CRIPFTOGRAFIA ASSIMÉTRICA DE IMAGENS UTILIZANDO ALGORITMO RSA

Bruno da Silva[*], Humberto Pessoa Almeida[*], Cintia Carvalho Oliveira[†] e Daniele Carvalho Oliveira[†]
[*]Universidade de Uberaba
Engenharia de Computação, Uberaba – Minas Gerais
E-mail: yirho@hotmail.com; humbertopessoa@edu.uniube.br
[†]Universidade Federal de Uberlândia; Universidade de Uberaba
Ciência da Computação, Uberlândia, Minas Gerais
E-mail: cintia@facom.ufu.br; daniele@cidaeli.com.br

Resumo - A transmissão de conteúdo gráfico pela Web, para ser confiável precisa mais do que a segurança da rede em si, mas o próprio conteúdo transmitido deve estar protegido. Métodos criptográficos proporcionam a segurança necessária ao converter o conteúdo de imagens para um equivalente criptográfico. Técnicas de criptografia simétrica como assimétrica podem ser utilizadas, porém o foco desse trabalho foi a análise de métodos com chave assimétrica. Foi analisada uma das técnicas mais utilizada, o algoritmo RSA, examinando seu comportamento em relação à criptografia de imagens.

***Palavras-Chave* – Criptografia de imagem; RSA; Segurança.**

ASYMMETRIC ENCRYPTION OF IMAGES USING RSA ALGORITHM

Abstract - The transmission of graphical content over the Web, need to be trusted more than the security of the network itself, but the actual streamed content must be protected. Cryptographic methods provide the necessary safety to convert the image content to a cryptographic equivalent. Symmetric encryption techniques can be used as asymmetric, but the focus of this work was the the analysis of asymmetric key methods . Was considered one of the techniques that are more used, the RSA algorithm, studying its behavior in relation to encryption of images.

***Keywords* - Image encryption, RSA, Security.**

I. INTRODUÇÃO

A criptografia permite estudar os métodos para codificar uma mensagem de modo que apenas seu destinatário legítimo consiga interpretá-la. Em grego, kryptós significa secreto e grápho se refere à escrita, portanto, a criptografia poderia ser definida como a ciência de se escrever em código secreto. [1]

Diffie e Hellman, em 1976, apresentaram a ideia de um sistema de criptografia de chave pública. Logo depois, em 1977, Ronald Rivest, Adi Shamir e Leonard Adleman, inventaram o famoso criptossistema RSA. O algoritmo RSA é denominado devido ao nome de seus autores, cujo trabalho foi primeiramente publicado em abril de 1977 [2].

Os criptossistemas de chave pública (assimétricos) tem a vantagem sobre os criptossistemas de chave privada (simétricos) pelo fato de que não é necessária a existência de um canal seguro para realizar o compartilhamento da chave pública. Mas, infelizmente, os criptossistemas de chave pública são muito mais lentos do que os sistemas de chave privada. Então, na prática, sistemas de chave privada são geralmente usadas para criptografar mensagens extensas.

O algoritmo RSA foi patenteado pelo M.I.T. em 1983 nos Estados Unidos, mas expirou em 21 de setembro de 2000. O RSA é, atualmente, o mais usado em aplicações comerciais. Este é o método utilizado, por exemplo, no Netscape, o mais popular dos softwares de navegação na Internet [3].

A Teoria da Complexidade Algorítmica estuda os aspectos relacionados aos recursos necessários (tais como tempo, espaço, número de bits e número de processadores) para resolver um determinado problema. Atualmente, os computadores resolvem problemas mediante algoritmos que tem uma complexidade ou custo computacional polinômico, que é menor que o custo computacional exponencial [3].

A segurança desta técnica é dada pelo fato da dificuldade em fatorar números primos extremamente grande. De acordo com o tamanho de chave escolhido é referenciado a um determinado nível de segurança, segundo o NIST – National Institute of Standard and Technology, uma chave RSA de 1024 bits não oferece segurança suficiente entre 2011 e 2019, ano cujo foi calculado para término de segurança pleno para a chave de 2048 bits, ou seja, não é recomendado uso de chave de 1024 bits.

Segundo Cavalcante (1997), Teoria dos números é uma ciência muito antiga, que visa primordialmente entender as propriedades e relações entre os números. Na busca de tais propriedades, surge uma grande interação entre este e

vários outros ramos da matemática pura (como Álgebra, Análise Real e Complexa, Geometria) e aplicada (como Ciência da Computação e Criptografia).

