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

(11) PI 0208624-7 B1

(22) Data do Depósito: 30/03/2002

(45) Data de Concessão: 21/02/2017

(54) Título: PROCESSO PARA TRANSMITIR MENSAGENS SMS COM IDENTIDADE PROTEGIDA

(51) Int.Cl.: H04L 29/06; H04M 3/42; H04W 88/18

(52) CPC: H04L 63/0407,H04L 63/0435,H04M 3/42008,H04W 88/184

(30) Prioridade Unionista: 04/04/2001 IT TO2001A000321

(73) Titular(es): TELECOM ITALIA S.P.A.

(72) Inventor(es): MARCO CINI; BORIS MOLTCHANOV

PROCESSO PARA TRANSMITIR MENSAGENS SMS COM IDENTIDADE PROTEGIDA

DESCRIÇÃO

[001] Esta invenção relaciona-se a sistemas de transmissão numérica de rede telefônica e, em particular, relaciona-se a um processo para transmitir mensagens SMS com identidade protegida.

[002] Como é conhecido, os sistemas de telecomunicação modernos permitem a transmissão de mensagens curtas do tipo SMS (Sistema de Mensagem Curta), que podem ser escritas com o teclado telefônico e exibida na tela do telefone, ao mesmo tempo que o sinal de voz sem causar interferência recíproca. Esta transmissão alfanumérica, que até recentemente era a prerrogativa dos sistemas de telefonia móvel de rede de rádio, é agora possível utilizando um equipamento adequado conectado à rede fixa, como telefones, máquinas de fax, caixas postais eletrônicas (correspondência eletrônica), etc.

[003] As mensagens SMS são compostas de campos diferentes. No cabeçalho da mensagem, há um campo que contém o número de telefone do usuário e denomina-se o campo OADC (Código de Destino do Endereço Originador), e no corpo da mensagem, há campos de serviço e de texto. O número de telefone do usuário permite que o gerente de sistema fature a chamada e o recipiente identifique a origem da mensagem. No entanto, este recurso, embora necessário para o gerente, poderá não ser aceitável para o remetente da mensagem ou poderá, de fato, colidir com as normas que governam a privacidade da comunicação, quando, por exemplo, as mensagens SMS são utilizadas para serviços

particulares, como votar, competições com prêmios, etc. O fornecedor do serviço final não pode ser capaz de obter os dados pessoais do usuário através do número telefônico, mas deve ser capa de alcançar o usuário por outros meios.

[004] Os métodos atualmente empregados para proteger a identidade do chamante que utiliza um telefone de voz não são adequados para este fim, pois eles normalmente funcionam ao tornar os três últimos números do número do telefone ilegíveis. Isto impede a identificação do usuário, mas também torna impossível para a pessoa que recebe a chamada chamar de volta.

[005] Também conhecido, do Documento WO 00 76231, é um método para transmitir uma mensagem em um serviço de comunicação que opera através de uma rede de telefonia móvel, permitindo comunicação anônima entre usuários do sistema. O número do telefone do emissor de cada mensagem é substituído pelo centro SMS com uma ID virtual, e essa correspondente é armazenada em uma base de dados. O usuário que recebe a mensagem, ser estar ciente do número de telefone real, é capa de responder utilizando a ID virtual, pois o centro SMS é capaz de associar a ID virtual ao número correto, consultando a base de dados. Esta solução implica mudanças estruturais na rede móvel, para a implementação da base de dados e para sua cooperação com o centro SMS. Ademais, o tamanho da base de dados não é desprezível e aumenta com o número de usuários.

