



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

(21) **PI0709262-8 A2**

(22) Data de Depósito: 20/03/2007
(43) Data da Publicação: 28/06/2011
(RPI 2112)



* B R P I 0 7 0 9 2 6 2 A 2 *

(51) *Int.Cl.:*
G06K 9/00 2006.01

(54) Título: **TRATAMENTO DE DADOS BIOMÉTRICOS DE UM REFERENCIAL MULTIDIRECIONAL**

(30) Prioridade Unionista: 29/03/2006 FR 0602724

(73) Titular(es): Sagem Securite

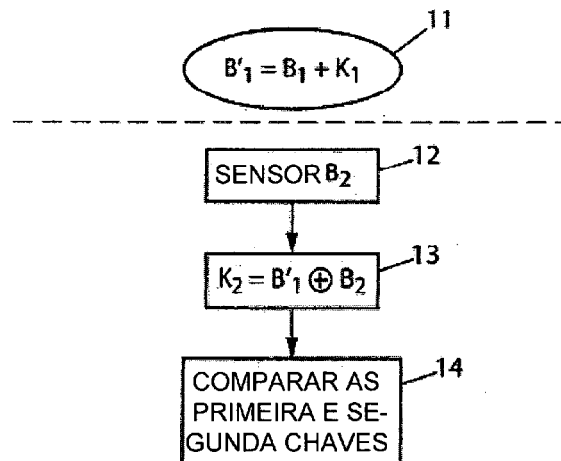
(72) Inventor(es): Hervé Chabanne , Julien Bringer , Martin Cottard

(74) Procurador(es): Montauray Pimenta, Machado & Lioce S/C Ltda

(86) Pedido Internacional: PCT FR2007000471 de 20/03/2007

(87) Publicação Internacional: WO WO2007/110498de
04/10/2007

(57) **Resumo:** TRATAMENTO DE DADOS BIOMÉTRICOS EM UM REFERENCIAL MULTIDIMENSIONAL. Um sistema biométrico dispõe de um conjunto de dados biométricos de referência (B'_{i}) resultante da aplicação de uma operação 'ou exclusivo' entre um primeiro conjunto de dados biométricos (B_{i}) e uma primeira chave codificada (K_{i}), e de uma informação relativa à primeira chave. Um segundo conjunto de dados biométricos (B_{2}) é obtido. Uma segunda chave codificada (K_{2}) é determinada aplicando-se uma operação 'ou exclusivo' entre o conjunto de dados biométricos de referência e o segundo conjunto de dados biométricos. A segunda chave é decodificada por decodificação iterativa. Em seguida, decide-se se os primeiro e segundo conjuntos de dados biométricos correspondem entre si comparando-se a informação relativa à primeira chave com a segunda chave. Os primeiro e segundo conjuntos de dados biométricos são expressos em um referencial multidimensional com N dimensões, os dados biométricos de acordo com pelo menos uma das referidas N dimensões sendo obtidos por aplicação de tratamentos relativamente à parte biométrica; e a primeira chave codificada é obtida por aplicação de uma codificação transformando uma palavra inicial de um comprimento determinado em uma palavra codificada no referencial multidimensional.



"TRATAMENTO DE DADOS BIOMÉTRICOS EM UM REFERENCIAL MULTIDIMENSIONAL"

A presente invenção refere-se ao tratamento de dados biométricos e, mais particularmente, ao
5 reconhecimento de dados biométricos na base de dados armazenados em memória.

Certos sistemas de controle de acesso baseiam-se em uma análise de características biométricas de uma pessoa para determinar, por exemplo, se esta última está
10 autorizada a acessar um local protegido. Uma tal análise de características biométricas é igualmente utilizada em certos sistemas de autenticação ou de identificação que visam autenticar ou identificar uma pessoa. Uma tal análise é classicamente baseada em uma comparação de dados
15 biométricos captados sobre uma pessoa em processo de controle com dados armazenados em uma base de dados.

Assim, por exemplo, no caso dos sistemas de controle de acesso, dados biométricos correspondendo às
20 pessoas para as quais um acesso é autorizado são armazenados em uma base de dados. Como resultado de uma etapa de comparação de dados captados sobre uma pessoa em processo de controle com dados armazenados, o sistema é dimensionado para determinar se esta pessoa faz parte daquelas para as quais um acesso é autorizado.

25 Neste tipo de sistema biométrico, esta etapa de comparação é uma etapa fundamental sobre a qual repousa a confiabilidade do sistema.

O documento 'A Fuzzy Commitment Scheme' de Juels e Wattenberg, 1999, propõe transformar esta etapa de
30 comparação em um problema clássico de decodificação. Dados biométricos b_1 previamente armazenados são comparados com dados biométricos b_2 captados sobre uma pessoa em processo

de controle. Para este fim, este documento propõe aplicar uma operação de 'ou exclusivo' nos dados biométricos b_1 destes dados com uma palavra de um código corretor de erro c . São então obtidos dados biométricos codificados f . Em
5 seguida, para comparar os dados biométricos captados b_2 com os dados biométricos b_1 , determina-se se a seguinte operação é verificada:

$$f \oplus b_2 = c \oplus e$$

na qual e é um erro apresentando um peso inferior à capacidade de correção do código.

10 No caso onde esta equação é verificada, deduz-se, então, que os dados biométricos b_1 armazenados e os dados biométricos captados b_2 se correspondem.

O documento 'Combining cryptography with biometrics effectively' de Hao Anderson e Daugman, 2005,
15 propõe aplicar este princípio geral consistindo em utilizar um código corretor de erro em uma etapa de comparação de um sistema biométrico, no caso preciso de dados biométricos correspondendo a uma íris. Dados biométricos relativos à íris são codificados em 256 octetos, formando, assim, um
20 código de íris. Previamente, um código de íris B é determinado para ser utilizado como dado de referência. Uma chave biométrica K é gerada por um gerador de números aleatórios. Esta chave biométrica K é, em seguida, codificada com um código corretor proveniente de um código
25 de Reed Solomon e de um código de Hadamard para fornecer um pseudocódigo de íris K' .

Em seguida, aplica-se a operação de 'ou exclusivo' entre o pseudocódigo de íris K' e o código de íris B representando o dado de referência para fornecer um
30 resultado R que verifica a seguinte equação:

$$R = B \oplus K'$$

Armazena-se, então, o resultado R desta última operação assim como a chave biométrica sob uma forma de Hash (hachée) H(K).

Em seguida, quando uma pessoa está em processo de controle, dados biométricos de sua íris são captados sob a forma de um código de íris captado B'.