A criptografia RSA entre outras está entrelaçada com a Teoria dos números, pois, seu algoritmo é desenvolvido com duas ferramentas fundamentais que são o Algoritmo de Euclides Estendido e o Teorema do Resto Chinês.

As técnicas de criptografia em imagens encontram aplicação em ambientes em que, imagens confidenciais, como médicas, contratos, escrituras, mapas, entre outros, precisam ser armazenadas ou transmitidas através de um canal de comunicação inseguro.

Este artigo está organizado da seguinte forma: na Seção II serão apresentados os conceitos de gerenciamento de chaves dos tipos de criptografia; a Seção III apresentará brevemente os conceitos de imagens digitais; na Seção IV será mostrado um estudo de como foi realizada a aplicação do criptossistema RSA em documentos gráficos, a Seção V apresenta os resultados e por fim na Seção VI, as conclusões obtidas durante o desenvolvimento do artigo e propostas de trabalhos futuros.

II. GERENCIAMENTO DE CHAVES

Na criptografia tradicional, ou seja, criptografia simétrica, o remetente e o destinatário compartilham a mesma chave secreta. O remetente usa uma chave privada para criptografar a mensagem e o receptor usa a mesma chave para descriptografar a mensagem cifrada.

Na criptografia simétrica, é necessário realizar o compartilhamento, de forma secreta, da chave. Esse compartilhamento tem o objetivo de fazer com que as pessoas envolvidas na comunicação tenham o conhecimento da mesma chave. Esse compartilhamento deve ser feito de forma que nenhum intruso possa obter essa informação.

O problema desse compartilhamento reside na insegurança do canal de comunicação, ou seja, é confiar em um sistema de comunicação tal como o telefone, internet, ou algum outro meio de transmissão, formas de comunicação em que não se pode atestar a segurança do envio da informação, e onde é possível a existência de ataques maliciosos. Caso um intruso ouça ou intercepta a chave em algum momento da transição de informações entre o emissor e o remetente, o mesmo pode ler, modificar e criar mensagens criptografadas.

Outra forma de criptografia, denominada criptografia assimétrica ou criptografia de chave pública, envolve a criação de duas chaves, uma pública que pode ser divulgada e uma privada, que é utilizada para descriptografar, de conhecimento apenas do destinatário.

A diferença entre os dois tipos de criptografia (simétrica e assimétrica) é grande, pois a segurança da criptografia assimétrica é maior pela existência da chave pública, que pode ser livremente divulgada, e é utilizada apenas para criptografar e da chave privada, conhecida apenas pelo destinatário, utilizada para descriptografar a mensagem. Apesar da maior segurança conferida às criptografias de chave pública, requerem maior custo computacional, uma vez que usa duas chaves distintas para esta técnica, a complexidade se dá pela fatoração de números inteiros. Quanto à criptografia simétrica o custo computacional é menor, pois possui apenas uma chave, tanto para crifrar e decifrar, no entanto possui menor segurança.

III. IMAGEM DIGITAL

Uma imagem digital é composta por pequenos pontos, chamados pixels. Cada pixel é composto por três bandas de cor, uma com tom de vermelho, outra verde e azul (Red, Green e Blue – RGB). As três cores podem apresentar tonalidades diferentes, de acordo com a sua intensidade, e combinadas podem exibir em torno de 16 milhões de cores. [4]

Cada banda de um pixel possui um valor que varia de 0 a 255, correspondente a 8 bits de informação para cada cor. Uma imagem é composta por linhas e colunas, cujos pontos são coordenadas (x, y), os pixels.

Como dito anteriormente, cada pixel de uma imagem possui uma localização, dada por sua coordenada (x, y), e a intensidade de cada banda associada ao padrão RGB, que varia de 0 a 255. Neste trabalho, utilizou-se como abordagem a criptografia do valor da intensidade de cada banda em cada pixel.

IV. RSA

A técnica de criptografia RSA utiliza o problema da fatoração de dois números primos grandes, como base de sua segurança. O Quadro 1 apresenta o algoritmo de criptografia RSA, que envolve desde o processo de cálculo para a geração das chaves pública e privadas às fórmulas de criptografia e de descriptografia.

Algoritmo RSA:
1) Escolher dois números primos grandes p e q
2) Calcular $n = p * q$
3) Calcular $\phi = (p - 1) * (q - 1)$
4) Escolher um número inteiro aleatório e, que respeita a condição $1 < e < \phi$
5) Calcular um número d que satisfaça a seguinte equação $d * e \equiv 1 (mod\ \phi)$
6) A Chave pública será (e, n)
7) A Chave privada será (d, n)
8) Para cifrar uma mensagem $m \in Z_n : c = m^e\ mod\ n$
9) Para decifrar a mensagem cifrada: $m = c^d\ mod\ n$

Quadro 1 - Algoritmo RSA adaptado de [1]

O algoritmo RSA deve possuir chaves na ordem de 1776 bits para ser considerado seguro. Por esse motivo, os cálculos mostrados no Quadro 3.1, aparentemente simples, se tornam complexos e de alto custo quando utilizados números primos grandes, por exemplo, os números por volta de 1024 a 2048 bits.