[006] O Documento EP 0 899 918 revela um sistema para gerar um endereço fonte de pseudônimo em um campo técnico diferente, isto é, para uma mensagem de correio eletrônico. O sistema inclui um substituidor do endereço fonte de

pseudônimo que substitui o endereço fonte de pseudônimo pelo endereço fonte real, utilizando uma chave secreta. Isto remove o endereço fonte real da mensagem de correspondência eletrônica e assim torna o remetente, localizado no endereço fonte real, anônimo. Ainda, uma correspondência eletrônica de resposta pode ser enviada por meio de um reenviador, por exemplo, pela adoção de algoritmos de criptografia simétricos. O procedimento conhecido desta documento, no entanto, não é transferível para mensagens SMS, devido a estrutura específica da SMS.

[007] Essas dificuldades são evitadas e os problemas técnicos citados resolvidos pela utilização do procedimento para transmitir mensagens SMS com identidade protegida (o tópico desta invenção) que impede que o recipiente de uma mensagem SMS veja o número de telefone do chamante, e portanto os dados pessoais correspondentes, mas que permite que ele entre em contato com o chamante pelo envio de uma mensagem SMS.

[008] O tópico desta invenção é um procedimento para transmitir mensagens SMS com identidade protegida, conforme descrito na parte de caracterização da reivindicação 1.

[009] O que antecede e outras características desta invenção serão tornadas claras pela descrição seguinte de uma forma preferida da invenção dada por meio de um exemplo não limitante, e pelos desenhos anexos, em que:

[0010] A Figura 1 representa um sistema de rádio móvel do tipo GSM no qual mensagens SMS são transmitidas de acordo com a invenção.

[0011] A Figura 2 é um fluxograma que mostra a operação de cifragem.

[0012] A Figura 3 é um fluxograma que mostra a operação de decifragem.

[0013] Durante o procedimento para transmitir mensagens SMS com identidade protegida, o gerente do serviço cifra o número de telefone do usuário contido no cabeçalho da mensagem para impedir que os dados pessoais do usuário sejam revelados, e subseqüentemente o decifra para restaurar o número de telefone original.

[0014] A Figura 1 dá um exemplo de um sistema de rádio móvel GSM em que um telefone celular TC com cartão SIM envia uma mensagem SMS com seu número de telefone exibido na rede GSM. A mensagem é recebida e processada pelo centro de serviço de mensagens SMS denominado SMSC (Centro de Serviço de Mensagens Curtas), e é então encaminhada para o equipamento em trânsito, denominado GW, em que o número de telefone do chamante é cifrado. O equipamento GW, também conhecido como Portal SMS, normalmente transforma as mensagens UDP (Protocolo de Datagrama do Usuário) recebidas do SMSC em mensagens IP, que são então enviadas à rede TCP/IP (Protocolo de Controle de Transmissão/Protocolo da Internet) através de um roteador TCP/IP.

[0015] A mensagem modificada é então transmitida para seu destino, que poderá ser um fornecedor de serviços FS que tem a base de dados do usuário, DB, contendo, por exemplo, a identificação do usuário (número cifrado), o número de mensagens que o usuário enviou, as datas do envio, a informação nas mensagens, etc.

[0016] Se o fornecedor de serviços FS não puder decifrar a identidade do usuário do número de telefone cifrado, ele ainda pode responder ao utilizar o número

cifrado. O GW SMS então decifrará o número para restaurá-lo a sua forma original, e então encaminhar a mensagem. O fornecedor de serviços não pode, obviamente, acessar o GW SMS e conseqüentemente não pode ver o número do telefone.

[0017] O número de telefone do usuário é cifrado utilizando uma aplicação adequada que consiste de um algoritmo especial.

[0018] Poderá ser uma boa idéia selecionar um algoritmo inversível e simétrico com uma única senha para cifrar/ decifrar, que age no fluxo de número de série para cifrar dados de comprimentos diferentes. Os algoritmos do tipo "fluxo", que podem cifrar os dados à medida que chegam, byte a byte, até o fim, satisfazem esses requisitos.

[0019] Para o algoritmo ser aplicado corretamente, o número de telefone original, consistindo de um vetor decimal, precisa ter as características seguintes:

conter o código internacional;

não iniciar com zero;

não superar 14 números decimais, código incluído.

