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

(21) **PI 1002551-0 A2**

* B R P I 1 0 0 2 5 5 1 A 2 *

(22) Data de Depósito: 14/07/2010
(43) Data da Publicação: 27/03/2012
(RPI 2151)

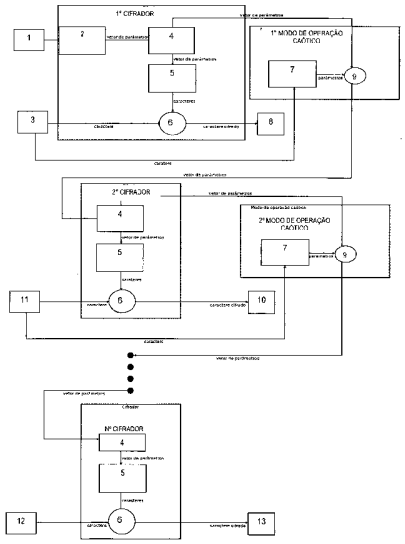
(51) Int.Cl.:
H04L 12/22
H04L 9/00

(54) Título: MÉTODO DE CRIPTOGRAFIA EM MODO DE OPERAÇÃO CAÓTICO

(73) Titular(es): UNIVERSIDADE DE SÃO PAULO - USP

(72) Inventor(es): ALEXANDRE SOUTO MARTINEZ, ANDERSON GONCALVES MARCO, ODEMIR MARTINEZ BRUNO

(57) Resumo: MÉTODO DE CRIPTOGRAFIA EM MODO DE OPERAÇÃO CAÓTICO. O invento proposto é de um algoritmo de criptografia de arquivos computacionais, baseado nas iterações dos mapas de sistemas dinâmicos no regime caótico. O algoritmo apresenta como características a segurança e o desempenho que o tornam especialmente adequado para o uso comercial. A segurança do algoritmo está baseada no uso de sistemas dinâmicos no regime caótico e também no modo de operação caótico. O algoritmo de criptografia baseado em sistemas caóticos tem como característica ser seguro, pela natureza matemática do caos. Entretanto, é muito fácil produzir um algoritmo de criptografia caótica com falhas de projeto que abrem brechas para criptoanálise. O método proposto apresenta também o modo de operação caótico que combina a mensagem a ser criptografada, a senha e o sistema caótico na codificação garantindo, assim, uma segurança sólida da criptografia gerada. O algoritmo proposto pode ser implementado para explorar o paralelismo de processadores principais, bem como da placa de vídeo (GPU) de modo a codificar e decodificar as mensagens com alto desempenho. O método proposto na presente invenção pode ser implementado em qualquer computador convencional, smartphones ou telefones celulares e eventualmente em outro dispositivo computacional.



MÉTODO DE CRIPTOGRAFIA EM MODO DE OPERAÇÃO CAÓTICO

CAMPO DA INVENÇÃO

A presente invenção se refere em geral a métodos de criptografia e, em particular, a um novo método de criptografia que emprega um novo algoritmo de criptografia de arquivos computacionais, baseado em iterações dos mapas de sistemas dinâmicos no regime caótico.

FUNDAMENTOS DA INVENÇÃO

A criptografia consiste em codificar uma mensagem (arquivo de computador, por exemplo) de forma que ela só possa ser compreendida por alguém autorizado através da decodificação. Uma chave (ou senha) é necessária para realizar esta decodificação. De acordo com o tipo de chave, a criptografia é dividida em duas categorias:

criptografia simétrica, onde uma mesma chave (obtida de argumentos da matemática discreta) é usada para criptografar e decriptografar; e

criptografia assimétrica, onde se utiliza uma chave para criptografar e outra para decriptografar (estas chaves são obtidas através de argumentos da teoria dos números).

Atualmente, além do uso militar, a criptografia é indispensável para o comércio eletrônico, sistemas bancários, proteção contra espionagem industrial e etc.

Os métodos de criptografia atuais, por se basearem quase que exclusivamente na matemática discreta ou na teoria dos números naturais, são extremamente complexos. Os métodos de criptografia simétrica realizam muitas operações matemáticas e combinatórias em bits agrupados em blocos (também chamadas de cifras de bloco, por causa desta propriedade). Os métodos de criptografia assimétrica necessitam considerar chaves muito grandes.

A criptoanálise é tão antiga quanto a própria criptografia. A criptoanálise busca formas de decifrar uma mensagem criptografada por um determinado algoritmo, sem conhecer o algoritmo e a chave secreta. Para que a criptoanálise seja viável nem todos os algoritmos nem todas as possíveis combinações de chaves devem ser considerados. Em muitos casos, as técnicas de criptoanálise reduzem muito a procura do número de possíveis chaves com que uma mensagem foi cifrada. Atualmente, muitos algoritmos simétricos já foram decodificados (quebrados) dessa maneira. Mesmo com a redução do número de possíveis chaves com as quais uma determinada mensagem é cifrada, este número ainda não é grande o suficiente para permitir, com o atual poder computacional existente, o uso prático das atuais formas de criptografia. Contudo, com a descoberta de novas formas de criptoanálise e com o aumento exponencial do poder computacional, a quebra dos atuais algoritmos de criptografia vai ser possível nas próximas décadas. Como exemplo pode-se citar o caso do algoritmo DES, proposto nos anos 1970 e

quebrado de forma prática em duas décadas.

Recentemente uma nova categoria de algoritmos de criptografia foi criada. São os algoritmos de criptografia caóticos (M.S. Baptista. Cryptography with chaos. *Physics Letters A*, 240:50–54, 1998; Tao Xiang, Xiaofeng Liao, Guoping Tang, Yong Chen, and Kwok wo Wong. A novel block cryptosystem based on iterating a chaotic map. *Physics Letters A*, 349(1-4):109–115, Jan 2005). Esses algoritmos exploram o determinismo dos mapas de sistemas dinâmicos e a sensibilidade às condições iniciais da região caótica, nos casos não-lineares. Por sensibilidade às condições iniciais queremos dizer que trajetórias completamente diferentes são obtidas nos mapas de sistemas dinâmicos caóticos. O determinismo dos sistemas dinâmicos e a sensibilidade às condições iniciais no regime caótico desses sistemas garantem a codificação e decodificação das mensagens.

Desde a década de 1990, há uma tendência de usar mecanismos matemáticos mais sofisticados nos algoritmos de criptografia e que se mostrou resistente às atuais técnicas de criptoanálise. Entre tais mecanismos matemáticos os sistemas dinâmicos caóticos se sobressaem. Entretanto, surgem dois problemas com estes algoritmos:

1. O desempenho computacional (relativo ao tempo que o computador leva para executar o programa) é muito baixo, o que os torna inviáveis para determinadas aplicações que exijam alta velocidade de codificação/decodificação sobre um grande volume de dados. Por exemplo, a codificação de um filme Blue Ray.

2. Recentemente foram reportadas na literatura falhas de segurança nestes sistemas, pois, não apenas é necessário se utilizar de uma matemática mais sofisticada como também é necessário desenvolver um bom algoritmo a fim de evitar falhas de design, o que implica em uma forma muito fácil de quebrar o código.

O pedido de patente US 2007/0050614, publicado em 1 de março de 2007, intitulado "Robust hyper-chaotic encryption-decryption system and method for digital secure-communication", emprega a sincronização de sistemas caóticos para criptografar. Isto faz com que, caso o atacante intercepte a comunicação durante a sincronização dos sistemas caóticos de A e B, ele possa sincronizar o sistema caótico dele com um dos participantes A - B, podendo fazer-se passar tanto por A, como por B. Além disto, a sincronização de sistemas dinâmicos requer que a comunicação (troca de informação) entre as partes A e B, para a sincronização do sistema dinâmico, seja alta antes da transmissão de um texto cifrado.

A patente US 5.751.811, de 12 de maio de 1998, intitulada "32N +D bit key encryption-decryption system using chaos", utiliza o fractal do Mandelbrot como sistema dinâmico cifrador/decifrador com chaves de 64 bits. Chaves com este comprimento são

curtas demais para os padrões de criptografia atuais.

A patente US 7.266.200, de 4 de setembro de 2007, intitulada "Method and apparatus for encryption of data", extrai bytes dos dígitos mais significativos das iterações que formam o sistema dinâmico para, então, combinar os mesmos usando uma operação bit a bit, com bytes do texto original produzindo, assim, o texto cifrado. Entretanto, o uso dos bytes mais significativos, extraídos das iterações de um sistema dinâmico, enfraquece a criptografia.

A patente US 6.792.111, de 14 de setembro de 2004, intitulada "Cryptation system for packet switching networks based on digital chaotic models", utiliza mapas caóticos como o logístico ou o de Henon, entre outros, para cifrar. Porém, estes mapas, em especial o logístico, possuem graves deficiências o que os torna inadequados à criptografia.

A patente US 7.106.864, de 12 de setembro de 2006, intitulada "Chaos-based data protection using time-discrete dynamical systems" usa o mapa logístico no regime caótico para criar misturas das cifras de bloco tradicionais.

O documento de patente PI 0602981-7, de 21 de julho de 2006, intitulado "WEDI: Método e sistema que utiliza algoritmos de criptografia simétricos ou assimétricos para geração de chaves criptográficas que possibilitam a identificação de documentos impressos e em meio eletrônico e a responsabilização de pessoas pela divulgação e utilização de informações, contidas nesses documentos, de forma ilegal, ilícita ou não autorizada", trata de um WEDI, que é o acrônimo de Watermark Encryption Document Identification. É um método e sistema que viabiliza a identificação de documentos impressos e em meio eletrônico e suas informações, mediante geração e impressão de uma chave criptográfica como marca d'água, gerada pela aplicação de algoritmos cifradores simétricos ou assimétricos e de função Hashing a partir de vários dados sobre o próprio documento, sobre dispositivos e pessoas envolvidos na sua geração, que possibilita a identificação desses documentos quanto à sua origem, ao destinatário, à data e horário de sua geração, à data de envio ao destinatário, ao usuário responsável pela geração, e outras informações sobre o documento, a partir da obtenção de apenas parte ou pedaços desses documentos que contenham fragmentos da chave criptográfica como marca d'água impressa.

O documento de patente PI 0703237-4, depositado em 06/07/2007, intitulado "Algoritmo de Criptografia Usando as Sequências Caóticas de Dígitos de Raízes Irracionais", trata de um método de criptografia baseado no comportamento caótico da sequência de dígitos de raízes irracionais descrevendo um algoritmo de criptografia/decriptografia baseado em dinâmicas caóticas das sequências de arranjos de

d-dígitos da representação visual (ou em outra base) das imagens irracionais de uma função real. O presente invento prevê, ainda, passos para controlar a segurança do sistema contra ataques por força bruta. Quanto a este documento, embora ele utilize o caos, ele apresenta uma maneira de criptografar diferente. Primeiro esse documento não combina criptografia tradicional e caótica como a presente invenção. Mas, mais importante que isso, o método descrito nesse documento armazena o mapa caótico na memória para o processo de criptografia. Este procedimento tem a desvantagem de ser custoso e lento e gasta muita memória. Por exemplo, se a mensagem criptografada for muito extensa como, por exemplo, um DVD a memória utilizada para guardar o mapa deve ser maior do que a mensagem, implicando em utilizar mais de 5GB de RAM. Este procedimento torna o método muito lento e inviável de ser utilizado nos micros atuais ou em computadores menores como notebooks, subnotebooks, smartfones ou celulares. Uma das vantagens do método da presente invenção é a performance. No presente método ele ainda pode ser paralelizado e executado em placas de vídeo, ou qualquer outro dispositivo com processamento tornando o processamento rápido, o que torna o método adequado ao mercado. O método proposto no documento PI 0703237-4 não seria viável de ser implementado com computação paralela ou em placas de vídeo. Ainda outro ponto importante, que diferencia esse método daquele da presente invenção, é que no método do PI 0703237-4 a mensagem cifrada fica maior do que a mensagem original. Já no presente método ambas têm o mesmo tamanho. Manter a cifra do mesmo tamanho é interessante por dois aspectos, economia de espaço, por exemplo, na criptografia de um DVD e ainda por segurança. Quando a mensagem é ampliada ela pode dar pistas do modo como a criptografia foi feita.