Aplica-se, então, a operação de 'ou exclusivo' entre o resultado armazenado R e este código de íris captado B', para obter o seguinte resultado R' :

$$R' = B' \oplus R$$

Em seguida, o resultado R' é decodificado na base do código corretor utilizado precedentemente para codificar a chave biométrica K a fim de fornecer uma chave biométrica C.

Em seguida, aplica-se a mesma função de Hash (hachage) à chave biométrica C assim obtida, e compara-se a chave biométrica armazenada sob sua forma de Hash H(K) e a chave biométrica C sob sua forma de Hash H(C).

Se a seguinte equação for verificada:

$$H(K) = H(C);$$

daí se deduz que os dados biométricos captados correspondem ao dado de referência.

Dados biométricos são aqui representados por um código de íris tendo um tamanho limitado a 256 octetos.

Este código de íris é obtido por tratamento de uma imagem de íris. Ora, uma tal imagem pode apresentar características diferentes em função da exposição à luz da íris no momento da captura da imagem ou ainda em função do movimento da pessoa durante a captura da imagem de íris.

Diferentes tratamentos permitem suavizar as diferentes perturbações potenciais que podem afetar uma tal imagem.

Assim, por exemplo, é possível aplicar diferentes
5 filtros de tratamento de imagens de forma a obter uma pluralidade de níveis respectivos de informações relativamente a uma mesma imagem, permitindo, assim, enriquecer as informações relativas à íris que se trata.

A fim de suavizar as perturbações da captura de
10 imagem de íris, é igualmente possível realizar uma pluralidade de capturas de imagem de íris. Neste caso, multiplicam-se também as informações relativas à íris, e obtêm-se diferentes níveis de informações.

Cada um destes níveis de informações poderia,
15 desta forma, corresponder, no contexto do documento 'Combining cryptography with biometrics effectively', a um código de íris codificado em 256 octetos. Em seguida, para tratar esta pluralidade de níveis de informações, poder-se-ia levar a aplicar sucessivamente o método descrito no
20 documento precitado, relativamente aos diferentes níveis de informações. Desta forma, a etapa de comparação consistiria, então, em comparar sucessivamente os códigos de íris B com códigos de íris B', cada um sendo proveniente da aplicação de um filtro de uma pluralidade de filtros
25 considerados, ou ainda proveniente de uma captura de imagem de uma pluralidade de capturas de imagem realizadas.

Uma tal etapa de comparação corresponderia, então, a uma pluralidade de etapas de comparação baseada em dados de 256 octetos, apresentando, cada uma, um nível de
30 confiabilidade limitado.

A presente invenção visa melhorar o nível de confiabilidade de uma tal etapa de comparação.

Um objetivo da presente invenção visa incrementar

os desempenhos de um tratamento de dados biométricos baseado em uma comparação de um primeiro conjunto de dados biométricos com um segundo conjunto de dados biométricos para determinar se estes primeiro e segundo conjuntos de dados biométricos pertencem a uma mesma pessoa.

Mais precisamente, é proposto realizar a etapa de comparação de dados biométricos de acordo com um método que permite tratar dados biométricos representados em um referencial multidimensional, de forma a levar em conta, de maneira simultânea, no curso de uma única etapa de comparação, dados biométricos obtidos por uma pluralidade de tratamentos aplicada relativamente à parte biométrica considerada, esses tratamentos podendo ser, por exemplo, aplicações de uma pluralidade de filtros, ou ainda capturas de imagem desta parte biométrica. Assim, o nível de confiabilidade de uma tal etapa de comparação pode ser melhorado.

Um primeiro aspecto da presente invenção propõe um processo de tratamento de dados biométricos relativos a uma parte biológica, em um sistema biométrico dispendo, de um lado, de pelo menos um conjunto de dados biométricos de referência resultante da aplicação de uma operação 'ou exclusivo' entre um primeiro conjunto de dados biométricos e uma primeira chave codificada, e, de outro lado, de uma informação relativa à primeira chave.

O processo compreende as seguintes etapas:

/a/ obter um segundo conjunto de dados biométricos;

/b/ determinar uma segunda chave codificada aplicando uma operação 'ou exclusivo' entre o conjunto de dados biométricos de referência e o segundo conjunto de dados biométricos;

/c/ decodificar a segunda chave; e

/d/ decidir se o segundo conjunto de dados biométricos corresponde ao primeiro conjunto de dados biométricos comparando a informação relativa à primeira chave com a segunda chave.

5 Os primeiro e segundo conjuntos de dados biométricos são expressos em um referencial multidimensional com N dimensões, N sendo um número inteiro superior ou igual a 2, os dados biométricos de acordo com pelo menos uma das N dimensões sendo obtidos por aplicação
10 de uma pluralidade de tratamentos aplicada relativamente à parte biológica.

Além disso, a primeira chave codificada é obtida por aplicação de uma codificação transformando uma palavra inicial de um comprimento determinado em uma palavra
15 codificada no referencial multidimensional.

Graças a essas disposições, os dados biométricos manipulados podem ser expressos em um referencial multidimensional permitindo, assim, vantajosamente, levar em conta uma grande quantidade de informações relativas aos
20 dados biométricos tratados e, dessa forma, permitindo melhorar a eficácia e a confiabilidade deste tipo de processo de tratamento biométrico.

De fato, quanto maior a quantidade de informações pertinentes tratadas simultaneamente, mais elevado é o
25 nível de confiabilidade, associado à comparação com dados biométricos inicialmente memorizados.

Nenhuma limitação está ligada ao tipo da pluralidade de tratamentos aplicada relativamente à parte biométrica.

30 Como os dados são manipulados em um referencial multidimensional, é aqui possível considerar, de maneira simultânea, dados biométricos relativos a uma imagem tratada, por exemplo, de acordo com um primeiro filtro e

dados biométricos relativos a uma imagem tratada de acordo com pelo menos segundo filtro, esses filtros sendo filtros de mesmo tipo que pertencem a uma mesma família de filtros.

5 Pode-se igualmente prever tratar aqui uma pluralidade de famílias de filtros. Neste caso, cada família de filtros suplementar pode induzir, então, uma dimensão suplementar no referencial multidimensional de dimensão N.

10 Assim, em um modo de realização da presente invenção, os dados biométricos de acordo com pelo menos uma dimensão são obtidos aplicando-se uma pluralidade de filtros a uma imagem da parte biométrica.

15 É também possível considerar, de maneira simultânea, dados biométricos provenientes de capturas de imagem diferentes da parte biométrica considerada.

 Assim, em um modo de realização da presente invenção, os dados biométricos de acordo com pelo menos uma dimensão são obtidos capturando-se uma pluralidade de imagens da parte biométrica.