[0020] A aplicação emite um vetor de no máximo 16 números. Este limite é estabelecido pela dimensão do campo OADC da mensagem SMS. O vetor de saída consiste de uma parte inicial cifrada de não mais que o número de dígitos da entrada do número telefônico, isto é, 14, e uma segunda parte de dois dígitos que consiste do índice da senha utilizada para cifrar.

[0021] Uma tabela de 33 senhas é criada, em que cada senha corresponde a um índice. Os 99 índices possíveis que podem ser expressos com os dois dígitos decimais disponíveis são utilizados para transmitir outra

informação, conforme descrito em maior detalhe abaixo.

[0022] A tabela de senhas cifradas não é incluída no código fonte, mas é gerada dinamicamente cada vez que a aplicação de cifragem/decifragem é iniciada no bloco GW SMS. As 33 senhas permanecem as mesmas, mas não podem ser deduzidas do código fonte da aplicação ou do algoritmo matemático utilizado para calculá-las. O algoritmo utilizado pode ser facilmente modificado.

[0023] Em particular, a senha pode ser selecionada aleatoriamente da tabela ou ela pode ser a mesma para o mesmo número de telefone, de acordo com o valor que o gerente, quando solicitado pelo fornecedor do serviço, designa a uma variável booleana "histórica" considerada pela aplicação.

[0024] Se esta variável "histórica" for "verdadeira", o fornecedor de serviço pode construir a estória das operações realizadas pelo usuário móvel, e a armazena em um aparelho ao qual apenas o fornecedor pode acessar. Desta forma, o fornecedor de serviço pode coletar dados estatísticos sobre os usuários e armazenar o conteúdo das mensagens individuais, por exemplo, qual usuário deu a resposta correta em uma competição com prêmios.

[0025] Durante a decifragem, a aplicação dá entrada no vetor com não mais que 16 dígitos decimais, que contém o número de telefone cifrado e o índice da senha utilizado para cifrar que ocupa as duas últimas posições do vetor.

[0026] A variável "histórica" "verdadeira" não é necessária para decifrar, porque ela pode ser deduzida da faixa de valores ao qual pertence o índice da senha.

[0027] Na entrada, a aplicação restaura o número de

telefone original de não mais que 14 dígitos decimais, sem quaisquer zeros no início do código internacional.

[0028] Outros detalhes das operações individuais para cifrar o número de telefone do usuário são dadas no fluxograma mostrado na Figura 2.

[0029] Após o início, etapa 1, em que o número de telefone no campo OADC do cabeçalho da mensagem é adquirido, é feita uma verificação para ver de quantos bytes ele é composto, etapa 2. Se ele for mais de 14 bytes de comprimento, ele é enviado diretamente para a saída, etapa 13, sem efetuar qualquer operação. Caso contrário, o número de telefone é convertido do formato utilizado para transmissão SMS em um formato de número decimal, etapa 3. O formato SMS, na verdade, consiste de um vetor de 14 bytes, cada um dos quais representa um número de 0 a 9 do número de telefone, que precisa ser convertido em decimais para que ele possa ser submetido às operações subseqüentes.

[0030] A subseqüente etapa 4 verifica se a variável booleana "histórica" foi fixada para "verdadeira". Se não for este o caso, isto é, o valor lógico é "falso", um número inteiro inferior a 33 com a função denominada RAND(32) é gerado aleatoriamente para obter o índice de tabela de senha. Caso contrário, a operação de módulo de base 33 é efetuada no número de telefone, com a função MOD_{33}(OADC), para dar um índice que sempre será o mesmo para o mesmo número, etapa 6. Como é conhecido, a operação do módulo de base 33 consiste em dividir o número por 33 até um resto inferior a 33 ser obtido. Este resto é o índice de tabela de senha.