Outro ponto importantíssimo quanto ao documento PI 0703237-4 está no item 3.2 – Cifragem, subitem 1. Segundo ele é necessário ter um ponto flutuante do tamanho da mensagem. Deste modo, o método é completamente inviável. Isso impossibilita este método de ser utilizado em qualquer computador real; se a mensagem for maior que 20KB, por exemplo, seria impossível de ser calculada. Matematicamente o método é viável, mas tecnologicamente não é possível implementar o algoritmo proposto nesse documento. No presente método temos o programa rodando, sendo capaz de fazer a criptografia de arquivos com virtualmente qualquer tamanho, por exemplo, um DVD ou ainda maior.

OBJETO DA INVENÇÃO

A presente invenção soluciona ambos os problemas relatados acima, o desempenho computacional e as falhas de segurança. O algoritmo utilizado no método da presente invenção é mais seguro do que aqueles conhecidos na técnica. Ele combina

a criptografia convencional e a criptografia caótica. Para isso foi proposta uma técnica denominada modo de operação caótico, cujo funcionamento será explicado adiante. Outro ponto forte é que o algoritmo empregado no método da presente invenção pode ser paralelizado e é de alto desempenho. O seu desempenho computacional é adequado para uso comercial imediato.

A presente invenção é de interesse de todas as entidades relacionadas com sigilo e comunicação de dados tais como: bancos, entidades financeiras, governamentais e também lojas eletrônicas na internet (e-commerce). O método proposto na presente invenção pode ser implementado em qualquer computador convencional, smartphones ou telefones celulares e eventualmente em outro dispositivo computacional.

SUMÁRIO DA INVENÇÃO

Método de criptografia em modo de operação caótico compreendendo um 1° cifrador para obter um caractere cifrado 1; um 1° modo de operação caótico para obter parâmetros que são enviados a um 2° cifrador; um 2° cifrador para obter um caractere cifrado 2; um 2° modo de operação caótico para obter parâmetros que são enviados a um n° cifrador e um n° cifrador para obter um caractere cifrado n.

BREVE DESCRIÇÃO DAS FIGURAS

A Figura 1 é um diagrama de blocos representativo da implementação da metodologia da presente invenção.

A Figura 2 é um diagrama de blocos representativo da influência dos dados na cifra como um todo.

A Figura 3 é um diagrama de blocos representativo da implementação da metodologia da presente invenção sem o modo de operação caótico.

A Figura 4a é um gráfico de análise de frequência de caractere no livro original.

A Figura 4b é um gráfico de análise de frequência de caractere no livro cifrado com uma senha.

A Figura 4c é um gráfico de análise de frequência de caractere no livro cifrado usando uma senha diferente da senha usada na Figura 4b.

A Figura 5a é um gráfico mostrando a matriz de correlação do livro original.

A Figura 5b é um gráfico mostrando a matriz de correlação do livro cifrado.

A Figura 5c é um gráfico mostrando a matriz de correlação de ruído branco.

A Figura 6a mostra matriz de imagem original.

A Figura 6b mostra matriz de imagem cifrada.

A Figura 6c mostra matriz de imagem de ruído branco.

A Figura 6d mostra histograma de imagem original.

A Figura 6e mostra histograma de imagem cifrada.

A Figura 6f mostra histograma de imagem de ruído branco.

A Figura 6g mostra espectro de Fourier de imagem original.

A Figura 6h mostra espectro de Fourier de imagem cifrada.

A Figura 6i mostra espectro de Fourier de imagem de ruído branco.

A Figura 7a é um gráfico de desempenho do algoritmo sequencial.

A Figura 7b é um gráfico comparativo de desempenho entre o algoritmo da versão GPU e o método de criptografia AES.

DESCRIÇÃO DA INVENÇÃO

A presente invenção será agora descrita em detalhes com base nas figuras em anexo sem, entretanto, limitar a invenção ao que está representado nas figuras.

Na presente invenção apresentamos um método de criptografia de mensagens baseado em sistemas dinâmicos caóticos. A mensagem é considerada como sendo um arquivo qualquer de computador ou qualquer outro dispositivo eletrônico. Um arquivo de computador é decomposto em "bytes", que corresponde a oito unidades binárias chamadas de "bits". Todo arquivo de computador por ser descrito pelo número de bytes n_p e pela configuração de cada byte através do vetor P $(P_i) = (P_1, P_2, \ldots, P_{np})$, onde P_i representa o estado de um byte, ou seja, é um número inteiro entre 0 e $255 = 2^8 - 1$. Criptografar o arquivo P, consiste em transformar este arquivo em outro arquivo, do mesmo tamanho n_p, mas com valores inteiros entre 0 e 255 embaralhados, o qual representamos pelo vetor C. A transformação de cada componente de (P_i) em uma componente de (C_i) é dada através de uma função de encriptação E_α, assim $P_i = E(C_i)$, onde α é um vetor de tamanho n_α, onde cada componente representa um parâmetro da função de encriptação E. Um dos parâmetros da função de codificação é a chave ou senha. Uma senha é um texto representado no computador por n_π bytes e pelo vetor π. O processo de encriptação mais simples (cifragem de Cesar) consiste em fazer $\alpha = \pi$ e transfomar α em um número inteiro α e considerar $P_i = (C_i + \alpha) \bmod 2^8$, onde a função mod é o resto da divisão de $C_i + \alpha$ por 2^8. Em suma, $P_i = E_\alpha(C_i)$ com $E_\alpha(C_i) = (C_i + \alpha) \bmod 2^8$. A decodificação consiste em reencontrar a partir de dada a senha . Para isto, utiliza-se a função de decodificação D, que é a função inversa de E. Como exemplo, a decodificação pela cifragem de Cesar é dada por $P_i = (C_i - \alpha) \bmod 2^8$.

Um método de criptoanálise para quebrar a cifragem de Cesar, consiste em fazer uma estatística do aparecimento de um dado caractere, ou seja, um número entre 0 e 255, que chamamos de representação ASCII. O caractere mais frequente corresponde a letra que mais aparece em um dado idioma e assim por diante. Através desta técnica simples é possível decodificar mensagens ingenuamente cifradas. Para corrigir este problema, uma alternativa é criar um modo de operação. Cria-se uma tabela de

correspondência entre C_i e P_i que depende da posição i dos caracteres no texto. Um modo simples de fazer isso é acrescentar um novo parâmetro C_0 a α e fazer a codificação depender da posição no texto através do caractere precedente no texto cifrado. Uma possível implementação do modo de operação é considerar a seguinte função de encriptação $E_\alpha(P_i,C_{i-1}) = (P_i \oplus C_{i-1} + \alpha) \bmod 2^8$, onde a operação *oplus* representa a operação XOR (ou exclusivo).

É possível demonstrar matematicamente que uma cifra é impossível de ser quebrada se o comprimento da tabela de correspondência OTP (do inglês, one-time pad) entre mensagem cifrada e texto original n_t for igual ao comprimento da mensagem $n_t = n_T$. Para isto ser verdade é ainda necessário que esta tabela de correspondência seja criada de modo aleatório e usada uma única vez. Estas últimas considerações tornam o OTP inviável do ponto de vista prático, pois considere os seguintes números. Uma música de 5 minutos comprimida no formato MP3 possui 5242880 letras que devem ser criptografadas em grandes volumes. Por exemplo, o Itunes vende mais de 1 milhão de musicas por dia.

Basicamente a presente invenção consiste em utilizar o modo de operação, mas no lugar de utilizar a operação XOR, utilizamos uma equação de recorrência $r_i = F(r_{i-1})$, onde o mapa $F(x)$ é não-linear. Ao uso na criptografia de uma equação de recorrência que utiliza um mapa não-linear, que apresenta a região caótica, se dá o nome de modo de operação caótico.

Um sistema dinâmico caótico, que apesar de ser determinista, possui um comportamento errático similar ao de um sistema estocástico. Além disso, ele é muito sensível às condições iniciais, ou seja, a sequência de números r_i gerados pela condição inicial r_0 é completamente diferente da sequência de números gerados por uma condição ligeiramente diferente de r_0. O determinismo e a sensibilidade às condições iniciais é que garantem a ótima qualidade no método de criptografia proposto na presente invenção.

O modo de operação caótico foi inspirado nos modos de operação dos algoritmos de bloco simétricos tradicionais. Nesses algoritmos, um bloco do texto original é combinado com uma região do sistema dinâmico que foi utilizada para cifrá-lo. Isto produz uma nova condição inicial que irá re-alimentar o sistema dinâmico. Como vimos, nos algoritmos de bloco simétricos tradicionais, o modo de operação mais utilizado re-alimenta o algoritmo com o bloco cifrado de texto.

O modo de operação caótico da presente invenção possui uma característica diferente dos modos de operação tradicionais de cifra de bloco. O referido modo de operação caótico da presente invenção permite a propagação de erro (quando o algoritmo de criptografia objeto da presente invenção é implementado em sua forma

sequencial). Até hoje, o único modo de operação para cifras de bloco que possibilitou permitir a propagação de erro foi o PCBC (Virgil Gligor, "Integrity-Aware PCBC Encryption Schemes". Lecture Notes In Computer Science, V 1796/200, pp: 169-171, 2000 DOI - 10.1007/10720107_23). Entretanto, atualmente ele já foi quebrado e está em desuso. No ano de 2000 (Charanjit S. Jutla, "Encryption Modes with Almost Free Message Integrity", Proc. Eurocrypt 2001, LNCS 2045, May 2001) uma abordagem alternativa surgiu para se descobrir a intregridade de uma mensagem criptografada gerando um MAC - Message Authentication Code (ref-MAC - especificação da IEEE). Uma sequência de bits gerada durante o processo de criptografia informa se a mensagem criptografada é autêntica (porém, não informa a partir de que parte da mensagem houve a alteração da mesma ou não). Tais algoritmos geradores de MAC apesar de garantirem a integridade da mensagem, não informam em que ponto a mensagem foi alterada. No caso do modo de operação descrito na presente patente é possível saber com precisão o ponto em que a mensagem foi alterada.

O método da presente invenção consiste em utilizar o sistema dinâmico caótico como um pseudo gerador de números aleatórios.

A Figura 1 é um diagrama de blocos representativo da implementação da metodologia da presente invenção. Nesse diagrama, as entradas do método são os itens (1, 3, 11 e 12) e as saídas são os itens (8, 10). Como entrada tem-se a senha (1) que é uma sequência de caracteres e também cada um dos caracteres (3, 11, 12) da mensagem a ser criptografada. É importante lembrar que no caso de sinais ou arquivos estes caracteres serão denominados bytes. Para simplificar vamos considerar a entrada como texto e chamá-los de caractere. Cada caractere é separado para entrar em um determinado ponto do diagrama. Isto é necessário para o modo de operação caótico, que utiliza o caractere anterior como combinação para criptografar o caractere seguinte.

O diagrama da Figura 1 compreende o bloco 1° CIFRADOR que tem como entrada a senha (1), o caractere 1 (3) e como saída o caractere cifrado 1 (8) e o bloco de 1° MODO DE OPERAÇÃO CAÓTICO que recebe o caractere 1 (3) o transforma em parâmetro (7) e o encaminha para a soma (9) de onde é alimentado como vetor de parâmetro para o bloco 2° CIFRADOR.

