMÉTRICO
10
MODELO BIOMÉTRICO
CORRESPONDENDO
À IMAGEM
EM QUALQUER PONTO ACIMA
DO FIREWALL
CORRUPÇÃO OU SUBSTITUIÇÃO
DOS DADOS DE IMAGEM SERÁ
SIGNIFICATIVAMENTE MAIS
DIFÍCIL, E REQUER UM INTRUSO
"DO LADO DE DENTRO"
COMPARADOR
VERIFICAÇÃO DE
IDENTIDADE/IDENTIFICAÇÃO

FIG.2

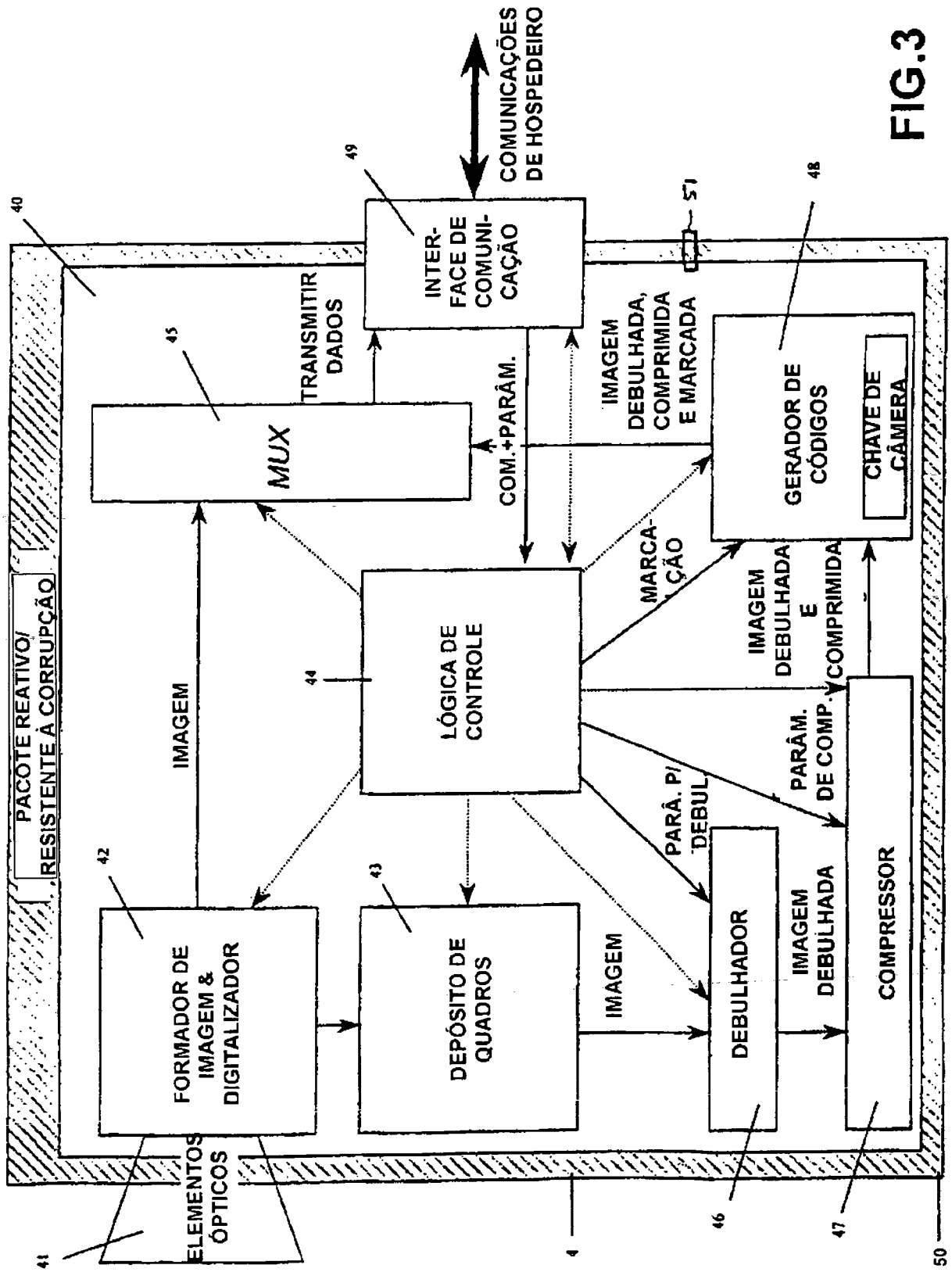

COMUNICAÇÕES DE HOSPEDEIRO
INTER-FACE DE COMUNI-CAÇÃO
TRANSMITIR DADOS
MUX
COM.+PARÂM.
IMAGEM DEBULHADA, COMPRIMIDA E MARCADA
GERADOR DE CÓDIGOS
CHAVE DE CÂMERA
MARCA-ÇÃO
IMAGEM DEBULHADA E COMPRIMIDA
LÓGICA DE CONTROLE
IMAGEM
PARÂM. DE COMP.
PARÂ. P/ DEBUL
FORMADOR DE IMAGEM & DIGITALIZADOR
DEPÓSITO DE QUADROS
IMAGEM
DEBULHADOR
IMAGEM DEBULHADA
COMPRESSOR
ELEMENTOS ÓPTICOS
PACOTE REATIVO/ RESISTENTE À CORRUPÇÃO
40
41
42
43
44
45
46
47
48
49
50
51