[0031] Na subseqüente etapa 7, se o número de telefone

e o índice da tabela de senha, calculado de uma das duas formas descritas anteriormente, estão disponíveis, pode-se cifrar utilizando o algoritmo simétrico de "fluxo" selecionado.

[0032] A etapa 8 consiste em verificar quantos dígitos decimais compõem o número cifrado. Se ele consiste de não mais que 14 dígitos decimais, ele é reconvertido do número decimal em um vetor de byte, adequado para a transmissão da mensagem SMS, e dois bytes de índice são acrescentados ao final, etapa 12, para ser restaurado ao final das operações, etapa 13. No entanto, se ele consiste de mais de 14 dígitos decimais, é verificado se ele é mais ou menos que $2x10^{14}$, etapa 9. Se ele é inferior a $2x10^{14}$, o índice é aumentado por 33, etapa 10, enquanto se ele é maior que ou igual a $2x10^{14}$, o índice é aumentado por 66, etapa 11.

[0033] Desta forma, o índice de tabela de senha poderá estar em uma de três faixas: 0-32, 33-65, 66-99 e, conseqüentemente, fornece a informação que o número cifrado inclui um 15º dígito além dos 14 dígitos decimais, que poderá ser 0, 1 ou 2, respectivamente. Obviamente, os índices que diferem de 00, 33 ou 66 sempre identificam a mesma senha.

[0034] Como no caso anterior, o número decimal é reconvertido em um vetor de byte que inclui os dois bytes de índice, assim obtendo um vetor de 16 bytes, etapa 12, que é então emitido, etapa 13.

[0035] Maiores detalhes sobre as operações individuais para decifrar o número de telefone do usuário são dados no fluxograma mostrado na Figura 3.

[0036] Após uma fase inicial de inicialização, etapa

20, em que o número de telefone cifrado no campo OADC da mensagem é adquirido, ele é convertido de seu formato vetorial, utilizado para a transmissão SMS, em um número decimal ao extrair os dois últimos dígitos que representam o índice de tabela de senha, etapa 21.

[0037] A etapa 22 então verifica o valor do índice. Se o índice for inferior a 33, a senha correspondente pode ser encontrada e a decifragem pode ser efetuada diretamente, etapa 27. O número obtido é mais uma vez reconvertido em um vetor adequado para transmissão de mensagem SMS, etapa 28, e depois emitido, etapa 29.

[0038] No entanto, se o índice for maior ou igual a 33, é feita uma verificação para ver se ele é maior ou igual a 66, etapa 23. Se for, o número de telefone cifrado é aumentado por $2x10^{14}$, etapa 25, caso contrário ele é aumentado por $1x10^{14}$, etapa 24, assim obtendo o número cifrado original. Em qualquer caso, o índice é submetido à operação do módulo base 33, etapa 26, para obter um valor na faixa 0-32, e ele é então decifrado, etapa 27, reconvertido em formato vetorial, etapa 28 e então completado, etapa 29.

[0039] Obviamente, esta descrição é dada como um exemplo não limitativo. Variantes e modificações são possíveis, sem emergir do campo de proteção das reivindicações.

REIVINDICAÇÕES

1. Processo para a transmissão de mensagens SMS com identidade protegida, no qual um número de telefone do chamante é contido no campo de cabeçalho (OADC) da mensagem SMS enviada, a mensagem SMS enviada pelo usuário com seu número de telefone visível sendo recebida e processada por um centro de serviço de mensagem SMS (SMSC), e então encaminhada ao equipamento de trânsito (GW) onde ela é cifrada com uma aplicação com base num algoritmo adequado, e depois transmitida para seu destino, que não pode descobrir a identidade do usuário do número de telefone cifrado, mas que pode responder ao usar o número cifrado, devido ao fato de o equipamento de trânsito (GW) ser ativado para decifrar o número e restaurá-lo a sua forma original, e depois encaminhar a chamada corretamente, o processo **caracterizado** pelo fato de que o dito número de telefone cifrado compreende uma primeira parte contendo o número de telefone do chamante cifrado, usando uma senha selecionada de uma pluralidade de senhas diferentes, por meios do dito algoritmo de cifragem, e uma segunda parte contendo um índice identificando a senha usada para cifragem entre a dita pluralidade de senhas diferentes.