Primeiramente, a senha (1) é transformada em um vetor de parâmetros em (2) com valores reais (ponto flutuante). O número de parâmetros extraídos da senha (1) depende do número de parâmetros utilizados no sistema dinâmico, uma vez que o método da presente invenção tem possibilidade de utilizar qualquer sistema caótico dinâmico. Estes parâmetros extraídos da senha (1) alimentam o sistema dinâmico do bloco 1° CIFRADOR que realiza x iterações em (4). O parâmetro x é determinado pelo

método da invenção e pode variar para cada programa. Alterando o valor de x, todo o resultado do processo é alterado. Com isso x é um parâmetro que pode ser utilizado para personalizar o método da presente invenção ou ainda explorado para torná-lo mais seguro. O parâmetro X é arbitrário. Ele pode ser utilizado para personalizar o método para diferentes clientes. Por exemplo, supondo que uma empresa utilize o método da presente invenção para o fornecimento de sistemas de criptografia a referida empresa poderia vender os sistemas de criptografia como exclusivos para clientes apenas alterando o parâmetro X. Neste caso a empresa utilizando o método da presente invenção compila e vende um par de programas de criptografia e decriptografia com X valendo um valor específico para um cliente e alterando o valor de X a referida empresa poderia vender um sistema de criptografia para outro cliente como exclusivo também. O parâmetro do primeiro cliente não funcionaria com o parâmetro do segundo cliente, ou seja, somente pode-se fazer o processo de criptografia-decriptografia com o mesmo X.

O sistema dinâmico em (4) irá retornar um vetor de parâmetros como resultado. Este vetor de parâmetros é enviado como entrada para o bloco 1° modo de operação caótico e também para cifrar o primeiro caractere em (5) transformando o vetor em dois caracteres. Para cifrar o caractere 1 (3) é realizada uma operação algébrica qualquer (6) que permite combinar os caracteres ou bytes recebidos de (5). Qualquer operação que possua uma inversa com correspondência biunívoca (por exemplo, a+b mod 2^8 para n=8 (8 bits)). Ou qualquer operação que apresente a propriedade de que para qualquer elemento (dentro do grupo de elementos) operado com ele mesmo de o elemento neutro da operação (operação xor - ou exclusivo). Como exemplo, utilizamos a função XOR, mas poderia ser qualquer outra que possuísse inversa (como explicado anteriormente). Os parâmetros do sistema dinâmico são transformados em um caractere por meio de uma função que transforma os elementos reais do vetor em um número inteiro (que varia de 0 a 255). Este valor é combinado com o caractere 1 e é realizada a cifragem do caractere 1 (3), gerando o caractere cifrado 1 (8). No bloco 1° modo de operação caótico, o caractere 1 (3) será transformado em um vetor de parâmetros em (7) e este vetor de parâmetros será combinado com o vetor de parâmetros oriundo do 1° cifrador. Esta combinação pode ser realizada com uma função algébrica (9) qualquer. Neste caso utilizamos uma operação aritmética de soma, mas poderia ser uma função mais complexa.

O procedimento descrito acima para o 1° CIFRADOR e o 1° MODO DE OPERAÇÃO CAÓTICO com relação ao caractere 1 se repete para os demais caracteres. O que muda nos demais blocos é alimentação do bloco cifrador. No 2° CIFRADOR que realiza a cifragem do caractere 2 (11) ao invés de receber o vetor de parâmetros da

senha (1), o 2° CIFRADOR recebe o vetor de parâmetros do bloco 1° MODO DE OPERAÇÃO CAÓTICO relativo ao caractere anterior (no caso o caractere 1) para alimentar o sistema dinâmico (4). Este procedimento se repete para todos os n caracteres.

Uma vez que o modo de operação caótico do método da presente invenção utiliza o caractere anterior no processo de criptografia, o conjunto de blocos para cifrar o último caractere, n° caractere, não possui o bloco modo de operação caótico, mas apenas o bloco n° CIFRADOR.

O diagrama de blocos da Figura 2 é semelhante ao diagrama de blocos da Figura 1, apresentando a mesma composição e funcionamento. A diferença entre os mesmos está na representação dos caracteres de entrada e de saída. Na Figura 2 o caractere cifrado 1 (8) de entrada e o caractere 1 (3) de saída estão representados por bits. Deste modo, cada caractere tem 8 bits. O diagrama da Figura 2 ilustra a propagação de informação no sistema. Para ilustrar isto, foi marcado um bit (bit 4) no primeiro caractere. Este bit está sendo representado como um erro (sendo alterado de 1 para 0 ou vice-versa). Observa-se que a alteração de apenas um bit na mensagem original implica na alteração de todos os bits na sequência de cifragem. Observa-se que os bits dos caracteres cifrados 1 têm apenas uma alteração, entretanto, os bits dos próximos caracteres são influenciados por esta única alteração, podendo seus valores não corresponder à cifra sem o erro.

Esta propagação de informação na cifragem é um ponto forte dos algoritmos de criptografia, pois a dificuldade de decifragem é muito maior quando ocorre a propagação. Na Figura 2 o módulo MODO DE OPERAÇÃO CAÓTICO é responsável pela combinação da cifragem com a mensagem anterior, garantindo uma segurança muito maior da criptografia.

Na Figura 3, temos o mesmo exemplo, porém, nessa Figura 3 o sistema de criptografia é o mesmo, com a única exceção que o módulo MODO DE OPERAÇÃO CAÓTICO é retirado. Como ilustrado no diagrama de blocos da Figura 3, não ocorre propagação da informação. Observe que o bit com erro ou alterado influencia apenas o caractere correspondente à alteração, os demais permanecem com a mesma cifra, indicando que esta cifragem não é tão forte quanto aquela representada na Figura 2, podendo ser criptoanalisada facilmente.

EXPERIMENTOS COM O MÉTODO INVENTIVO

Dois experimentos foram realizados em computador que mostram a eficiência da metodologia de criptografia da presente invenção.

As Figuras 4 a 7 mostram os resultados obtidos com o método de criptografia

proposto na presente invenção.

Foram considerados dois exemplos para o método de criptografia: (a) Criptografia de Texto e (b) Criptografia de Imagem.

Criptografia de Texto:

Uma metodologia tradicional para a análise de criptografia e tentativa de quebrar cifras é por meio da análise de frequência e busca de padrões nas mensagens criptografadas. Deste modo, quanto maior é a mensagem codificada, mais fácil é quebrar a sua cifra. Para pegar um texto longo, foi adotado o livro "The Return of Sherlock Holmes".

A Figura 4a apresenta o histograma de frequência em que os caracteres do livro aparecem. Observe que surgem padrões, relativos à língua inglesa. Por exemplo, a letra E é a mais utilizada. Seguindo tais padrões, poderia ser comparada uma mensagem codificada e tentar localizar os códigos ou quebrar a cifra. Nas Figuras 4b e 4c são apresentados os histogramas de frequência do texto codificado usando o método proposto na presente invenção com as senhas: "123456" e "123457", respectivamente.

Pode ser observado facilmente que não é possível verificar nenhum tipo de padrão no histograma, sendo que o mesmo apresenta uma distribuição regular e próxima de ruído constante. Comparando as Figuras 4b e 4c, também pode ser facilmente verificado que houve grande variação nos histogramas, o que demonstra a influência do código cifrado pela senha. Esta variação mostra que a senha altera o padrão de codificação de toda a mensagem, o que também garante segurança à criptografia. Outra medida importante é a entropia. Uma vez que cada caractere do texto é codificado em ASCII com 8bits (256 caracteres), a entropia máxima, ou seja, o máximo de embaralhamento do sistema é 8. A mensagem criptografada pelo método proposto na presente invenção apresentou uma entropia igual a 8, sugerindo deste modo embaralhento máximo.

Outra possibilidade de encontrar padrões nos textos é verificar a correlação entre os caracteres. Por exemplo, as sequências de caracteres em português, "mp", "qu", "rr" e "ss" aparecem com mais frequência do que "ax" "zb" ou "sf". A matriz de correlação sugere quais são as letras ou caracteres que possuem mais correlação, ou seja, que se apresentam correlacionados no texto. As Figuras 5a, 5b e 5c mostram, respectivamente, a matriz de correlação do texto plano, a matriz de correlação do texto codificado pelo método proposto na presente invenção e a matriz de correlação entre o ruído uniforme. Como pode ser observado, o texto plano apresenta correlações fortes entre alguns caracteres, conforme apresentado pelos picos, o que sugere um padrão de correlação da língua do texto, no caso a língua inglesa. Já nas Figuras 5b e 5c, a correlação apresenta

uma distribuição sem padrões e de forma regular em todas as combinações indicando que o código criptografado apresenta uma correlação próxima de um ruído uniforme. Isto sugere que o método proposto na presente invenção foi capaz de eliminar os padrões de correlações presentes na mensagem original, de modo a impossibilitar a recuperação da mesma por análise criptográfica.

Criptografia de imagem

Além dos textos, as imagens podem ser outra possibilidade para validar um método de criptografia. Neste caso, a vantagem das imagens é a facilidade de verificar padrões visuais na mesma. A Figura 6 apresenta os resultados da criptografia de uma imagem e sua comparação com ruído uniforme. Na Figura 6a é apresentada a imagem a ser considerada no experimento, na Figura 6b é apresentada a imagem após ser codificada pelo método proposto na presente invenção e na Figura 6c é apresentada uma imagem de ruído uniforme. Numa primeira análise pode ser facilmente observado que não é possível verificar nenhum tipo de padrão visual em 6b e 6c, sugerindo que a informação codificada é semelhante a um ruído uniforme. Para quantificar esta análise foi realizada a análise da frequência com que aparecem os pixels na imagem. Isto pode ser feito por um histograma que quantifica a frequência com que uma intensidade de cinza (variando de 0 a 255) ocorre na imagem. As Figuras 6d, 6e e 6f apresentam, respectivamente, os histogramas da imagem original, codificada e do ruído. Observe que em 6d existe um padrão definido no histograma, ao passo que o histograma da imagem codificada e o ruído uniforme apresentam padrões semelhantes, o que indica que não existe correlação entre a intensidade dos pixels; sugerindo que a informação presente na imagem codificada é tão inteligível quanto o ruído. Ainda uma possibilidade de análise das imagens é considerar cada linha e cada coluna como um sinal e aplicar a transformada de Fourier na mesma. A transformada de Fourier apresenta o espectro da frequência, ou seja, os componentes (cossenos) necessários para compor um sinal. Por meio desta análise pode-se verificar quais as componentes de um sinal e sua frequência. As Figuras 6g, 6h e 6i apresentam, respectivamente, o logaritmo da potência do espectro de Fourier da imagem original, codificada e do ruído. Observe que os componentes de sinais da imagem podem ser identificados e quantificados no espectro. Por outro lado não foi observado padrão nos componentes do espectro da imagem codificada e do ruído. O que indica um alto nível de embaralhamento do método de criptografia da presente invenção; sugerindo que as informações lá contidas são tão inteligíveis quanto o ruído.

Desempenho (tempo de execução de um programa)

Um dos problemas que impedem a utilização de métodos de criptografia baseados em caos é o seu alto tempo de processamento. Uma vez que algoritmos de

criptografia podem criptografar mensagens, sinais ou arquivos de computador com tamanhos que podem apresentar grande volume de dados, uma necessidade é que o programa seja rápido. Os programas baseados em métodos de criptografia baseados em caos são muito mais lentos que a criptografia tradicional.

O método proposto na presente invenção faz uso de computação paralela, ou seja, permite rodar em várias unidades de processamento simultaneamente, de modo a aumentar o seu desempenho e permitir a sua utilização no tempo adequado para aplicações comerciais.

Na Figura 7, são apresentados os gráficos do tempo de execução do método proposto na presente invenção. Na Figura 7a é apresentado o tempo de execução da versão sequencial do algoritmo, ou seja, sendo executada passo a passo em uma única unidade de processamento. O gráfico apresenta em seu eixo vertical o tempo em minutos e no eixo horizontal o volume de dados. Na Figura 7b é apresentado o tempo de execução do algoritmo paralelo rodando em uma placa de vídeo. São utilizados os processadores da placa de vídeo, de modo que o programa é executado em paralelo, ou seja, ao mesmo tempo nos 200 processadores da placa. Esta abordagem faz com que o programa fique muito mais rápido que a versão sequencial. Na Figura 7b é também apresentado o tempo de execução do método de criptografia AES. O AES utiliza criptografia convencional e é utilizado comercialmente. Observa-se que o tempo do método proposto na presente invenção apresenta desempenho relativamente próximo ao AES, o que indica que está apto a aplicações comerciais.