20 Em uma variante, o referencial multidimensional considerado compreende pelo menos uma dimensão relativa à pluralidade de capturas de imagem realizada para a parte biométrica considerada e pelo menos uma outra dimensão relativa à aplicação de uma pluralidade de filtros aplicada
25 à pluralidade de imagens capturada.

 Pode-se igualmente prever, vantajosamente, que pelo menos uma dimensão do referencial multidimensional de acordo com um modo de realização da presente invenção corresponde a dados biométricos obtidos fazendo-se variar
30 pelo menos uma característica condicionando o contexto da captura de imagem. Assim, uma dimensão pode corresponder, por captura de imagem, a uma pluralidade de valores de luminosidade, ou uma pluralidade de valores de contraste,

ou ainda a uma variação do histograma dos níveis de cores.

Pode-se também considerar dados biométricos de acordo com pelo menos uma dimensão obtidos a partir de uma imagem captada, fazendo-se variar um limite de
5 quantificação da escrita numérica da imagem captada.

Em uma variante, pode-se prever levar em consideração uma combinação de todas essas pluralidades de tratamentos, o número de dimensões do referencial multidimensional sendo-lhe diretamente dependente.

10 Um tal processo pode vantajosamente ser implementado em qualquer sistema biométrico que é baseado em uma etapa de comparação, entre primeiros e segundos dados biométricos, destinada a determinar se esses primeiros e segundos dados biométricos pertencem a uma
15 mesma pessoa.

Em um modo de realização da presente invenção, o referencial multidimensional compreende dados de comprimento n_i de acordo com cada uma das N dimensões do referencial, i estando compreendido entre 1 e N . A
20 codificação da primeira chave pode então compreender as seguintes etapas:

- transformar a primeira chave em um outro referencial com N dimensões compreendendo dados de comprimento respectivo k_i de acordo com as N dimensões, o
25 produto dos comprimentos k_i , para i compreendido entre 1 e N , sendo igual ao comprimento determinado da primeira chave;

- aplicar sucessivamente de acordo com as N dimensões respectivamente N códigos em bloco C_i ,
30 transformando os dados de comprimento respectivo k_i em dados codificados de comprimento respectivo n_i .

A informação relativa à primeira chave pode ser obtida por aplicação de uma função de Hash na primeira

chave. Neste caso, a etapa (d) pode compreender as seguintes etapas:

- aplicar a função de Hash na segunda chave;
- comparar a segunda chave sob a forma de Hash com a informação relativa à primeira chave.

Um segundo aspecto da presente invenção propõe um dispositivo de tratamento de dados biométricos relativos a uma parte biológica em um sistema biométrico, o dispositivo de tratamento dispondo, de um lado, de pelo menos um conjunto de dados biométricos de referência resultante da aplicação de uma operação 'ou exclusivo' entre um primeiro conjunto de dados biométricos e uma primeira chave codificada, e, de outro lado, de uma informação relativa à primeira chave.

O dispositivo pode compreender:

- uma unidade de interface própria para receber um segundo conjunto de dados biométricos;
- uma unidade de determinação própria para fornecer uma segunda chave codificada aplicando uma operação 'ou exclusivo' entre o conjunto de dados biométricos de referência e o segundo conjunto de dados biométricos recebido pela referida unidade de interface;
- uma unidade de decodificação própria para decodificar a segunda chave codificada; e
- uma unidade de decisão própria para decidir se o segundo conjunto de dados biométricos corresponde ao primeiro conjunto de dados biométricos comparando a informação relativa à primeira chave com a segunda chave.

Os primeiro e segundo conjuntos de dados biométricos podem ser expressos em um referencial multidimensional com N dimensões, N sendo um número inteiro superior ou igual a 2, os dados biométricos de acordo com pelo menos uma das referidas N dimensões sendo obtidos por

aplicação de uma pluralidade de tratamentos aplicada relativamente à parte biológica.

A primeira chave codificada pode ser obtida por aplicação de uma codificação transformando uma palavra inicial de um comprimento determinado em uma palavra codificada no referencial multidimensional.

Os dados biométricos de acordo com pelo menos uma dimensão podem ser obtidos capturando-se uma pluralidade de imagens da parte biológica.

Os dados biométricos de acordo com pelo menos uma dimensão podem também ser obtidos aplicando-se uma pluralidade de filtros em uma imagem da parte biológica.

A informação relativa à primeira chave pode ser obtida por aplicação de uma função de Hash na primeira chave; e a unidade de decisão pode então compreender:

- uma unidade de Hash própria para aplicar a função de Hash na segunda chave decodificada; e
- uma unidade de comparação própria para comparar a informação relativa à primeira chave e a segunda chave sob a forma de Hash.

O conjunto de dados biométricos de referência e/ou a informação relativa à primeira chave podem estar disponíveis em uma base de dados.

Um terceiro aspecto da presente invenção propõe um sistema de tratamento de dados biométricos compreendendo um dispositivo de tratamento de dados biométricos de acordo com o segundo aspecto da presente invenção e pelo menos um sensor biométrico próprio para fornecer um segundo conjunto de dados biométricos ao referido dispositivo de tratamento de dados biométricos.

Outros aspectos, objetivos e vantagens da invenção aparecerão na leitura da descrição de um de seus modos de realização.

A invenção será igualmente melhor compreendida com o auxílio dos desenhos, nos quais:

5 - a figura 1 ilustra as principais etapas realizadas de acordo com um modo de realização da presente invenção;

- a figura 2 ilustra uma aplicação de uma codificação de acordo com um modo de realização da presente invenção; e

10 - a figura 3 ilustra uma aplicação de uma família de filtros a uma impressão digital;

- a figura 4 ilustra um dispositivo de tratamento de dados biométricos de acordo com um modo de realização da presente invenção; e

15 - a figura 5 ilustra um sistema de tratamento de dados biométricos de acordo com um modo de realização da presente invenção.

A figura 1 ilustra as principais etapas realizadas de acordo com um modo de realização da presente invenção.

20 Em uma etapa de inicialização 11, o sistema biométrico considerado dispõe de um conjunto de dados biométricos de referência B'_1 . Este conjunto de dados biométricos verifica a seguinte equação:

$$B'_1 = B_1 + K_1$$

25 onde B_1 corresponde a um primeiro conjunto de dados biométricos;

e K_1 corresponde a uma primeira chave codificada.