2. Processo, de acordo com a reivindicação 1, **caracterizado** pelo fato de o dito algoritmo adequado ser um algoritmo inversível simétrico com uma única senha para cifrar/decifrar, adequado para agir em um fluxo de número serial para cifrar dados de comprimentos diferentes.

3. Processo, de acordo com a reivindicação 1 ou 2, **caracterizado** pelo fato da aplicação criar, a cada vez, uma tabela de senhas, classificada pelo dito índice, que pode

ser gerado aleatoriamente ou pode ser o mesmo para o mesmo número de telefone, dependendo do valor que um gerente, quando da solicitação do fornecedor do serviço, designa a uma variável booleana (histórica), que permite que a parte chamada armazene o histórico das operações efetuadas pelo usuário chamante.

4. Processo, de acordo com qualquer uma das reivindicações 1 a 3, **caracterizado** pelo fato de a dita aplicação efetuar a operações de cifragem conforme segue:

adquirir o número de telefone visível (etapa 1);

verificar para ver de quantos bytes ele consiste (etapa 2);

se o número superar 14 bytes, ele é enviado diretamente para a saída (etapa 13), sem efetuar qualquer operação;

se o número não superar o primeiro comprimento, ele é convertido do formato usado para a transmissão SMS num formato de número decimal (etapa 3);

avaliar o valor lógico da variável booleana (histórica) (etapa 4);

se a variável booleana tem um primeiro valor lógico (falso), ela gera aleatoriamente um número inteiro que é inferior ao número de senhas para obter o índice da tabela (etapa 5);

se a variável booleana tem um segundo valor lógico (verdadeiro), ela efetua uma operação de módulo no número de telefone, utilizando o número de senhas como base, obtendo um índice que sempre será o mesmo para o mesmo número de telefone (etapa 6);

efetuar uma operação de cifragem utilizando o dito

algoritmo (etapa 7);

verificar quantos dígitos decimais compõem o número cifrado (etapa 8);

se os dígitos decimais não são maior que um primeiro número, ela reconverte o número cifrado do número decimal num vetor de byte, adequado para transmissão da mensagem SMS (etapa 12);

se os dígitos decimais são maiores que o primeiro número, ela verifica se o número cifrado é maior ou igual a duas vezes de elevado à potência do primeiro número (etapa 9);

se o número cifrado for menor que duas vezes dez elevado à potência do primeiro número, o índice da senha é aumentado pelo número de senhas (etapa 10);

se o número cifrado é maior ou igual a duas vezes dez elevado à potência do primeiro número, o índice da senha é aumentado duas vezes pelo número de senhas (etapa 11);

ela reconverte o número cifrado do número decimal em um vetor de byte incluindo dois bytes de índice (etapa 12);

encerrar a operação de cifragem (etapa 13).

5. Processo, de acordo com a reivindicação 4, **caracterizado** pelo fato de a aplicação efetuar a operação de decifragem conforme segue:

adquirir o número de telefone cifrado (etapa 20);

converter o número do formato utilizado para transmissão SMS em um formato de número decimal, extraindo os últimos dois dígitos que representam o índice de tabela de senha (etapa 21);

verificar o valor do índice (etapa 22);

se o índice é inferior ao número da senha (33), ela

obtém a senha correspondente e realiza a decifragem diretamente (etapa 27);

se o índice é maior ou igual ao número de senhas (33), ela decide se ele é duas vezes ou mais o número de senhas (66) (etapa 23);