REINVIDICAÇÕES

1. Método de criptografia em modo de operação caótico, **caracterizado pelo** fato de que compreende:

em um 1° cifrador:

entrar uma senha (1) em um transformador (2) de senha em vetor de parâmetros e entrar um caractere 1 (3) no operador algébrico (6);

entrar o vetor de parâmetros obtido em (2) em um calculador do sistema dinâmico caótico (4) para obter um vetor de parâmetros a ser entrado no 1° modo de operação caótico e no transformador (5) de vetor de parâmetros em dois caracteres;

entrar os caracteres obtidos em (5) no operador algébrico (6) para juntamente com o caractere 1 (3) obter o caractere cifrado 1 (8);

em um 1° modo de operação caótico:

entrar o caractere 1 (3) no transformador (7) de parâmetros para gerar um vetor de parâmetros que é entrado no operador de soma (9) que também recebe o vetor de parâmetros obtido em (4) no 1° cifrador e gera um vetor de parâmetros a ser entrado no próximo cifrador;

em um 2° cifrador:

entrar o vetor de parâmetros obtido no operador de soma (9) no calculador do sistema dinâmico caótico (4) para obter um vetor de parâmetros a ser entrado no 2° modo de operação caótico e no transformador (5) de vetor de parâmetros em dois caracteres;

entrar os caracteres obtidos em (5) no operador algébrico (6) para juntamente com o caractere 2 (11) obter o caractere cifrado 2 (10);

em um 2° modo de operação caótico:

entrar o caractere 2 (11) no transformador (7) de parâmetros para gerar um vetor de parâmetros que é entrado no operador de soma (9) que também recebe o vetor de parâmetros obtido em (4) no 2° cifrador e gera um vetor de parâmetros a ser entrado no próximo cifrador; e

em um n° cifrador:

entrar o vetor de parâmetros obtido no operador de soma (9) no calculador do sistema dinâmico caótico (4) para obter um vetor de parâmetros a ser entrado no transformador (5) de vetor de parâmetros em dois caracteres;

entrar os caracteres obtidos em (5) no operador algébrico (6) para juntamente com o caractere n (12) obter o caractere cifrado n (13).

2. Método, de acordo com a reivindicação 1, **caracterizado pelo** fato de que o operador algébrico (6) pode incluir qualquer operação algébrica que possua inversa.

3. Método, de acordo com a reivindicação 1, **caracterizado pelo** fato de que:

no 1° cifrador um caractere cifrado 1 (8) entra na operação algébrica inversa (14) para obter um caractere 1 (3);

no 1° modo de operação caótico o caractere 1 (3) entra no transformador (7) para gerar um vetor de parâmetros;

no 2° cifrador um caractere cifrado 2 (10) entra na operação algébrica inversa (14) para obter um caractere 2 (11);

no 2° modo de operação caótico o caractere 2 (11) entra no transformador (7) para gerar um vetor de parâmetros; e

no n° cifrador um caractere cifrado n (13) entra na operação algébrica inversa (14) para obter um caractere n (12) para gerar um cifra com erro.

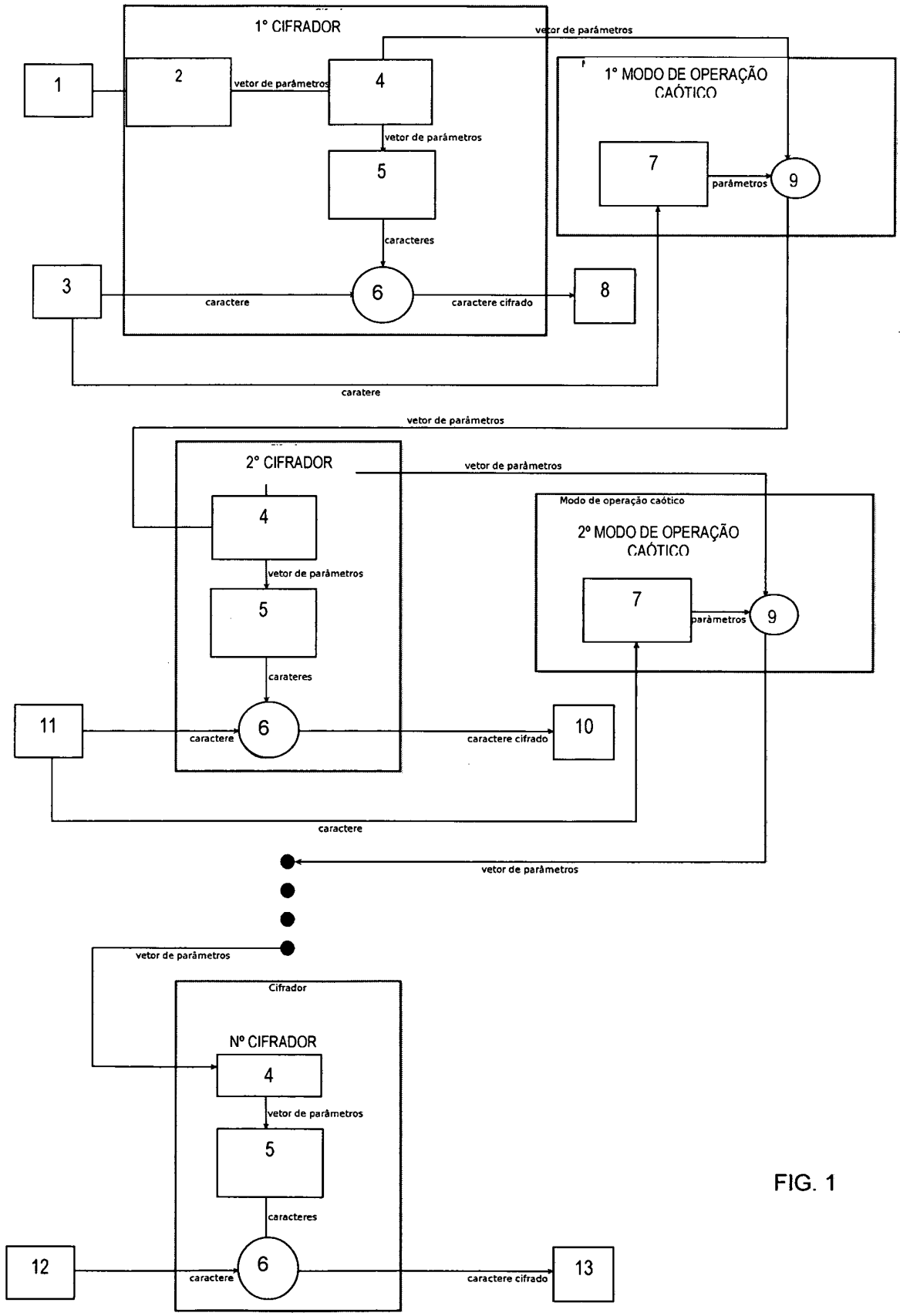

1° CIFRADOR
vetor de parâmetros
1° MODO DE OPERAÇÃO CAÓTICO
1
2
vetor de parâmetros
4
vetor de parâmetros
5
caracteres
7
parâmetros
9
3
caractere
6
caractere cifrado
8
caratere
vetor de parâmetros
2° CIFRADOR
vetor de parâmetros
Modo de operação caótico
2° MODO DE OPERAÇÃO CAÓTICO
4
vetor de parâmetros
5
carateres
7
parâmetros
9
11
caractere
6
caractere cifrado
10
caractere
vetor de parâmetros
vetor de parâmetros
Cifrador
Nº CIFRADOR
4
vetor de parâmetros
5
caracteres
12
caractere
6
caractere cifrado
13

FIG. 1

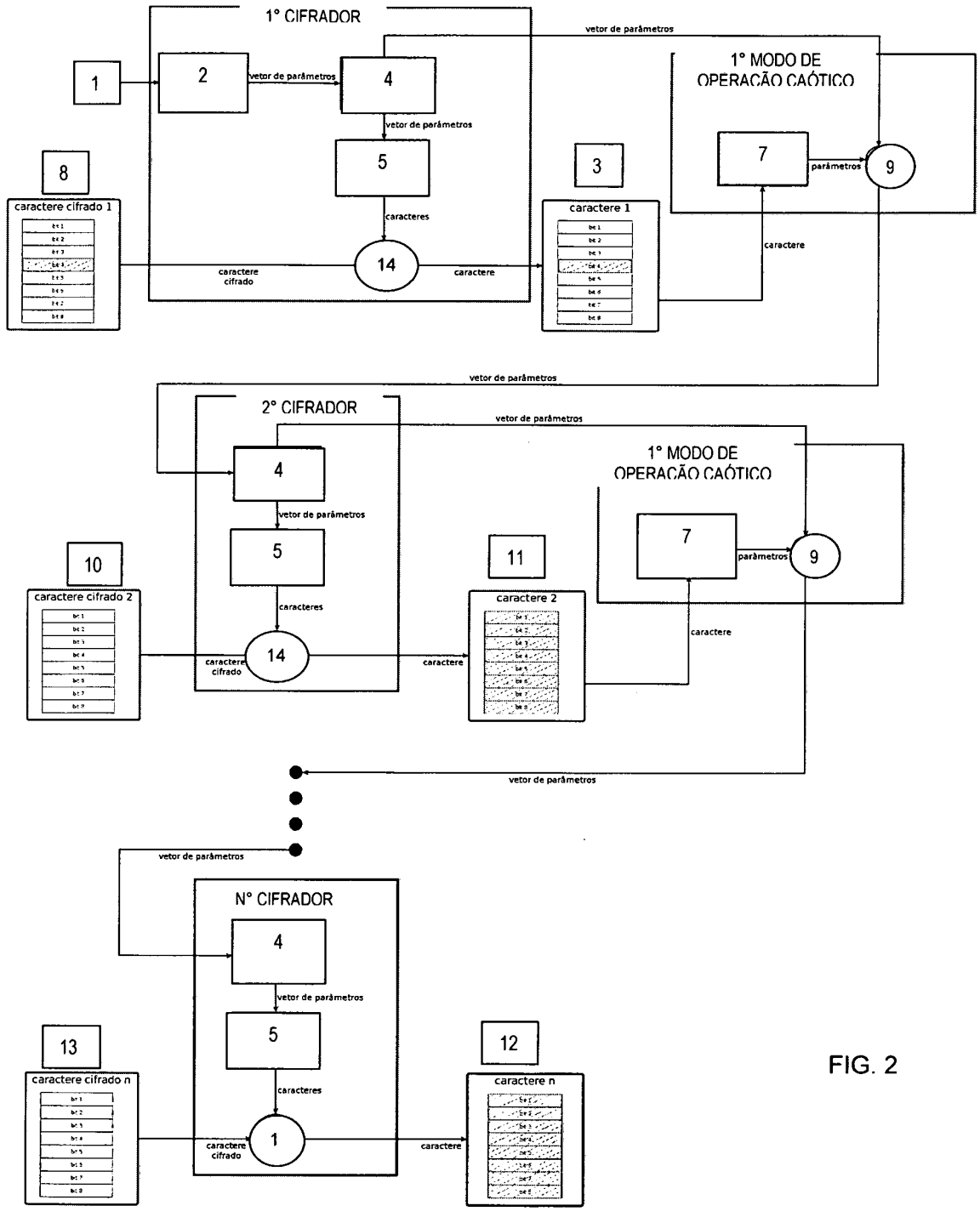

1° CIFRADOR
vetor de parâmetros
1° MODO DE OPERAÇÃO CAÓTICO
1
2
vetor de parâmetros
4
vetor de parâmetros
5
caracteres
8
caractere cifrado 1
caractere cifrado
14
caractere
3
caractere 1
7
parâmetros
9
caractere
vetor de parâmetros
2° CIFRADOR
vetor de parâmetros
1° MODO DE OPERAÇÃO CAÓTICO
4
vetor de parâmetros
5
caracteres
10
caractere cifrado 2
caractere cifrado
14
caractere
11
caractere 2
7
parâmetros
9
caractere
vetor de parâmetros
vetor de parâmetros
N° CIFRADOR
4
vetor de parâmetros
5
caracteres
13
caractere cifrado n
caractere cifrado
1
caractere
12
caractere n