O primeiro conjunto de dados biométricos pode ser obtido em uma fase de inicialização clássica de um sistema biométrico deste tipo, no curso da qual são captados dados
30 biométricos correspondentes às pessoas consideradas no sistema biométrico, isto é, as pessoas para as quais um

acesso é autorizado ou uma identificação é possível ou ainda uma autenticação é possível

Em um modo de realização da presente invenção, este primeiro conjunto de dados biométricos pode ser
5 relativo a uma parte biológica correspondendo a uma impressão digital, ou ainda a uma íris. Os dados biométricos captados correspondem nesses exemplos a uma imagem em duas dimensões (2D). Este primeiro conjunto de dados biométricos pode também ser relativo a um rosto e
10 corresponder, assim, seja a uma imagem em 2D, seja ainda a uma imagem em três dimensões (3D).

No caso onde um conjunto de dados biométricos a tratar corresponde a uma imagem em 2D, e quando esta imagem é filtrada de acordo com duas famílias de filtros distintas
15 f_i e g_i , então os dados biométricos correspondentes são vantajosamente manipulados e tratados de acordo com um modo de realização da presente invenção, em um referencial com quatro dimensões.

Em uma variante, uma única família de filtros é
20 utilizada. Aqui, os dados biométricos são então vantajosamente tratados em um referencial 3D.

É, em seguida, fácil deduzir, dos exemplos enunciados logo acima, um princípio geral que é adaptado a dados biométricos captados de acordo com X dimensões e
25 filtrados respectivamente com um número Y de famílias de filtros de imagem. Neste último caso, os dados biométricos são vantajosamente tratados em um referencial com N dimensões, N verificando a seguinte equação:

$$N = X + Y$$

Qualquer que seja a parte biológica visada (íris,
30 impressão digital, rosto), em um modo de realização da presente invenção, a imagem considerada é tratada de acordo

com pelo menos uma família de filtros próprios para a parte biológica visada. Uma tal característica permite melhorar os desempenhos de um sistema biométrico desse tipo aumentando o nível de confiabilidade da tomada de decisão baseada na etapa de comparação de dados biométricos de acordo com um modo de realização da presente invenção.

Neste contexto, o primeiro conjunto de dados biométricos B_1 corresponde a dados biométricos dispostos em um referencial multidimensional do qual pelo menos uma das dimensões é relativa à aplicação de uma família de filtro sobre uma imagem da parte biológica visada.

No caso onde os dados biométricos relativos à parte biológica visada são expressos de acordo com uma dimensão, sob a forma de uma palavra de n_1 bits, n_1 sendo um número inteiro, como, por exemplo, um código de íris tal como descrito precedentemente, pode-se aplicar um processo de acordo com um modo de realização em um referencial com duas dimensões, uma primeira dimensão correspondendo aos n_1 bits da palavra codificando a parte biológica visada e uma segunda dimensão correspondendo à aplicação de uma família de filtros nesta parte biológica visada.

Aqui, um conjunto de dados biométricos pode, dessa forma, ser escrito sob a forma de uma matriz de n_1 colunas e de n_2 linhas, n_2 correspondendo ao número de filtros compreendidos na família de filtros aplicados à imagem da parte biológica visada.

A primeira chave codificada K_1 , aplicada nesta etapa 11, pode ser vantajosamente obtida gerando-se, em primeiro lugar, uma primeira chave de k bits de maneira aleatória e aplicando-se uma codificação nesses k bits que é própria para passar a partir de um referencial definido em uma dimensão e em um comprimento k ao referido referencial multidimensional.

Um código da família dos 'Códigos Turbo' pode ser adaptado a este modo de realização. Tais códigos são descritos, por exemplo, no documento EP 827284 'Processo de transmissão de bits de informações com codificação corretora de erro, codificador e decodificador para a implementação deste processo'. As seções seguintes descrevem um exemplo de aplicação de um tal Código Turbo em um modo de realização da presente invenção aplicado a um referencial com duas dimensões. É fácil de deduzir daí uma aplicação a um referencial multidimensional com N dimensões, N sendo um número qualquer superior a 2.

Mais precisamente, as seções seguintes descrevem um exemplo de um Produto de Código Turbo (TCP), baseado em um produto de dois códigos C1 e C2 de parâmetros respectivamente (n_1, k_1, d_1) e (n_2, k_2, d_2) , onde n_i (i compreendido entre 1 e 2) corresponde ao comprimento do código C_i , k_i corresponde ao número de símbolos de informação do código C_i e d_i corresponde à distância de Hamming mínima entre duas palavras quaisquer.

A figura 2 ilustra a aplicação de um tal Código Turbo na chave de k bits para obter a primeira chave codificada K_1 . A primeira chave de k bits é, em primeiro lugar, escrita sob a forma de uma matriz 21 compreendendo k_1 linhas e k_2 colunas de elementos correspondendo, cada um, a um bit da primeira chave, k_1 e k_2 verificando a seguinte equação:

$$k_1 \times k_2 = k$$

Em seguida, as k_1 linhas são, cada uma, codificadas com o código C_2 , fornecendo k_1 linhas de n_2 elementos. Obtém-se, assim, uma matriz de $k_1 \times n_2$ elemento. Em seguida, as n_2 colunas desta matriz são codificadas com o código C_1 , fornecendo n_2 colunas de n_1 elementos. Como

resultado da aplicação do Código Turbo baseado nos códigos
 em bloco C_1 e C_2 , obtém-se, então, uma matriz 23 de $n_1 \times n_2$
 elementos. Em geral, em uma tal matriz, uma parte 24
 compreende elementos de controle nas colunas permitindo
 5 controlar a validade dos k_1 primeiros elementos das k_2
 primeiras colunas desta matriz 23. Esta última compreende
 igualmente uma parte 25 de elementos de controle nas linhas
 permitindo controlar a validade dos k_2 primeiros elementos
 das k_1 primeiras linhas desta matriz, uma parte 26
 10 permitindo controlar os elementos de controle nas linhas e
 nas colunas das partes 25 e 24 respectivamente.

Assim, aplicando-se uma tal codificação na chave
 de k bits, obtém-se uma chave codificada K_1 de dimensão
 $n_1 \times n_2$.

15 Em tais condições, o sistema biométrico dispõe de
 um conjunto de dados biométricos de referência que resulta
 da aplicação de um 'ou exclusivo' entre o primeiro conjunto
 de dados biométricos B_1 e a primeira chave codificada K_1 , B_1
 e K_1 sendo expressos em um mesmo referencial
 20 multidimensional.

O processo de acordo com um modo de realização da
 presente invenção consiste, então, em uma etapa 12, em
 captar um segundo conjunto de dados biométricos B_2 , por
 exemplo, a partir de uma pessoa em processo de controle no
 25 sistema biométrico considerado.