FIG.3

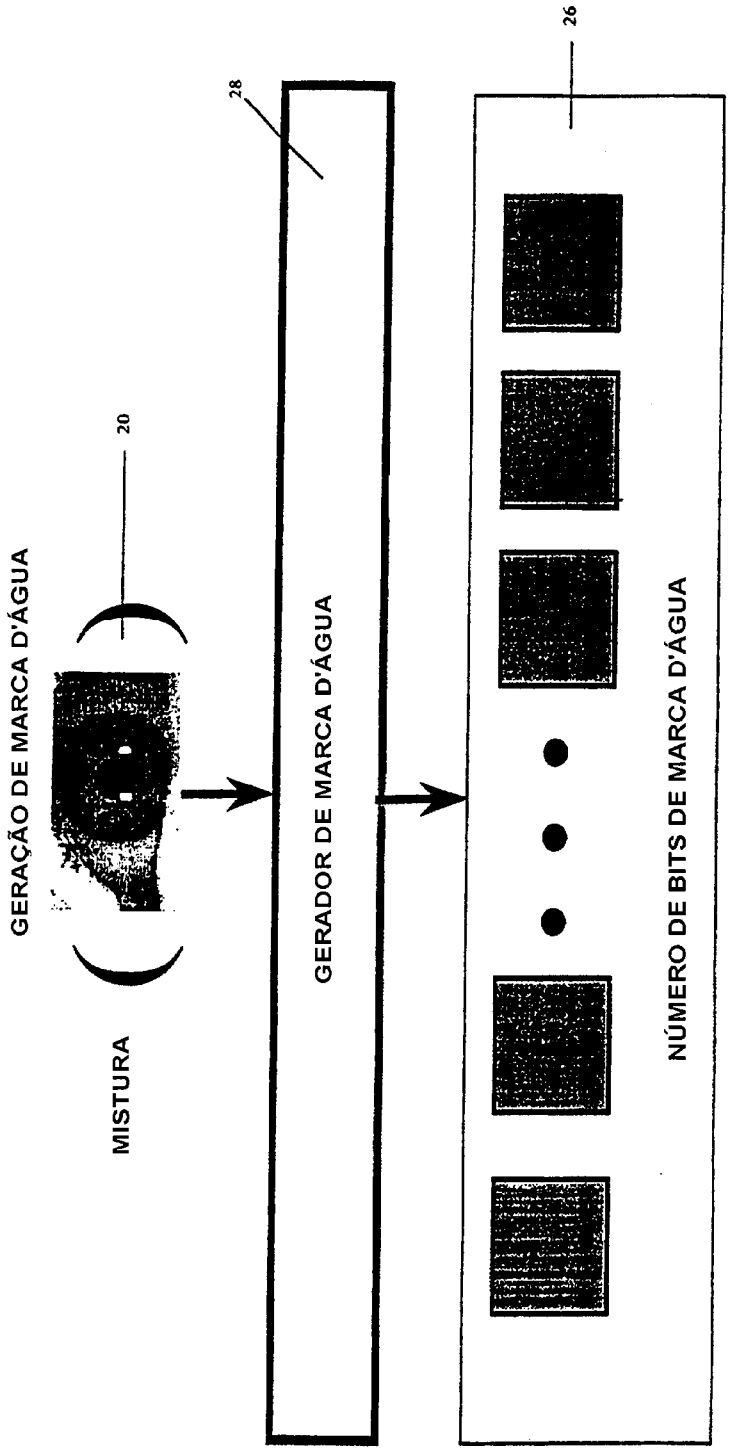

GERAÇÃO DE MARCA D'ÁGUA
20
MISTURA
GERADOR DE MARCA D'ÁGUA
28
26
NÚMERO DE BITS DE MARCA D'ÁGUA

FIG.4

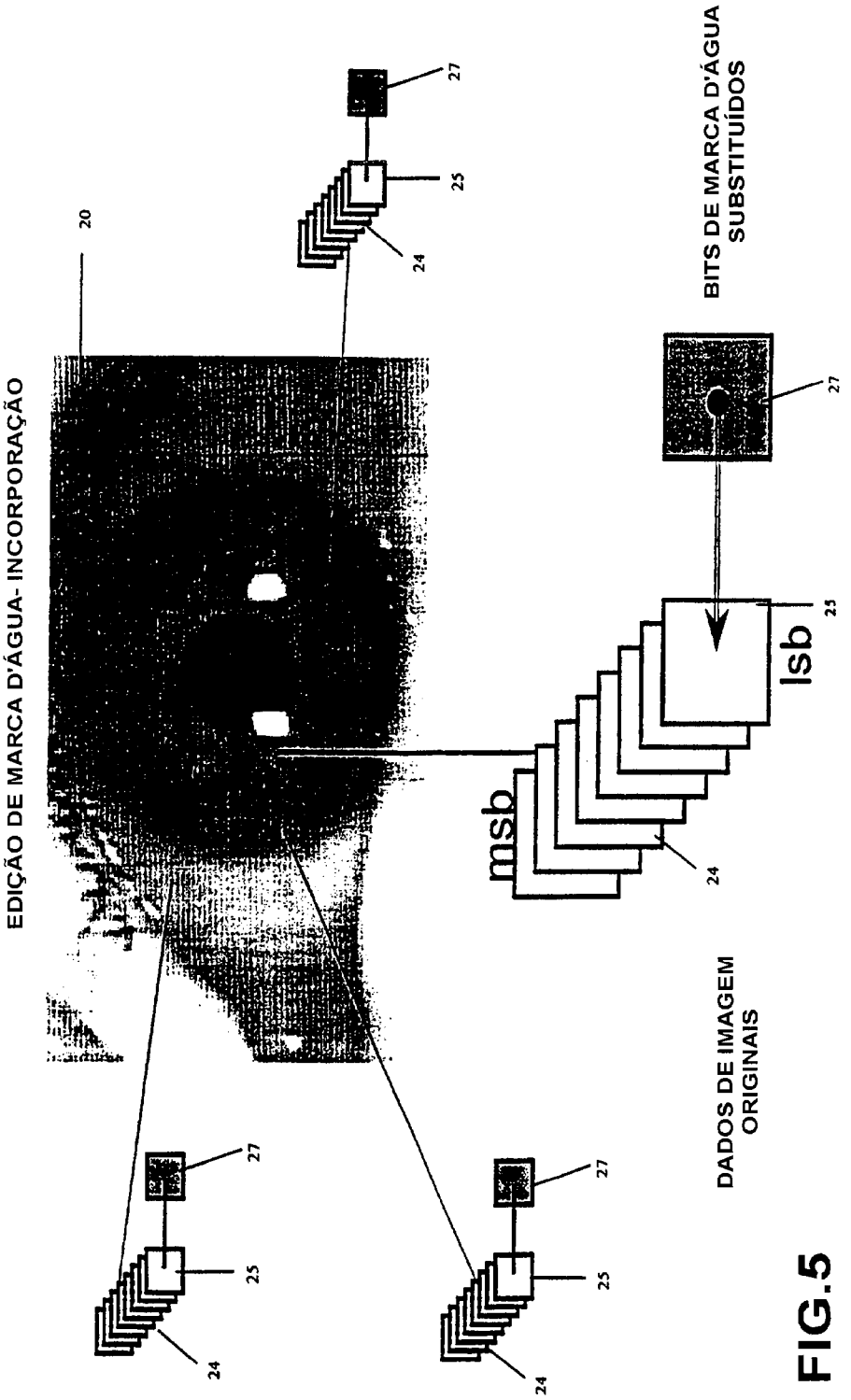