FIG. 2

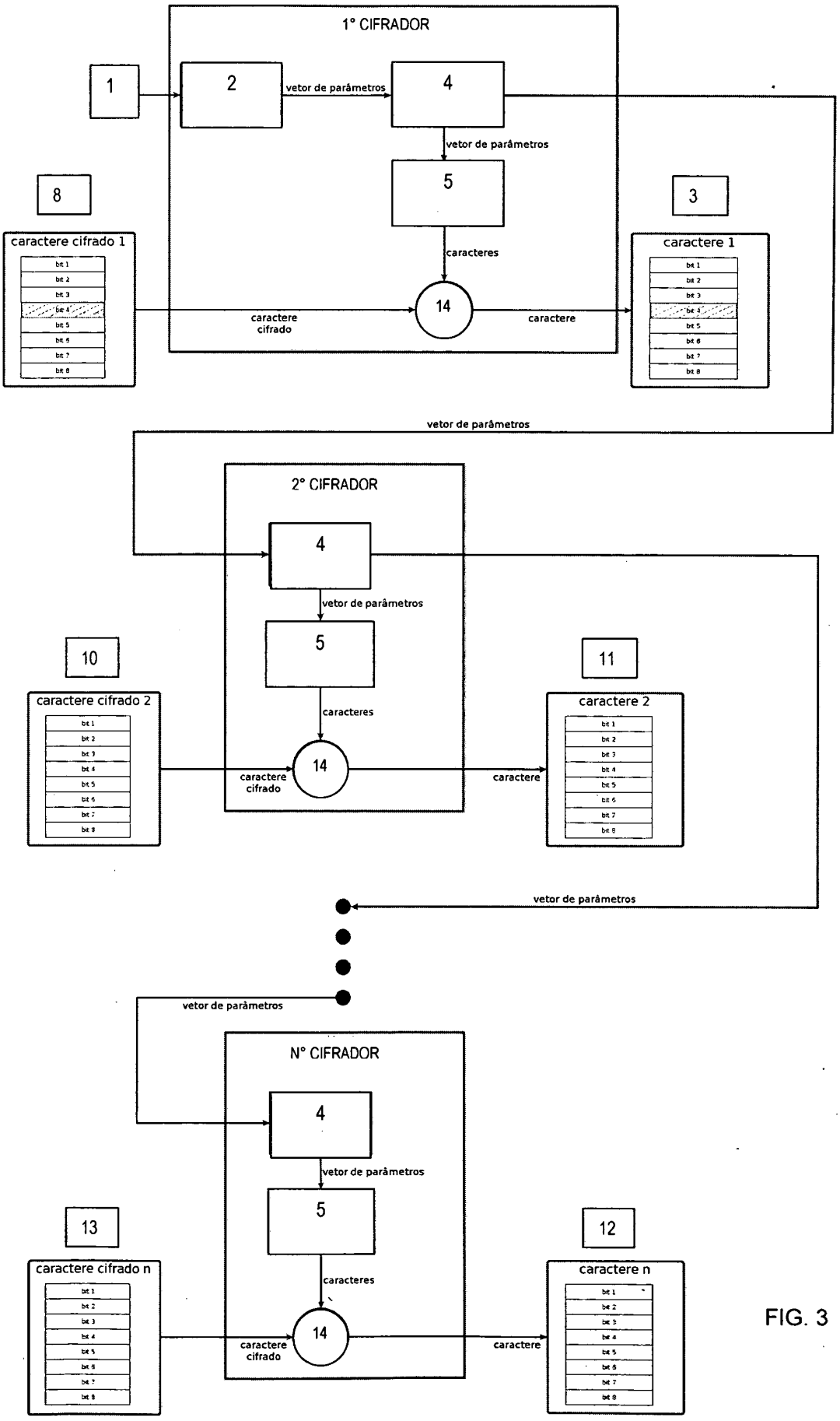

1° CIFRADOR
1
2
vetor de parâmetros
4
vetor de parâmetros
5
caracteres
8
caractere cifrado 1
3
caractere 1
caractere cifrado
14
caractere
vetor de parâmetros
2° CIFRADOR
4
vetor de parâmetros
5
caracteres
10
caractere cifrado 2
11
caractere 2
caractere cifrado
14
caractere
vetor de parâmetros
vetor de parâmetros
N° CIFRADOR
4
vetor de parâmetros
5
caracteres
13
caractere cifrado n
12
caractere n
caractere cifrado
14
caractere

FIG. 3

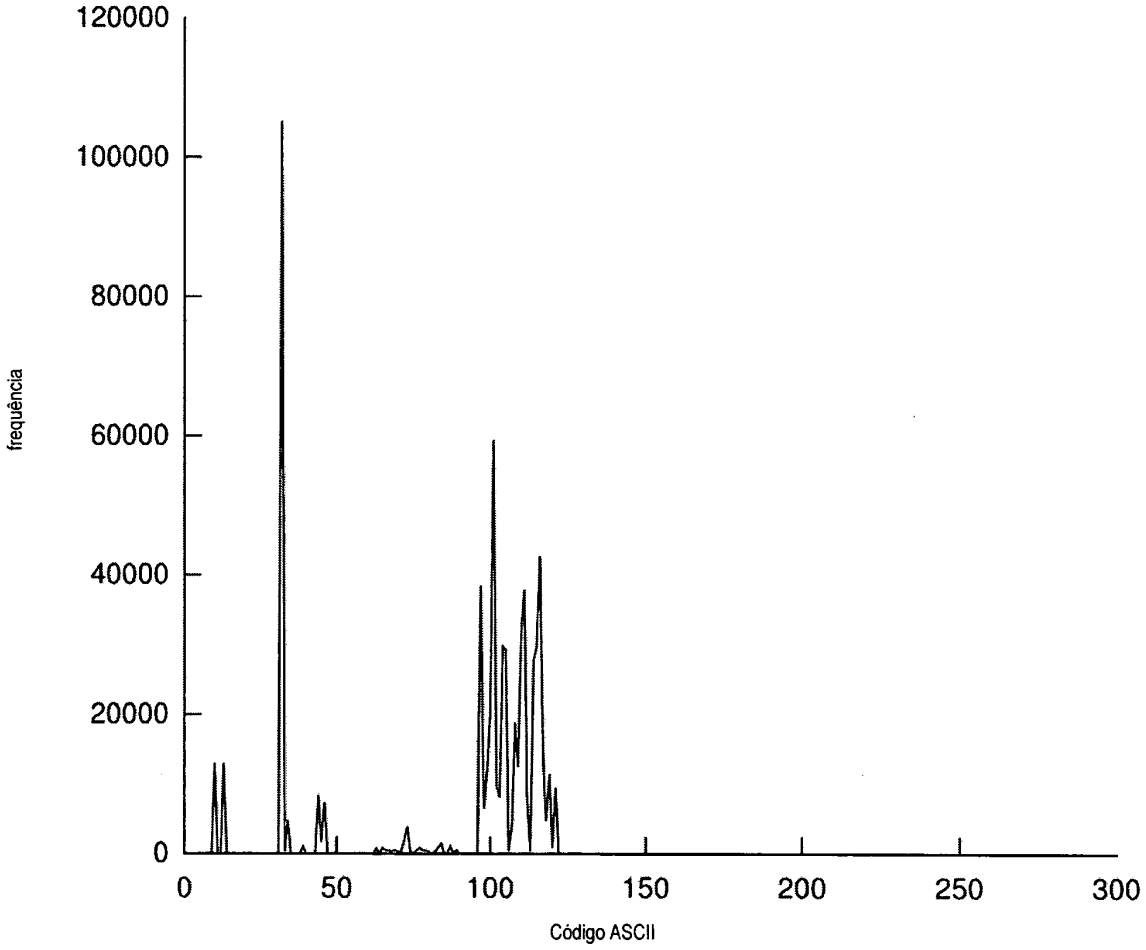

120000
100000
80000
60000
40000
20000
0
frequência
0
50
100
150
200
250
300
Código ASCII

FIG. 4a

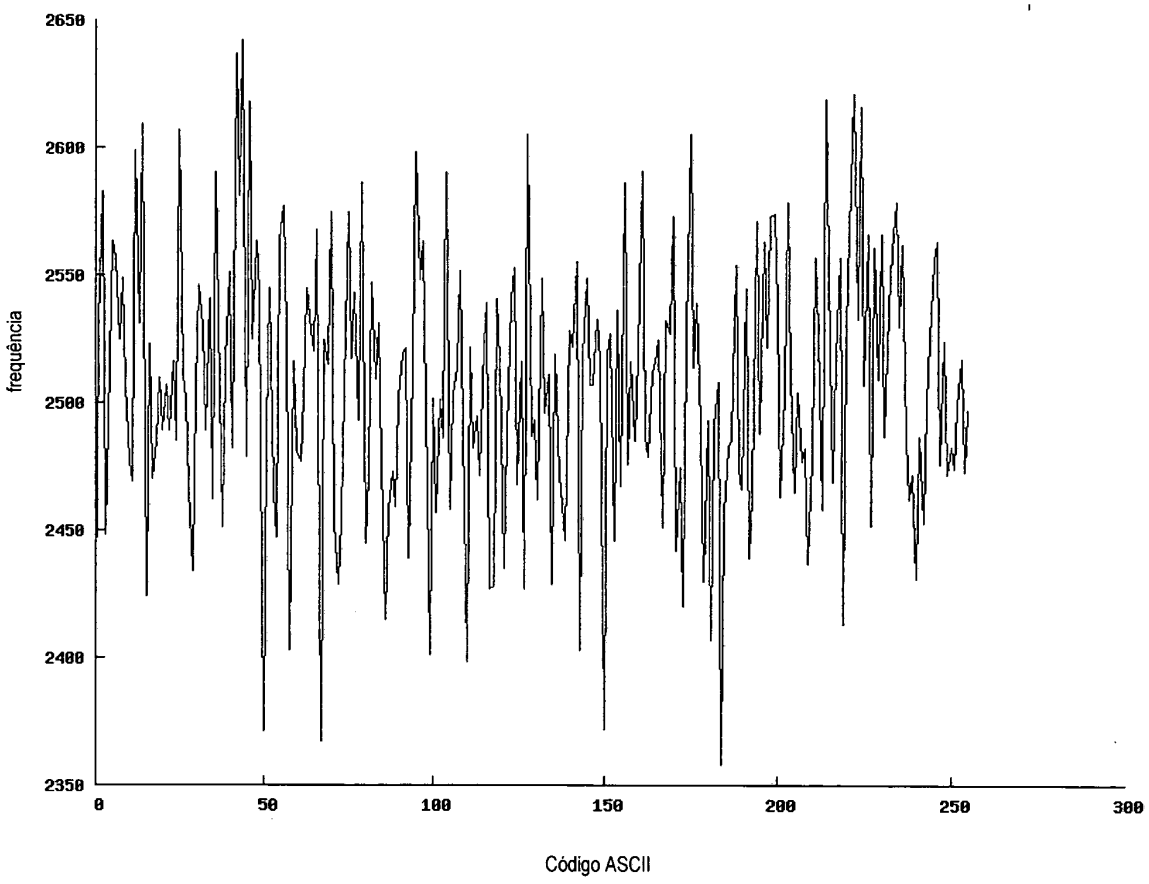

2650
2600
2550
2500
2450
2400
2350
frequência
0
50
100
150
200
250
300
Código ASCII