Em seguida, em uma etapa 13, obtém-se uma segunda
 chave codificada K_2 que verifica a seguinte equação:

$$K_2 = B'_1 \oplus B_2$$

Esta última equação pode ser escrita sob a
 seguinte forma:

$$K_2 = B_1 \oplus B_2 \oplus K_1$$

No caso onde os dois conjuntos de dados biométricos B1 e B2 correspondem a uma mesma parte biológica de uma mesma pessoa, as chaves k_1 e k_2 devem igualmente se corresponder com um erro próximo.

5 Decodificando-se a segunda chave codificada K_2 , por aplicação de uma decodificação correspondendo à codificação aplicada na primeira chave para obter K_1 , obtém-se uma segunda chave. Na base de uma comparação entre a primeira chave e a segunda chave, se está, então,
10 dimensionado para determinar se os primeiro e segundo conjuntos de dados biométricos correspondem a uma mesma pessoa.

A decodificação de um dado assim codificado pode repousar em um procedimento iterativo que consiste em
15 efetuar uma decodificação das linhas seguida de uma decodificação das colunas. Uma decodificação deste tipo pode, por exemplo, ser baseada em um algoritmo de Viterbi, tal como descrito no documento G. D. Forney, "The Viterbi algorithm", Proc. *IEEE*, vol. 61, No. 3, pp. 268-278, Março
20 1973. Uma decodificação deste tipo pode igualmente ser similar àquela implementada em um "decodificador turbo" como proposto no documento EP 827284. No caso onde os dados de entrada de um tal decodificador estão em binário, a decodificação volta a encontrar a palavra de código com
25 distância de Hamming mínima. Este tipo de decodificação iterativa é bem conhecido do versado na técnica e permite alcançar um nível de desempenho elevado.

Uma tal decodificação consiste em efetuar iterativamente uma decodificação das linhas e uma
30 decodificação das colunas.

Visto que uma tal etapa de comparação é baseada em um tratamento simultâneo de uma grande quantidade de informações que compreendem notadamente dados provenientes

da aplicação de uma pluralidade de filtros em uma imagem da parte biológica considerada, esta etapa é eficaz e altamente confiável.

5 A aplicação de filtros em uma parte biológica visada permite melhorar a resistência às variações e/ou perturbações que podem mais ou menos afetar as etapas de captura de dados no curso de um tal processo.

10 Em um modo de realização da presente invenção, um conjunto de dados biométricos corresponde a uma captura da íris de uma pessoa de acordo com um método tal como aquele proposto no documento J. Daugman, 'High confidence visual recognition of persons by a test of statistical independence', IEEE Trans. Pattern Anal. Mach. Intell. 15(11)(1993) 1148-1161 e no documento J. Daugman, "The importance of being random: statistical principles of íris recognition", Pattern Recognition, Vol. 36, No. 2, pp. 279-15 291, 2003.

20 Convém notar que um modo de realização da presente invenção pode se aplicar facilmente a qualquer outra parte biométrica além da íris. As seções descrevem um exemplo de tratamento de imagem baseado em uma aplicação de filtros enunciada aqui a título ilustrativo unicamente.

25 Uma íris é aqui captada sob a forma de uma imagem infravermelha. Em seguida, esta imagem é filtrada de acordo com uma família de filtros do tipo 2D-Gabor, tais como aqueles definidos, por exemplo, no documento J. G. Gaugman, "Complete discrete 2D Gabor transforms by neural networks for image analysis and compression", IEEE Trans. Acoustics; Speech Signal Processing 36 (1988).

30 A imagem infravermelha é tratada segundo duas dimensões, por exemplo, segundo, de um lado, círculos concêntricos e, de outro lado, raios desses círculos. Assim, em tais condições, o referencial utilizado para os

conjuntos de dados biométricos é um referencial com três dimensões, correspondendo às duas dimensões de tratamento da imagem e à dimensão da família dos filtros utilizados.

Em uma variante, quando a parte biológica visada
5 corresponde a impressões digitais captadas sob a forma de uma imagem 2D, pode-se aplicar um método tal como aquele proposto no documento K. Jain, S. Prabhakar, e L. Hong, "A Multichannel Approach to Fingerprint Classification", IEEE Trans. PAttern Anal. And MAchine Intell., Vol. 21, No. 4,
10 pp. 348-359, 1999.

A figura 3 ilustra um método desse tipo. Uma imagem de impressão digital 31 é captada. Depois, um ponto de referência 32 é localizado nesta imagem. Em seguida, a partir deste ponto de referência 32, a imagem é dividida em
15 uma pluralidade de setores angulares. Depois, os setores assim definidos são normalizados, isto sendo ilustrado por uma imagem 34, antes que uma família de filtros seja aplicada respectivamente de acordo com orientações diferentes, isto sendo ilustrado por imagens 35.

A imagem é assim tratada, de um lado, de acordo com duas dimensões, e, de outro lado, de acordo com uma família de filtros. Daí resulta, neste caso igualmente, que os conjuntos de dados biométricos são vantajosamente tratados em um referencial de 3 dimensões de acordo com um
20 modo de realização da presente invenção.
25

A figura 4 ilustra um dispositivo de tratamento de dados biométricos próprio para implementar um modo de realização da presente invenção.

Um tal dispositivo de tratamento 42 compreende
30 uma unidade de interface 421 própria para receber um segundo conjunto de dados biométricos B_2 . Este segundo conjunto de dados biométricos pode, por exemplo, ser transmitido a partir de um sensor biométrico do sistema

considerado.

Este dispositivo de tratamento 42 compreende adicionalmente uma unidade de determinação 422 própria para fornecer uma segunda chave codificada K_2 aplicando uma
5 operação 'ou exclusivo' entre o conjunto de dados biométricos de referência e o segundo conjunto de dados biométricos recebido pela unidade de interface 421.

Ele compreende igualmente uma unidade de decisão 423 própria para decidir se o segundo conjunto de dados
10 biométricos B_2 corresponde ao primeiro conjunto de dados biométricos B_1 comparando a informação relativa à primeira chave com a segunda chave.

Esta comparação pode ser realizada em formas de Hash das primeiras e segundas chaves, o que permite
15 preservar a confidencialidade dessas chaves. De fato, neste contexto, a primeira chave é memorizada unicamente sob uma forma de Hash.

Em um modo de realização da presente invenção, a unidade de decisão compreende adicionalmente uma unidade de
20 decodificação 425 própria para decodificar a segunda chave codificada K_2 por aplicação de uma decodificação iterativa correspondente à codificação utilizada para obter a primeira chave K_1 .