se ele for duas vezes ou mais o número de senhas (66), o número de telefone cifrado é aumentado por $2x10^{14}$ do primeiro número (14) (etapa 25);

se ele é inferior a duas vezes o número de senhas (66), o número de telefone cifrado é aumentado por $1x10^{14}$ do primeiro número (14) (etapa 24);

se o índice é maior ou igual ao número de senhas (33), ela submete o índice à operação de módulo utilizando o número de senhas (33) como o módulo base (33) (etapa 26);

efetuar a decifragem (etapa 27);

reconverter o número decifrado em formato vetorial (etapa 28);

encerrar a operação de decifragem (etapa 29).

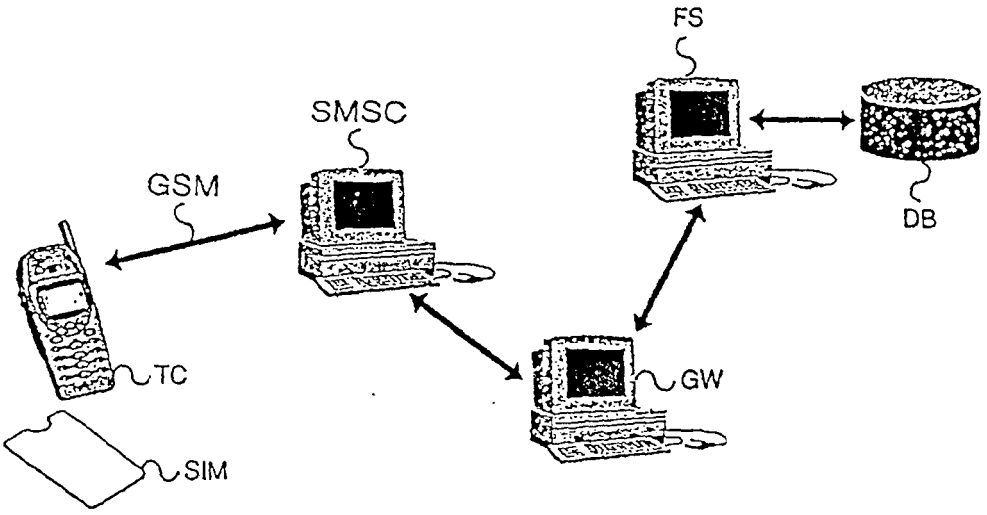

FIGURA: 1

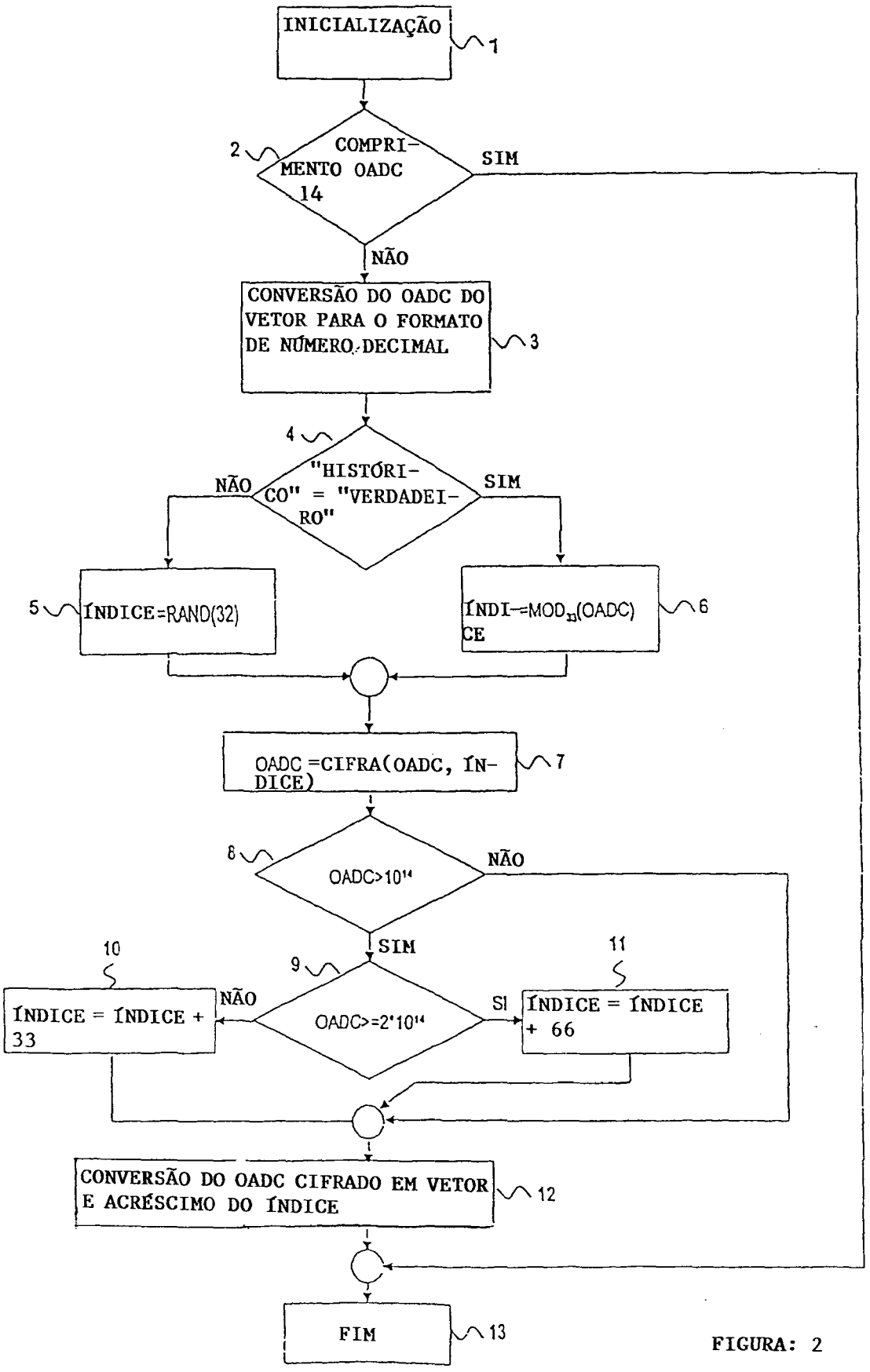
INICIALIZAÇÃO
1
2
COMPRI-MENTO OADC 14
SIM
NÃO
CONVERSÃO DO OADC DO VETOR PARA O FORMATO DE NÚMERO DECIMAL
3
4
"HISTÓRI-CO" = "VERDADEI-RO"
NÃO
SIM
5
ÍNDICE=RAND(32)
ÍNDI-CE=MOD32(OADC)
6
OADC =CIFRA(OADC, ÍN-DICE)
7
8
OADC>10^14
NÃO
SIM
10
9
11
ÍNDICE = ÍNDICE + 33
NÃO
OADC>=2*10^14
SI
ÍNDICE = ÍNDICE + 66
CONVERSÃO DO OADC CIFRADO EM VETOR E ACRÉSCIMO DO ÍNDICE
12
FIM
13