FIG. 4b

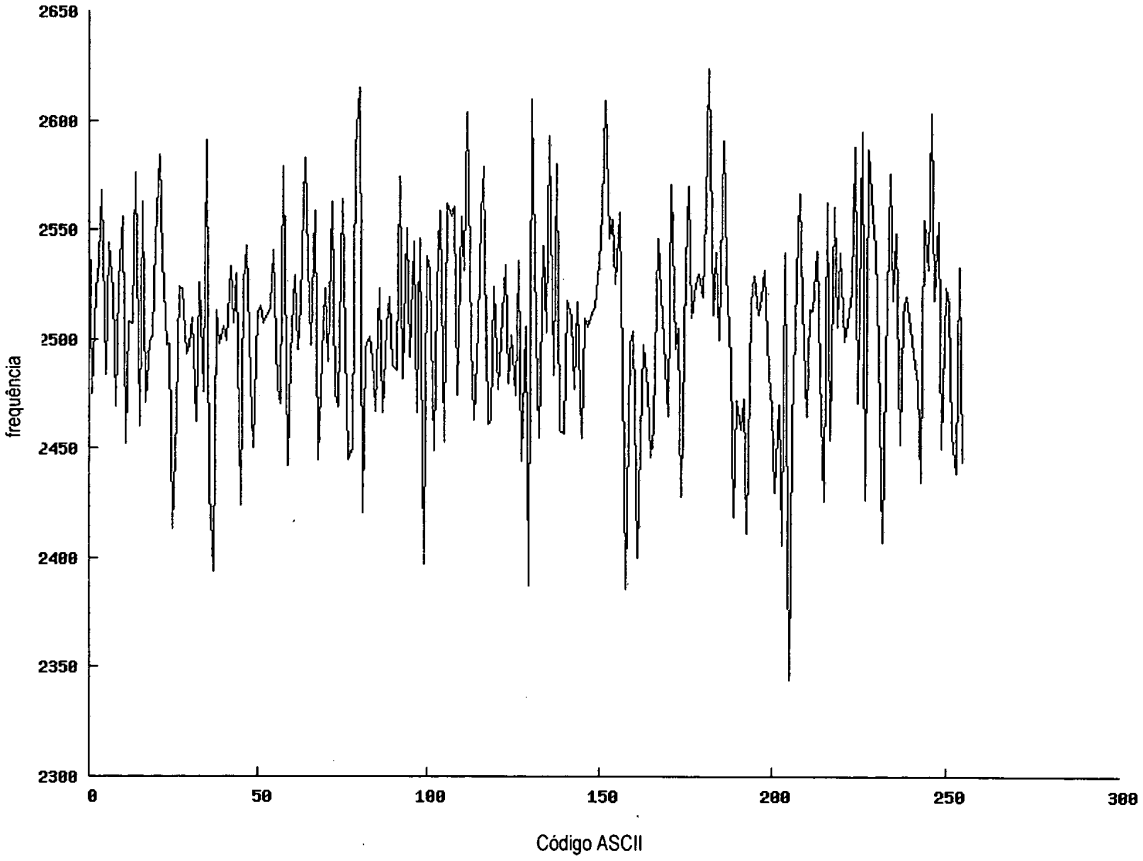

2650
2600
2550
2500
2450
2400
2350
2300
frequência
0
50
100
150
200
250
300
Código ASCII

FIG. 4c

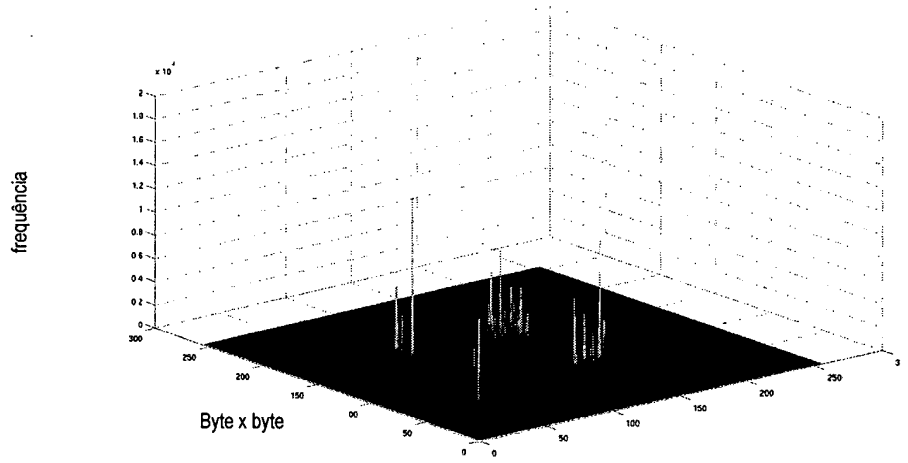


FIG. 5a

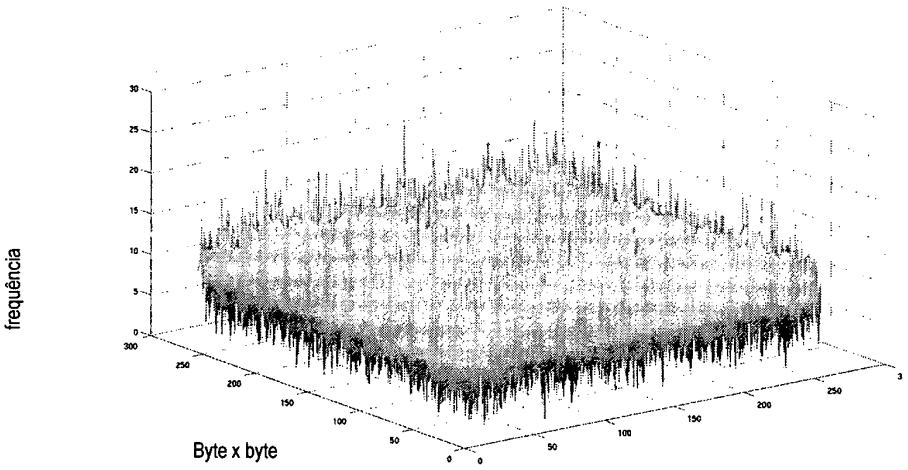


FIG. 5b

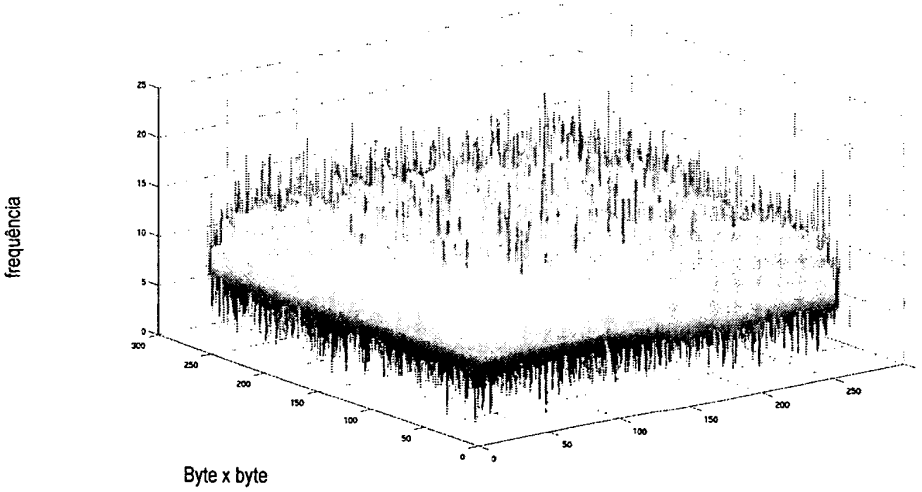


FIG. 5c

FIG. 6a

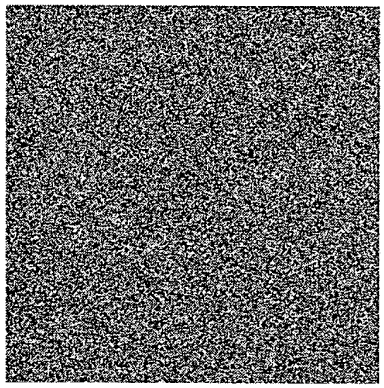


FIG. 6b

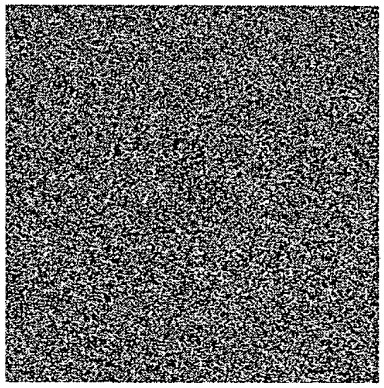


FIG. 6c

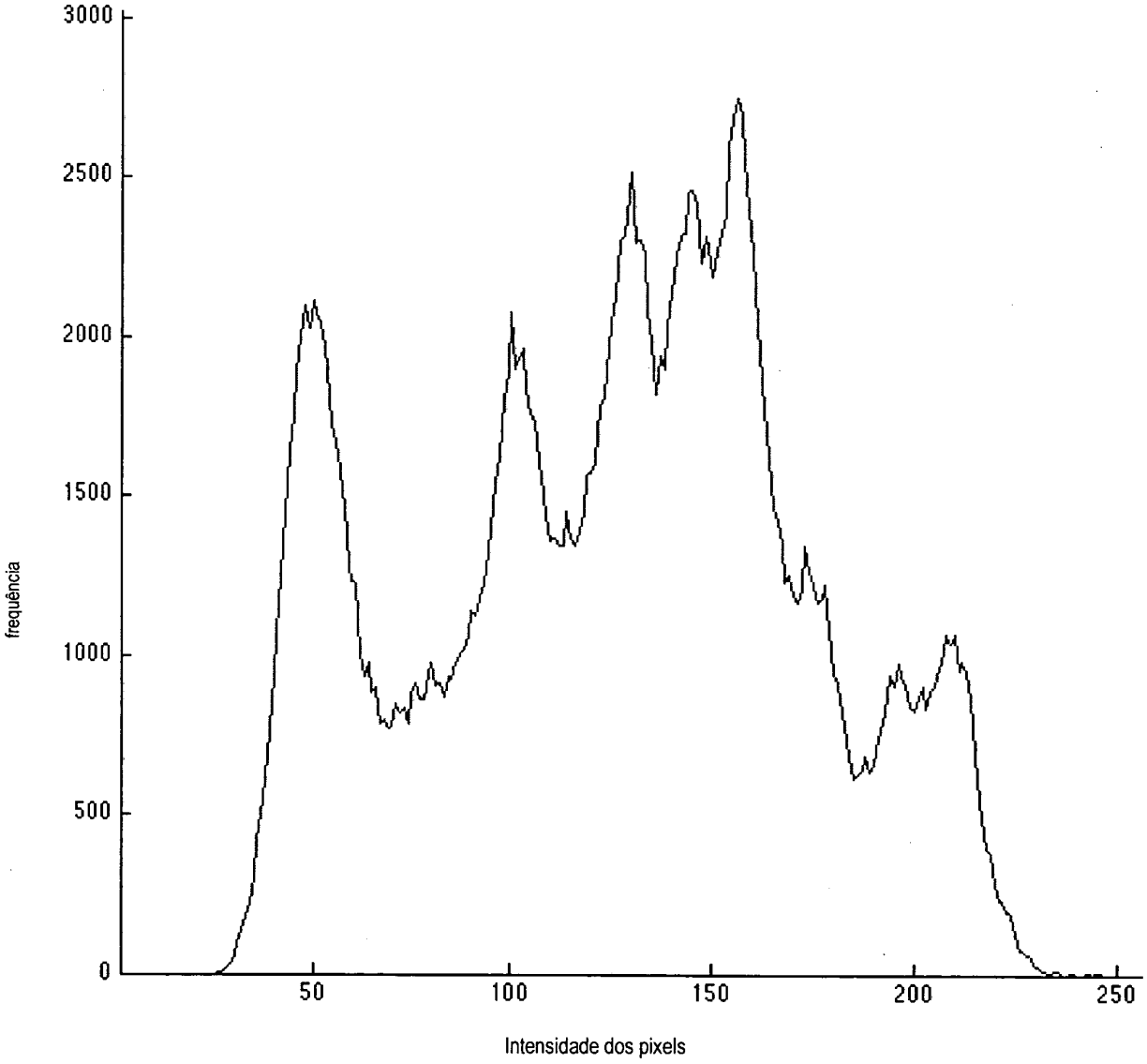

3000
2500
2000
1500
1000
500
0
frequência
50
100
150
200
250
Intensidade dos pixels