EDIÇÃO DE MARCA D'ÁGUA- INCORPORAÇÃO
20
27
25
24
BITS DE MARCA D'ÁGUA SUBSTITUÍDOS
msb
lsb
DADOS DE IMAGEM ORIGINAIS

FIG.5

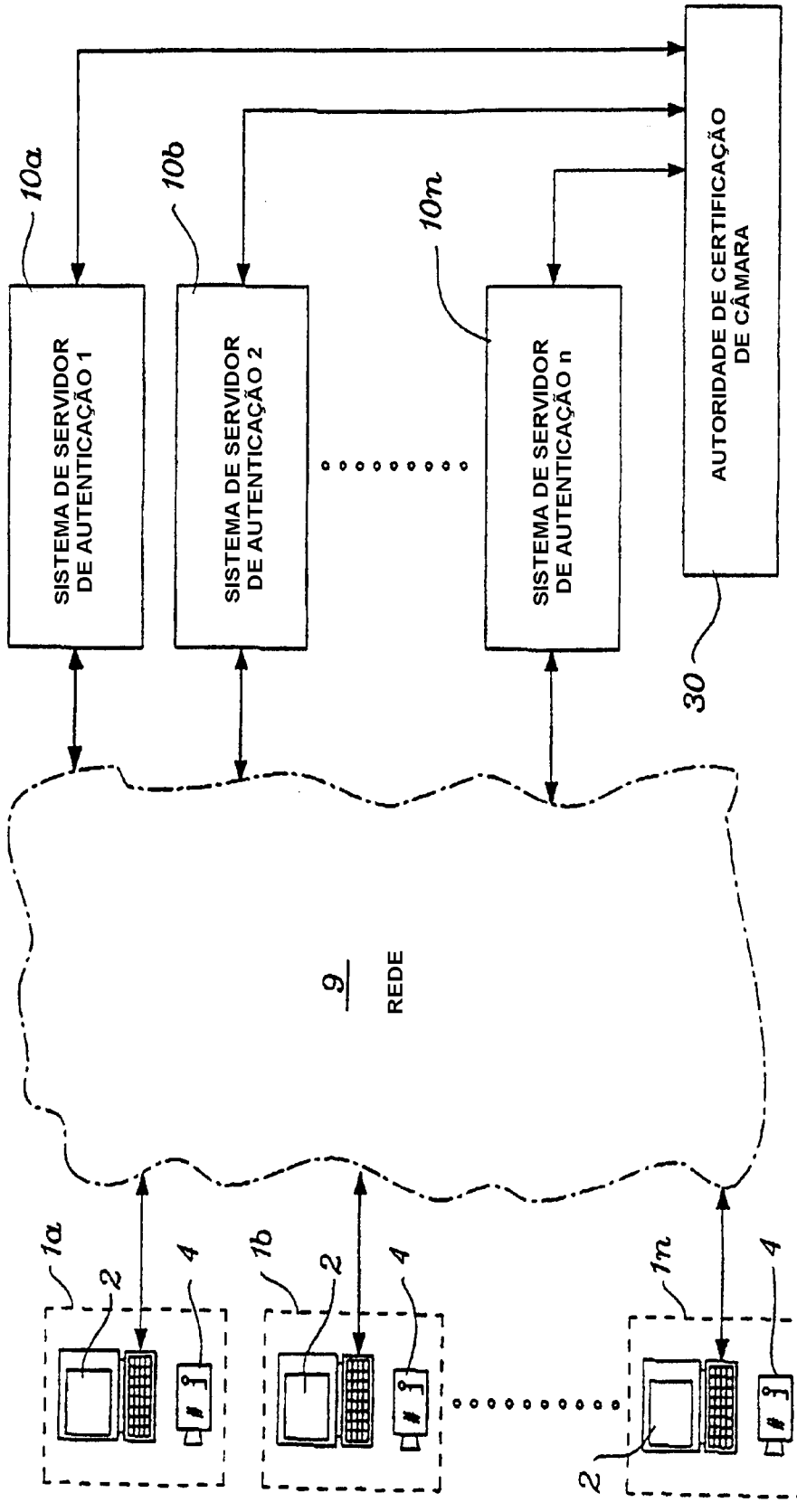

10a
10b
10n
SISTEMA DE SERVIDOR DE AUTENTICAÇÃO 1
SISTEMA DE SERVIDOR DE AUTENTICAÇÃO 2
SISTEMA DE SERVIDOR DE AUTENTICAÇÃO n
AUTORIDADE DE CERTIFICAÇÃO DE CÂMARA
30
9
REDE
1a
1b
1n
2
4