Ela pode compreender adicionalmente uma unidade de Hash 426 própria para aplicar a função de Hash na
25 segunda chave decodificada.

O conjunto de dados biométricos de referência B'_1 e/ou a primeira chave sob a forma de Hash podem estar disponíveis em uma base de dados 424 gerada pelo
30 dispositivo de tratamento 42.

A figura 5 ilustra um sistema de tratamento de dados biométricos compreendendo um dispositivo de tratamento de dados biométricos 42 e uma pluralidade de

sensores biométricos 51 adaptados para fornecer a este dispositivo 42 um segundo conjunto de dados biométricos B_2 .

REIVINDICAÇÕES

1. Processo de tratamento de dados biométricos relativos a uma parte biológica, em um sistema biométrico dispondo, de um lado, de pelo menos um conjunto de dados biométricos de referência (B'_1) resultante da aplicação de uma operação 'ou exclusivo' entre um primeiro conjunto de dados biométricos (B_1) e uma primeira chave codificada (K_1), e, de outro lado, de uma informação relativa à primeira chave;
- o processo compreendendo as seguintes etapas:
- (a) obter um segundo conjunto de dados biométricos (B_2);
 - (b) determinar uma segunda chave codificada (K_2) aplicando uma operação 'ou exclusivo' entre o conjunto de dados biométricos de referência e o segundo conjunto de dados biométricos;
 - (c) decodificar a segunda chave; e
 - (d) decidir se o segundo conjunto de dados biométricos corresponde ao primeiro conjunto de dados biométricos comparando a informação relativa à primeira chave com a segunda chave;
- no qual os primeiro e segundo conjuntos de dados biométricos são expressos em um referencial multidimensional com N dimensões, N sendo um número inteiro superior ou igual a 2, os dados biométricos de acordo com pelo menos uma das N dimensões sendo obtidos por uma pluralidade de tratamentos aplicados relativamente à parte biológica; e
- no qual a primeira chave codificada é obtida por aplicação de uma codificação transformando uma palavra inicial de um comprimento determinado em uma palavra codificada no referencial multidimensional.

2. Processo de tratamento de dados biométricos, de acordo com a reivindicação 1, no qual os dados biométricos de acordo com pelo menos uma dimensão são obtidos capturando uma pluralidade de imagens da parte biológica.

3. Processo de tratamento de dados biométricos, de acordo com a reivindicação 1 ou 2, no qual os dados biométricos de acordo com pelo menos uma dimensão são obtidos aplicando uma pluralidade de filtros em uma imagem da parte biológica.

4. Processo de tratamento de dados biométricos, de acordo com qualquer uma das reivindicações 1 a 3, no qual uma decodificação iterativa é implementada para realizar a etapa (c).

5. Processo de tratamento de dados biométricos, de acordo com qualquer uma das reivindicações precedentes, no qual o referencial multidimensional compreende dados de comprimento n_i de acordo com cada uma das N dimensões do referencial, i estando compreendido entre 1 e N ; e

no qual a codificação da primeira chave compreende as seguintes etapas:

- transformar a primeira chave em um outro referencial com N dimensões compreendendo dados de comprimento respectivo k_i de acordo com as N dimensões, o produto dos comprimentos k_i , para i compreendido entre 1 e N , sendo igual ao comprimento determinado da primeira chave;

- aplicar sucessivamente de acordo com as N dimensões respectivamente N códigos em bloco C_i , transformando os dados de comprimento respectivo k_i em dados codificados de comprimento respectivo n_i .

6. Processo de tratamento de dados biométricos, de acordo com qualquer uma das reivindicações precedentes,

no qual, a informação relativa à primeira chave é obtida por aplicação de uma função de Hash na primeira chave; e

no qual, a etapa (d) compreende as seguintes etapas:

- 5 - aplicar a função de Hash na segunda chave;
 - comparar a segunda chave sob a forma de Hash com a informação relativa à primeira chave.

7. Dispositivo (42) de tratamento de dados biométricos relativos a uma parte biológica em um sistema biométrico, o dispositivo de tratamento dispendo, de um
10 lado, de pelo menos um conjunto de dados biométricos de referência (B'_1) resultante da aplicação de uma operação 'ou exclusivo' entre um primeiro conjunto de dados biométricos (B_1) e uma primeira chave codificada (K_1), e,
15 de outro lado, de uma informação relativa à primeira chave;
o dispositivo compreendendo:

- uma unidade de interface (421) adaptada para receber um segundo conjunto de dados biométricos (B_2);
- uma unidade de determinação (442) adaptada para
20 fornecer uma segunda chave codificada (K_2) aplicando uma operação 'ou exclusivo' entre o conjunto de dados biométricos de referência e o segundo conjunto de dados biométricos recebido pela unidade de interface;
- uma unidade de decodificação (425) adaptada
25 para decodificar a segunda chave codificada (K_2); e
- uma unidade de decisão (423) adaptada para decidir se o segundo conjunto de dados biométricos corresponde ao primeiro conjunto de dados biométricos comparando a informação relativa à primeira chave com a
30 segunda chave;

no qual os primeiro e segundo conjuntos de dados biométricos são expressos em um referencial multidimensional com N dimensões, N sendo um número inteiro

superior ou igual a 2, os dados biométricos de acordo com pelo menos uma das N dimensões sendo obtidos por uma pluralidade de tratamentos aplicada relativamente à parte biológica; e

5 no qual a primeira chave codificada é obtida por aplicação de uma codificação transformando uma palavra inicial de um comprimento determinado em uma palavra codificada no referencial multidimensional.

10 8. Dispositivo (42) de tratamento de dados biométricos, de acordo com a reivindicação 7, no qual os dados biométricos de acordo com pelo menos uma dimensão são obtidos capturando uma pluralidade de imagens da parte biológica.

15 9. Dispositivo (42) de tratamento de dados biométricos, de acordo com a reivindicação 7 ou 8, no qual os dados biométricos de acordo com pelo menos uma dimensão são obtidos aplicando uma pluralidade de filtros em uma imagem da parte biológica.

20 10. Dispositivo (42) de tratamento de dados biométricos, de acordo com qualquer uma das reivindicações 7 a 9, no qual, a informação relativa à primeira chave é obtida por aplicação de uma função de Hash na primeira chave; e

no qual, a unidade de decisão compreende:

25 - uma unidade de Hash (426) adaptada para aplicar a função de Hash na segunda chave decodificada; e

- uma unidade de comparação adaptada para comparar a informação relativa à primeira chave e a segunda chave sob a forma de Hash.