FIG. 6d

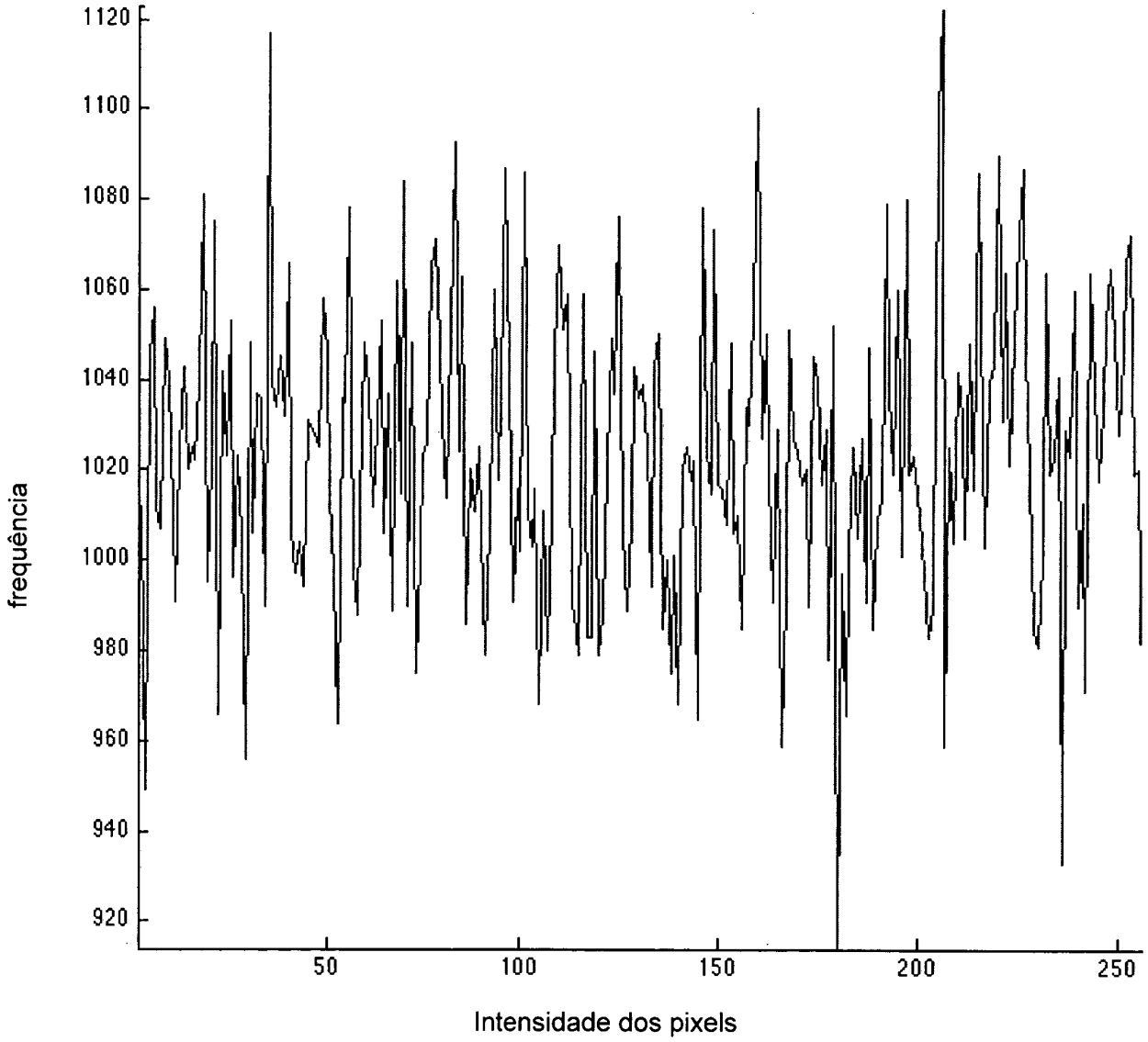

1120
1100
1080
1060
1040
1020
1000
980
960
940
920
frequência
50
100
150
200
250
Intensidade dos pixels

FIG. 6e

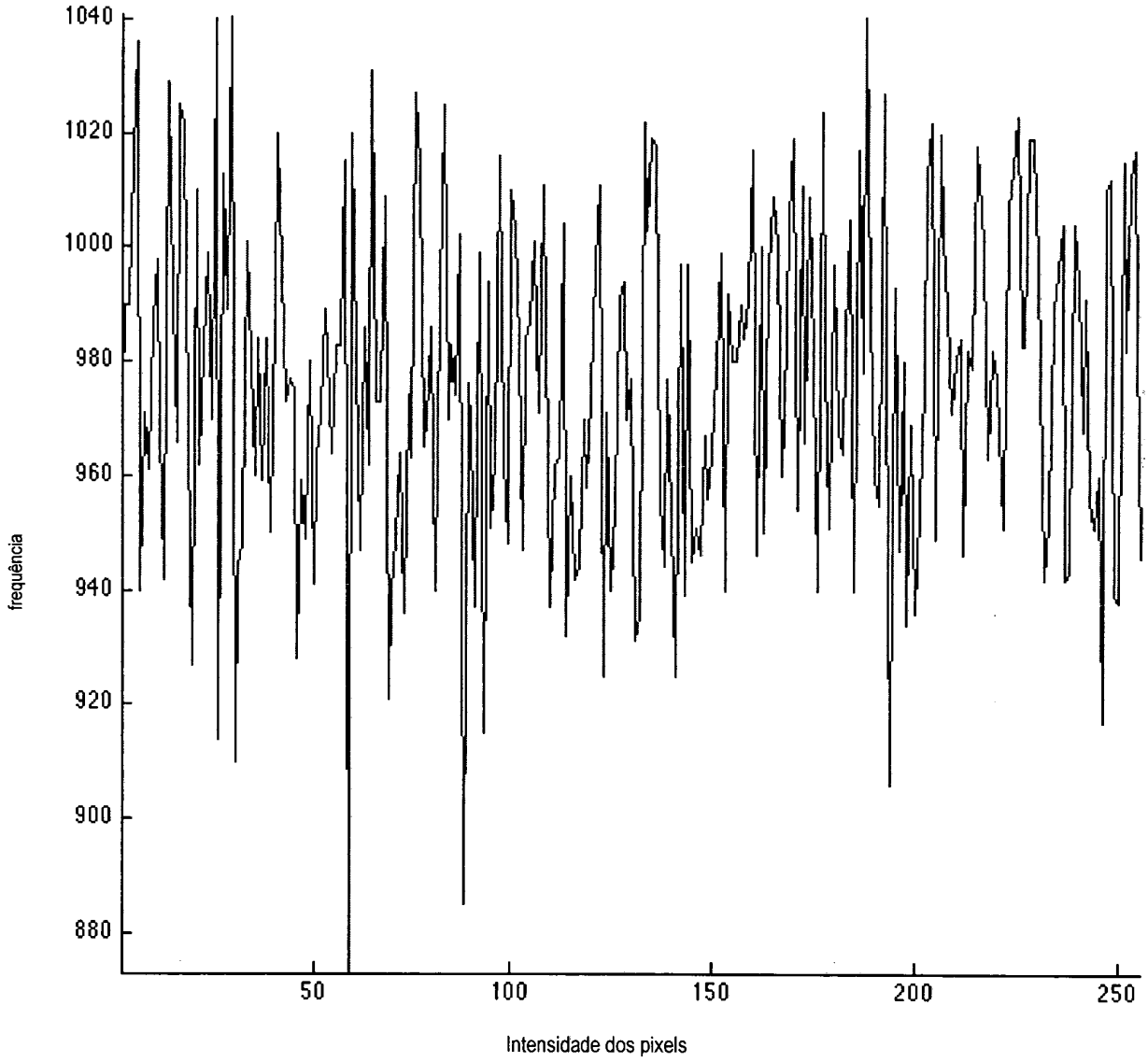

1040
1020
1000
980
960
940
920
900
880
frequência
50
100
150
200
250
Intensidade dos pixels