FIG.6

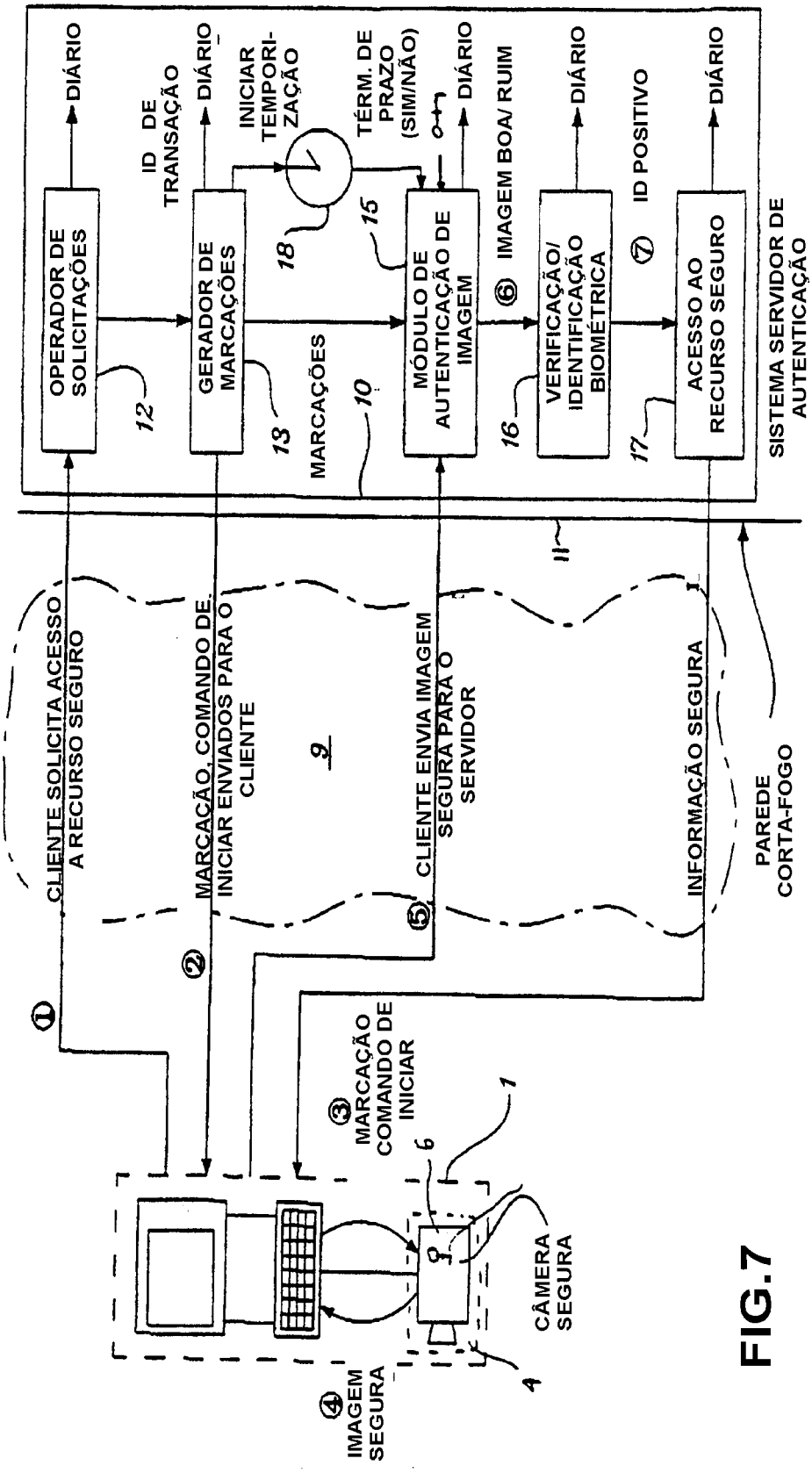