30 11. Dispositivo (42) de tratamento de dados biométricos, de acordo com qualquer uma das reivindicações 7 a 10, no qual o conjunto de dados biométricos de

referência (B'_1) e/ou a informação relativa à primeira chave estão disponíveis em uma base de dados (424).

12. Sistema de tratamento de dados biométricos compreendendo um dispositivo de tratamento de dados biométricos de acordo com qualquer uma das reivindicações 7 a 11 e pelo menos um sensor biométrico (51) adaptado para fornecer um segundo conjunto de dados biométricos ao dispositivo de tratamento de dados biométricos.

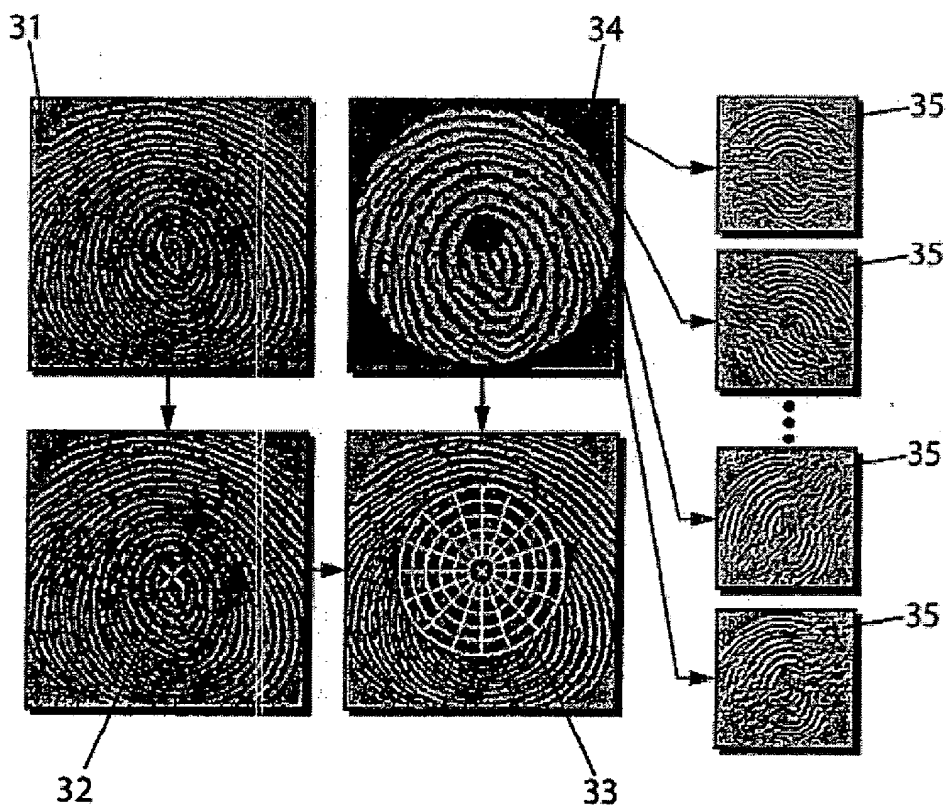
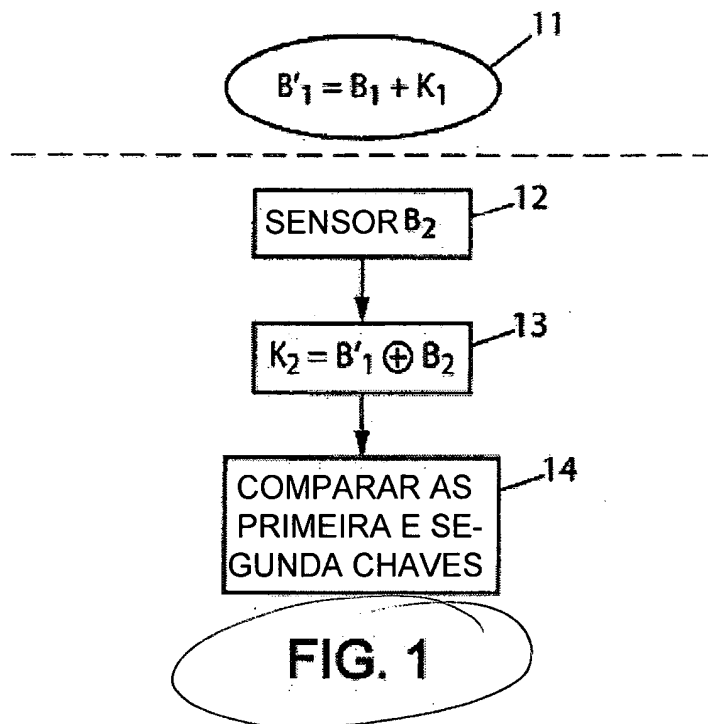