FIG. 6f

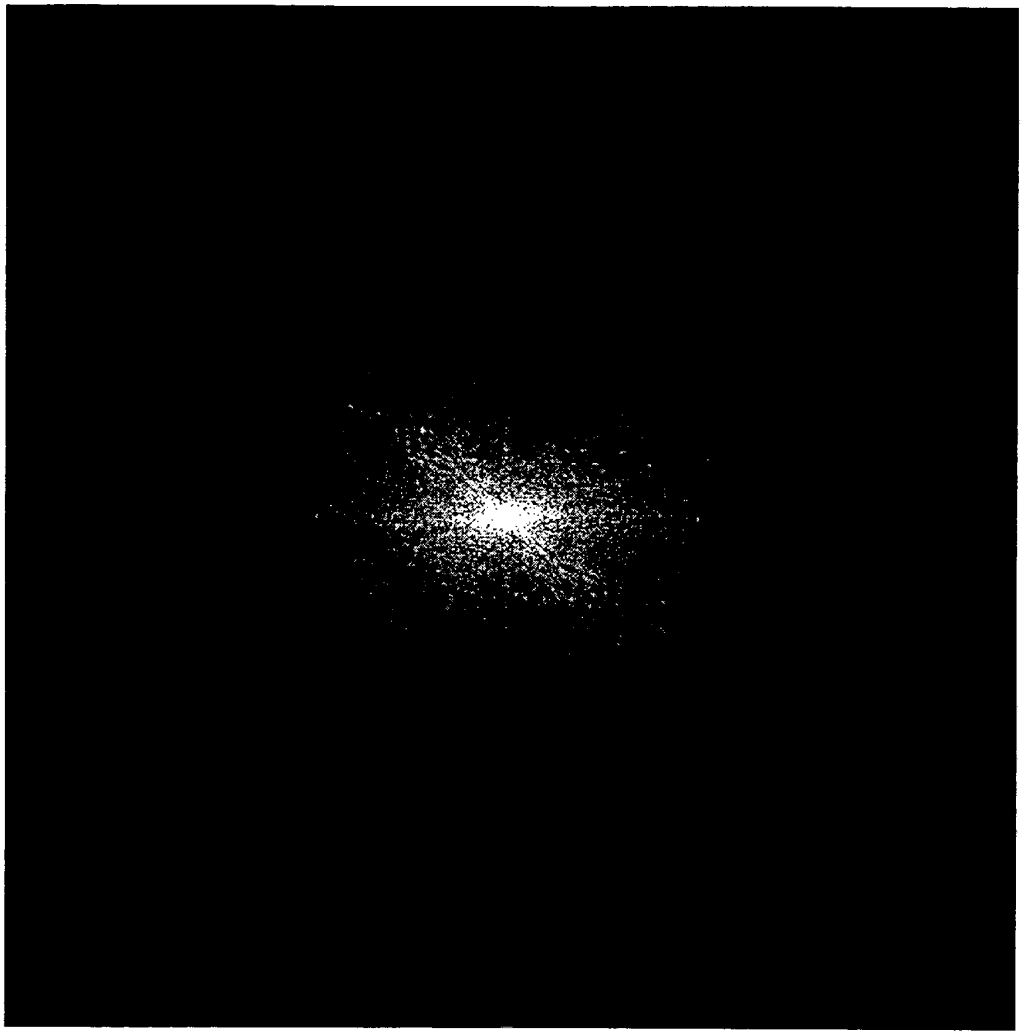


FIG. 6g

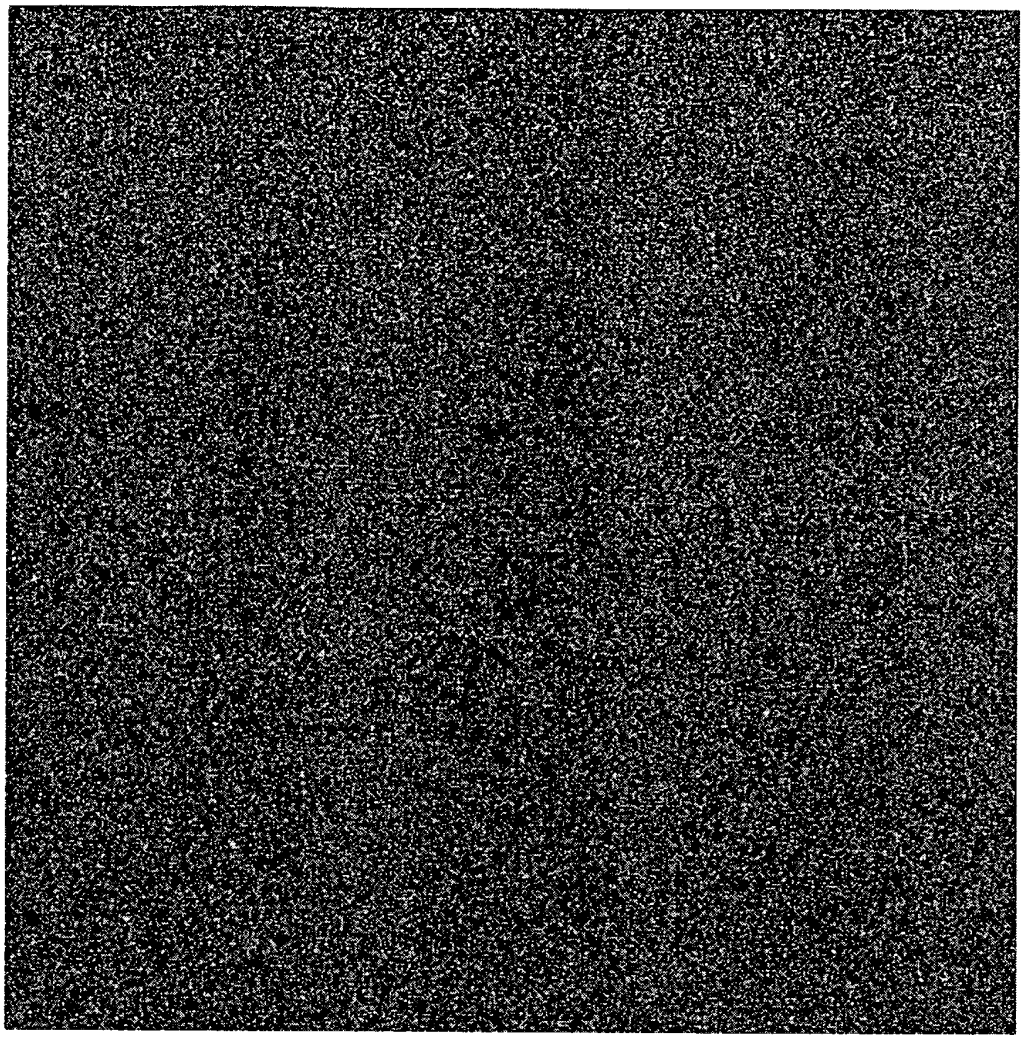


FIG. 6h

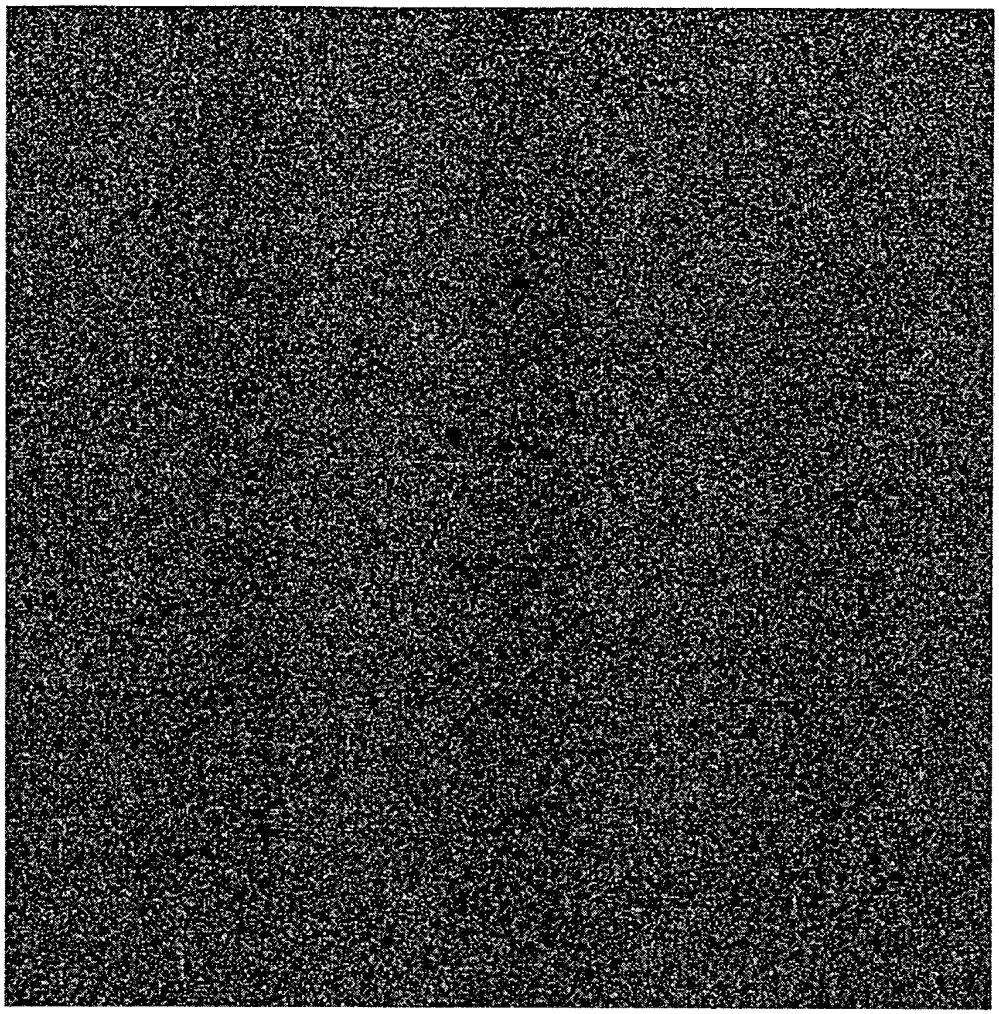


FIG. 6i

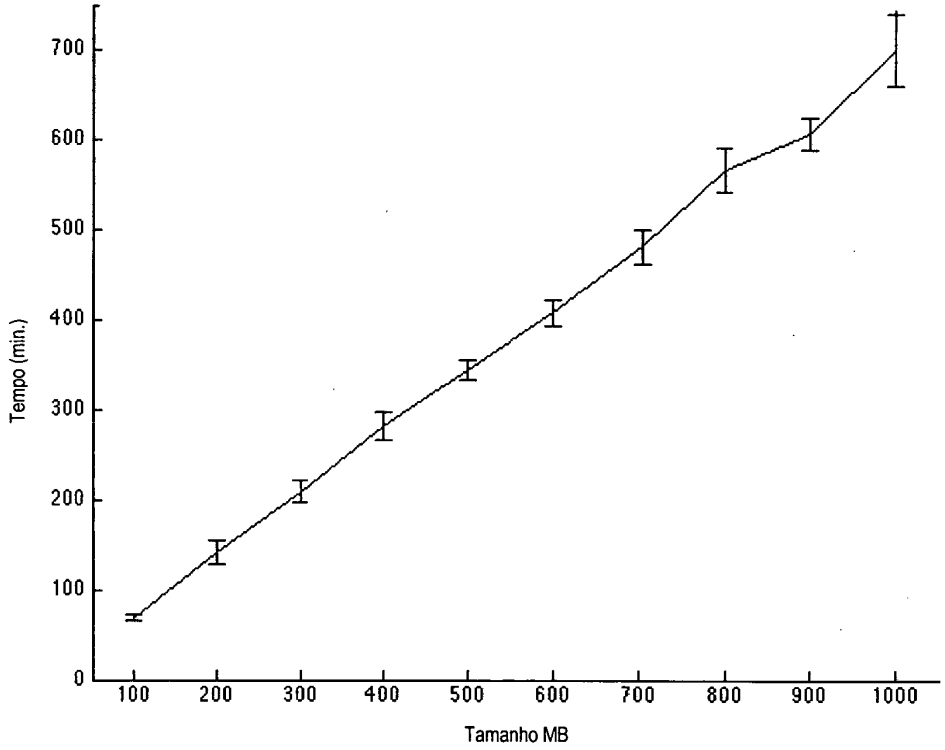

Tempo (min.)
0
100
200
300
400
500
600
700
100
200
300
400
500
600
700
800
900
1000
Tamanho MB

FIG. 7a

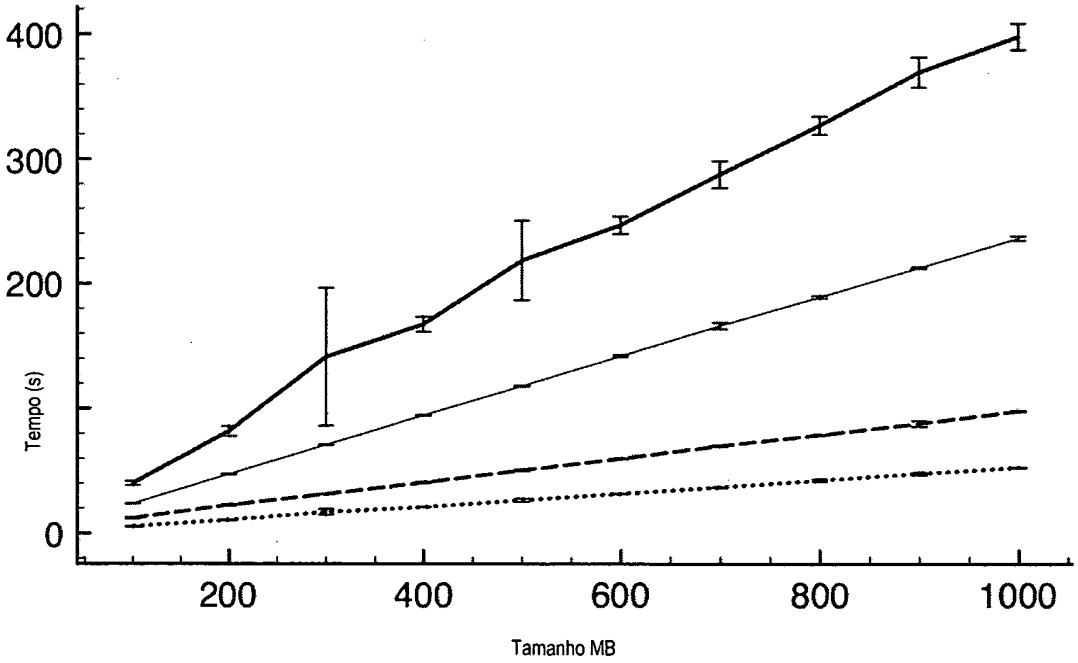

Tempo (s)
0
200
300
400
200
400
600
800
1000
Tamanho MB

FIG. 7b

RESUMO

MÉTODO DE CRIPTOGRAFIA EM MODO DE OPERAÇÃO CAÓTICO

O invento proposto é de um algoritmo de criptografia de arquivos computacionais, baseado nas iterações dos mapas de sistemas dinâmicos no regime caótico. O algoritmo apresenta como características a segurança e o desempenho que o tornam especialmente adequado para o uso comercial. A segurança do algoritmo está baseada no uso de sistemas dinâmicos no regime caótico e também no modo de operação caótico. O algoritmo de criptografia baseado em sistemas caóticos tem como característica ser seguro, pela natureza matemática do caos. Entretanto, é muito fácil produzir um algoritmo de criptografia caótica com falhas de projeto que abrem brechas para criptoanálise. O método proposto apresenta também o modo de operação caótico que combina a mensagem a ser criptografada, a senha e o sistema caótico na codificação garantindo, assim, uma segurança sólida da criptografia gerada. O algoritmo proposto pode ser implementado para explorar o paralelismo de processadores principais, bem como da placa de vídeo (GPU) de modo a codificar e decodificar as mensagens com alto desempenho. O método proposto na presente invenção pode ser implementado em qualquer computador convencional, smartphones ou telefones celulares e eventualmente em outro dispositivo computacional.