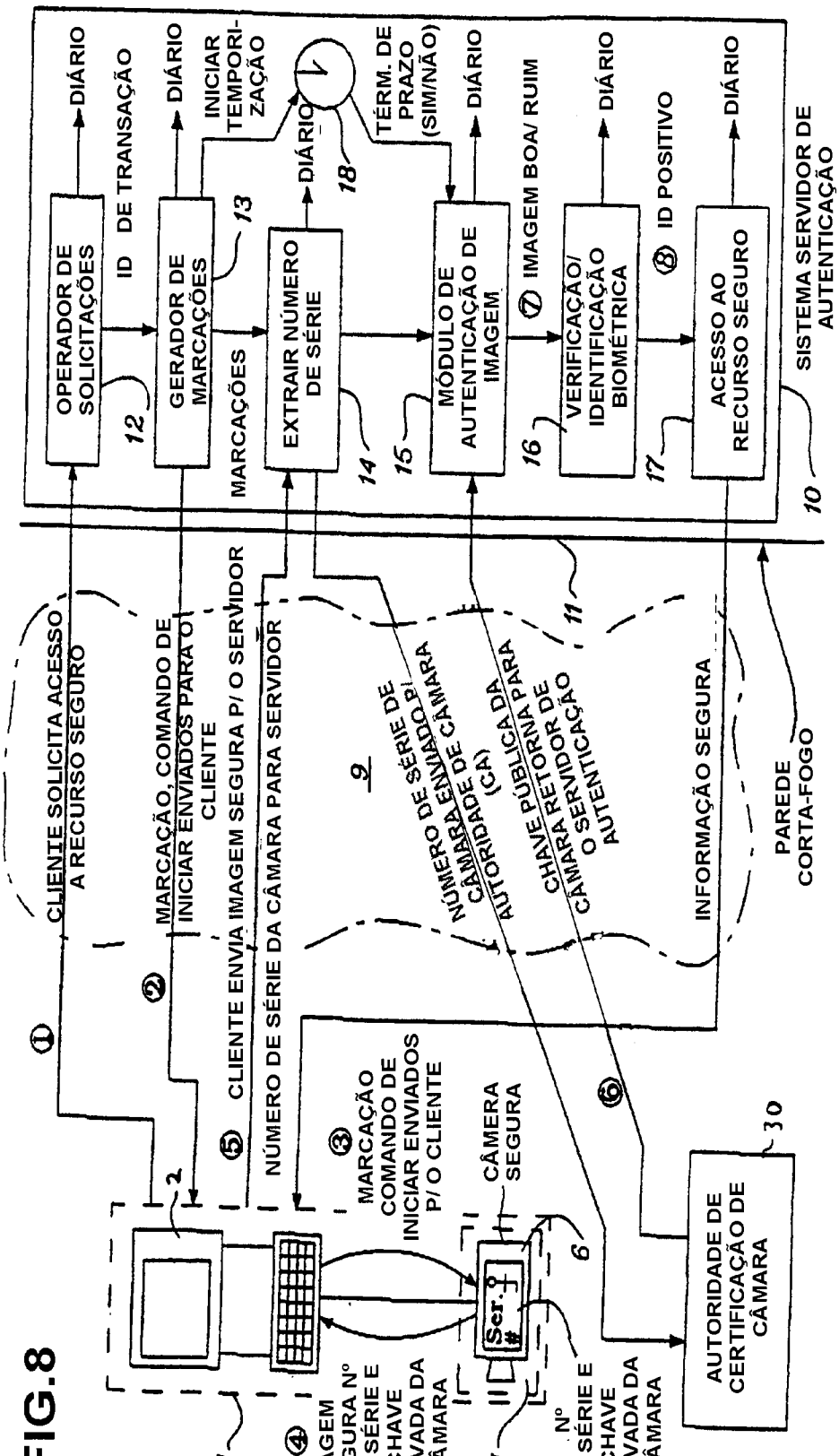