FIG. 3

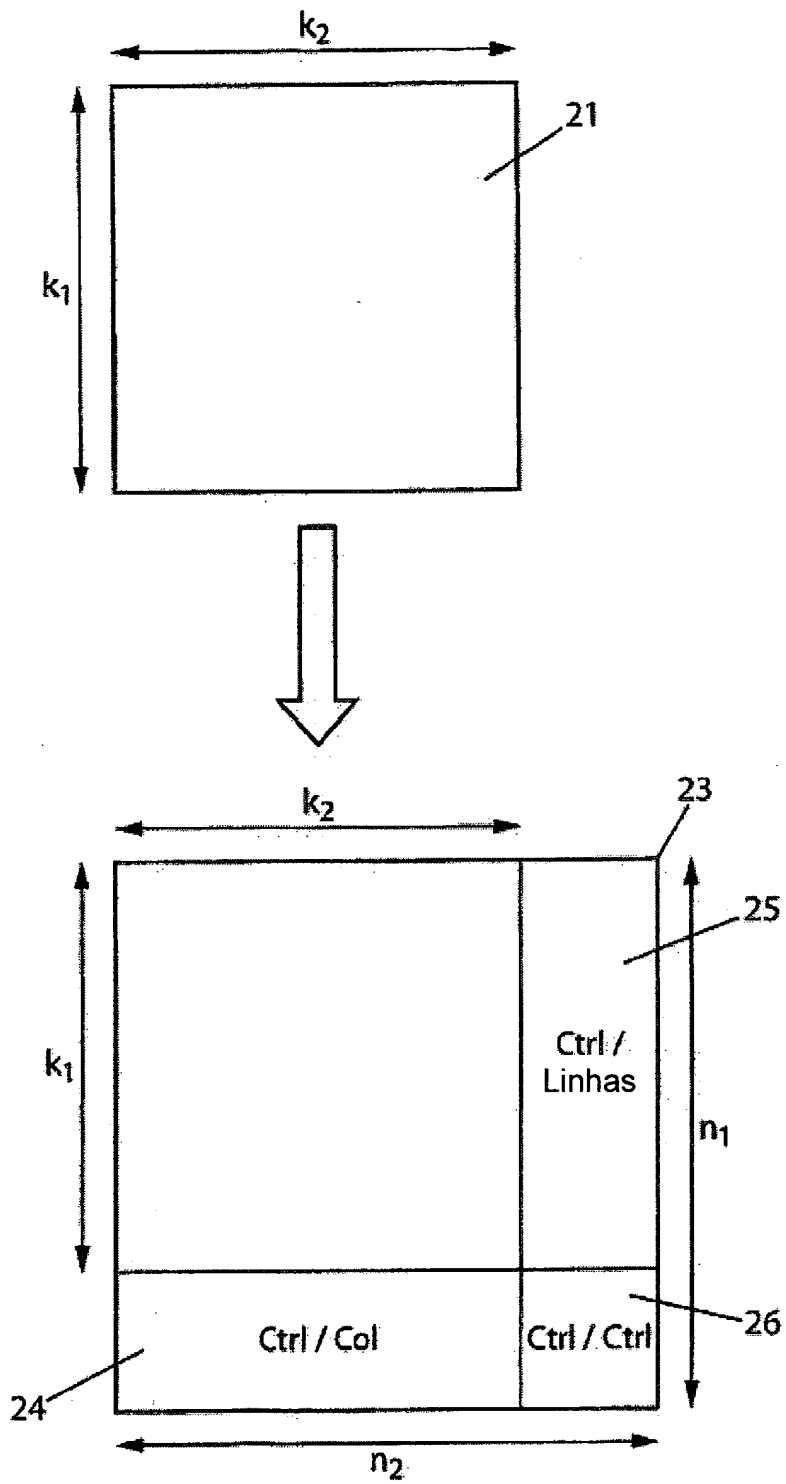


FIG. 2

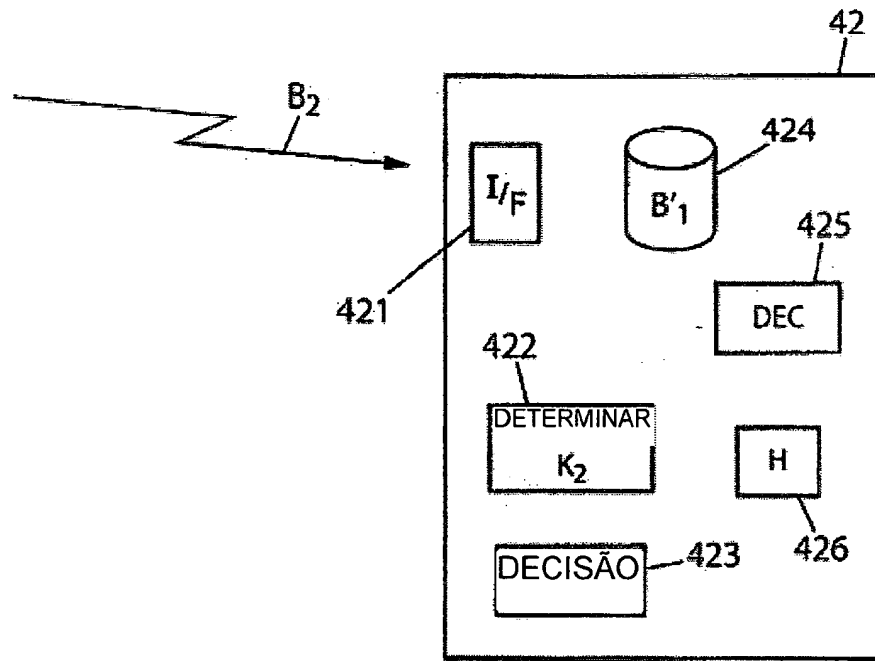


FIG. 4

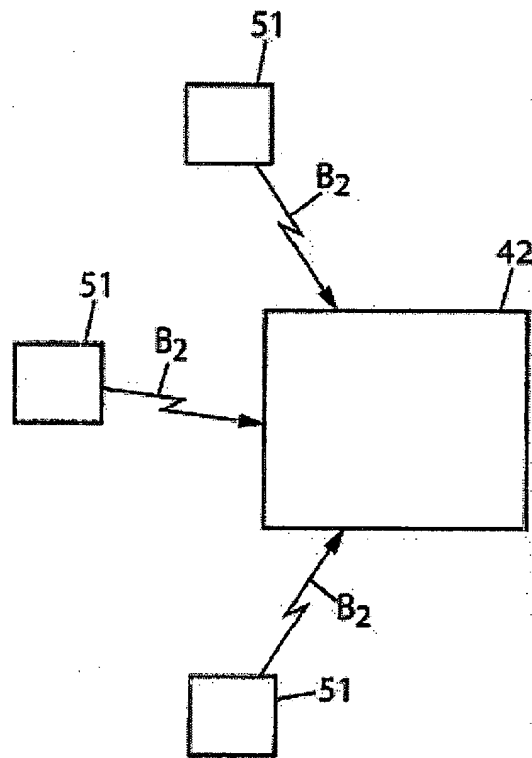


FIG. 5

RESUMO**"TRATAMENTO DE DADOS BIOMÉTRICOS EM UM REFERENCIAL
MULTIDIMENSIONAL"**

Um sistema biométrico dispõe de um conjunto de
5 dados biométricos de referência ($B'i$) resultante da
aplicação de uma operação 'ou exclusivo' entre um primeiro
conjunto de dados biométricos (B_1) e uma primeira chave
codificada (K_1), e de uma informação relativa à primeira
chave. Um segundo conjunto de dados biométricos (B_2) é
10 obtido. Uma segunda chave codificada (K_2) é determinada
aplicando-se uma operação 'ou exclusivo' entre o conjunto
de dados biométricos de referência e o segundo conjunto de
dados biométricos. A segunda chave é decodificada por
decodificação iterativa. Em seguida, decide-se se os
15 primeiro e segundo conjuntos de dados biométricos
correspondem entre si comparando-se a informação relativa à
primeira chave com a segunda chave. Os primeiro e segundo
conjuntos de dados biométricos são expressos em um
referencial multidimensional com N dimensões, os dados
20 biométricos de acordo com pelo menos uma das referidas N
dimensões sendo obtidos por aplicação de tratamentos
relativamente à parte biométrica; e a primeira chave
codificada é obtida por aplicação de uma codificação
transformando uma palavra inicial de um comprimento
25 determinado em uma palavra codificada no referencial
multidimensional.