FIGURA: 2

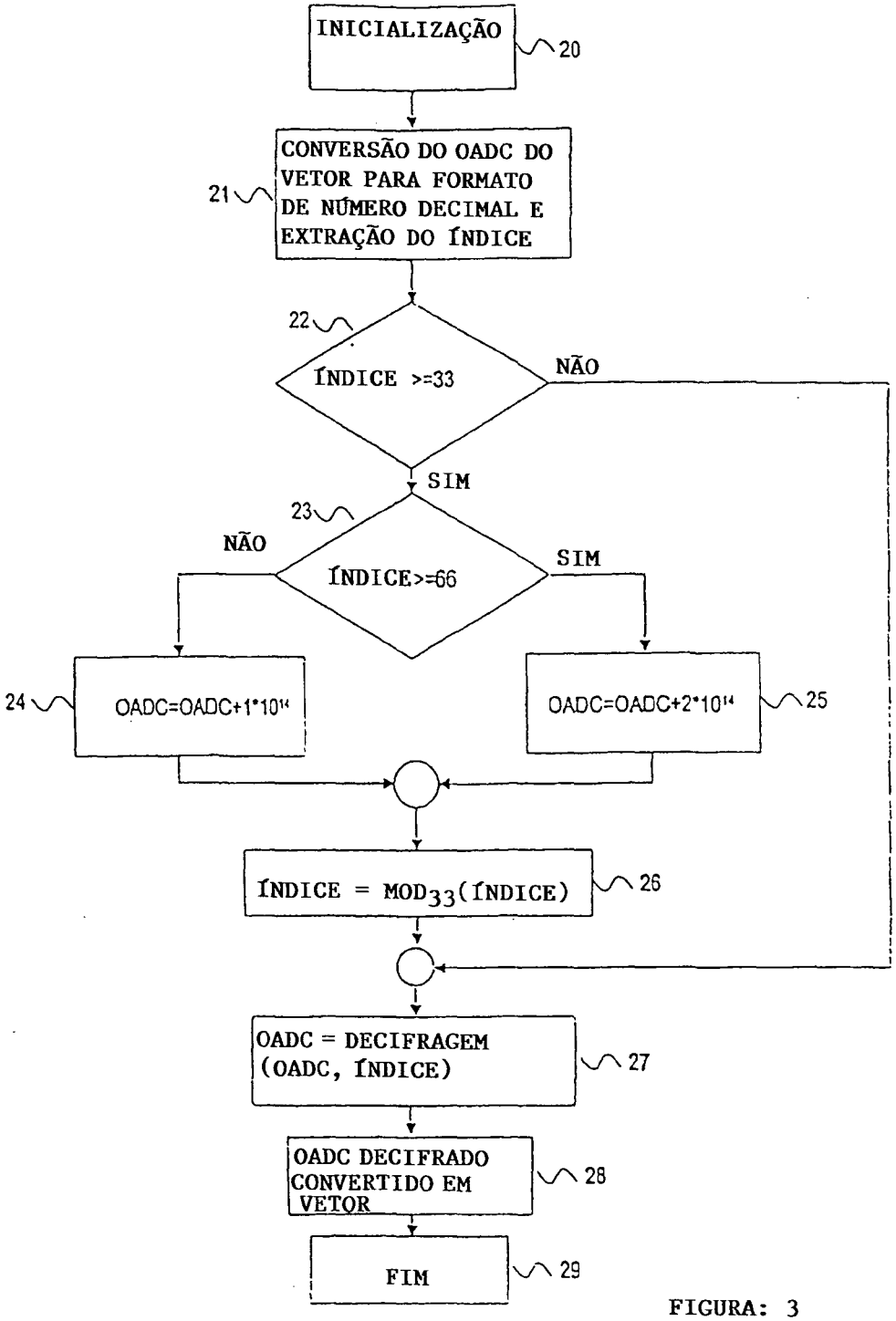
INICIALIZAÇÃO
20
CONVERSÃO DO OADC DO VETOR PARA FORMATO DE NÚMERO DECIMAL E EXTRAÇÃO DO ÍNDICE
21
22
ÍNDICE >=33
NÃO
SIM
23
NÃO
ÍNDICE>=66
SIM
24
OADC=OADC+1*10^14
OADC=OADC+2*10^14
25
ÍNDICE = MOD33(ÍNDICE)
26
OADC = DECIFRAGEM (OADC, ÍNDICE)
27
OADC DECIFRADO CONVERTIDO EM VETOR
28
FIM
29

FIGURA: 3