SISTEMA SERVIDOR DE AUTENTICAÇÃO
OPERADOR DE SOLICITAÇÕES
GERADOR DE MARCAÇÕES
MÓDULO DE AUTENTICAÇÃO DE IMAGEM
VERIFICAÇÃO/ IDENTIFICAÇÃO BIOMÉTRICA
ACESSO AO RECURSO SEGURO
DIÁRIO
ID DE TRANSAÇÃO
INICIAR TEMPORIZAÇÃO
TÉRM. DE PRAZO (SIM/NÃO)
IMAGEM BOA/ RUIM
ID POSITIVO
MARCAÇÕES
12
13
10
15
16
17
18
11
9
CLIENTE SOLICITA ACESSO A RECURSO SEGURO
MARCAÇÃO, COMANDO DE INICIAR ENVIADOS PARA O CLIENTE
CLIENTE ENVIA IMAGEM SEGURA PARA O SERVIDOR
INFORMAÇÃO SEGURA
PAREDE CORTA-FOGO
MARCAÇÃO COMANDO DE INICIAR
IMAGEM SEGURA
CÂMERA SEGURA
1
2
3
4
5
6
7
8

FIG.7

FIG.8


SISTEMA SERVIDOR DE AUTENTICAÇÃO
OPERADOR DE SOLICITAÇÕES
GERADOR DE MARCAÇÕES
EXTRAIR NÚMERO DE SÉRIE
MÓDULO DE AUTENTICAÇÃO DE IMAGEM
VERIFICAÇÃO/ IDENTIFICAÇÃO BIOMÉTRICA
ACESSO AO RECURSO SEGURO
DIÁRIO
ID DE TRANSAÇÃO
INICIAR TEMPORIZAÇÃO
TÉRM. DE PRAZO (SIM/NÃO)
IMAGEM BOA/ RUIM
ID POSITIVO
MARCAÇÕES
CLIENTE SOLICITA ACESSO A RECURSO SEGURO
MARCAÇÃO, COMANDO DE INICIAR ENVIADOS PARA O CLIENTE
CLIENTE ENVIA IMAGEM SEGURA P/ O SERVIDOR
NÚMERO DE SÉRIE DA CÂMARA PARA SERVIDOR
NÚMERO DE SÉRIE DE CÂMARA ENVIADO P/ AUTORIDADE DE CÂMARA (CA)
CHAVE PÚBLICA DA CÂMARA RETORNA PARA O SERVIDOR DE AUTENTICAÇÃO
INFORMAÇÃO SEGURA
PAREDE CORTA-FOGO
MARCAÇÃO COMANDO DE INICIAR ENVIADOS P/ O CLIENTE
CÂMERA SEGURA
IMAGEM SEGURA Nº DE SÉRIE E CHAVE PRIVADA DA CÂMARA
Nº DE SÉRIE E CHAVE PRIVADA DA CÂMARA
AUTORIDADE DE CERTIFICAÇÃO DE CÂMARA
Ser. #
1
2
4
6
9
10
11
12
13
14
15
16
17
18
30

RESUMO

"APARELHO PARA COLETAR E TRANSMITIR DADOS BIOMÉTRICOS ATRAVÉS DE UMA REDE E MÉTODO PARA COLETAR E TRANSMITIR DADOS BIOMÉTRICOS ATRAVÉS DE UMA REDE"

Um método e um aparelho, para coletar e transmitir com segurança dados biométricos através de uma rede, contêm um sensor, preferivelmente uma câmara para coletar dados biométricos, e hardware e software para gerar códigos. Os dados de câmara são digitalizados e um código único, que é função dos dados de câmara digitalizados, de uma chave de segredo, e de uma marcação de transação são anexados ao arquivo digital. O código pode identificar o sensor que adquiriu as informações biométricas, o momento em que as informações biométricas foram adquiridas, ou um intervalo de tempo no qual os dados eram considerados válidos, e um código de transação único. Os dados e código são transmitidos através de uma rede para um servidor que autentica que os dados não foram alterados, recomputando os mesmos usando seu próprio conhecimento da chave de segredo e da marcação de transação que são necessários para gerar os códigos. Se os dados resultarem autênticos, o servidor então computará um modelo biométrico usando tais dados. Este modelo biométrico então será comparado ao modelo previamente definido para identificar o usuário e permitir acesso a um recurso de segurança. O sistema pode ser usado para transações bancárias ou comerciais na Internet