Como ilustração, será apresentada, a seguir, a aplicação do RSA para criptografar o valor 65. Assim $m = 65$.

Utilizando, como exemplo, uma chave pública

$$(e, n) = (11, 221)$$

e a chave privada

$$(d, n) = (35{,}221)$$

a criptografia se dará da seguinte forma:

$$c = m^e \bmod n$$
$$c = 65^{11} \bmod 221$$
$$c = 78$$

Similarmente, a decifragem utilizando a chave privada apresentada anteriormente, será:

$$m = cd \bmod n$$
$$m = 78^{35} \bmod 221$$
$$m = 65$$

Pode-se observar que, apesar da mensagem e das chaves escolhidas serem pequenas, o cálculo é realizado sobre números grandes, devido às operações de exponenciação.

Ainda assim, para a técnica de criptografia do RSA ser considerada segura, as chaves devem ter tamanho de acordo com a Tabela I. [2]

Tabela I - Segurança das chaves X Tamanho, adaptado de [2]

Proteção	**Tamanho da chave em bits**
Curta proteção para dados de empresas de médio porte (2008-2011)	1248
(2009 até 2020)	1776
Médio prazo de proteção (2009 até 2030)	2432
Proteção para longo prazo (2009 até 2040)	3248

A. Aplicação do RSA em Imagens

Para a implementação da técnica de criptografia RSA foi utilizado à linguagem de programação Java, que possui métodos que facilitam a implementação do algoritmo. O pacote tem o nome java.security, no qual estão disponíveis algumas classes necessárias para utilização do método RSA, como criação das chaves, cifragem e decifragem, e algumas outras classes.

No primeiro teste foi gerado um arquivo txt como resposta da cifragem. O processo de criptografia é descrito a seguir.

Cada banda de um pixel cifrado era guardada no txt, de forma que se fosse utilizada uma chave de 1024 bits, cada número criptografado teria aproximadamente 1024 bits. Esse processo gerava um arquivo final muito maior que o arquivo original. Por exemplo, supondo uma imagen de 10 mil pixels, com 100x100 pixels, seria necessário armazenar 10 mil números cifrados de 1024 bits.

Esse fato, ainda acarretava em um segundo problema, o qual era a impossibilidade de gerar uma imagem criptografada, sem preda de informação.

Como exemplo, criptografou-se uma imagem contendo 10 mil pixels de tamanho, em Bytes igual a 5,83KB (o formato utilizado foi PNG). O resultado foi um arquivo de texto com tamanho de 9.074KB, um aumento significativo em relação ao seu tamanho anterior.

O tempo de processamento gasto para a cifragem dessa imagem foi de 7,8 segundos e 0,15 segundos gerando o arquivo de texto. Para decifragem da mesma foi gasto 585,78 segundos no processo de decifragem e 0,78 segundos lendo os números cifrados que estavam no arquivo de texto.

Observando os resultados obtidos com a geração do arquivo de texto, então foi adotada uma nova técnica de forma a permitir a geração da imagem criptografada .

O método adotado envolve a cifragem pixel a pixel da imagem. O algoritmo para gerar uma imagem cifrada é descrito a seguir.

O primeiro passo é transformar cada banda, de 255 bits, em sua representação binária. Em seguida são concatenadas as três bandas em binário, como nos exemplos a seguir:

Valor da intensidade de um pixel em inteiro: (255, 255, 255)

Binário: 111111111111111111111111

Valor da intensidade de um pixel em inteiro: (0,0,0)

Binário: 000000000000000000000000

O valor concatenado é transformado, novamente, para inteiro, conforme demostrado no exemplo a seguir. É possível observar que os números a serem cifrados variam de 0 a 16777215, ou seja, o tamanho máximo de uma mensagem a ser cifrada neste caso é um número de 24 bits.

Binário: 111111111111111111111111

Inteiro: 16777215

Binário: 000000000000000000000000

Inteiro: 0

Os números são, então, cifrados utilizando o algoritmo RSA com uma chave de 1024 bits. O número cifrado gerado será um número inteiro de tamanho máximo igual ao tamanho da chave. Portanto para armazenar 1024 bits em pixels de uma imagem deve ser feito o cálculo a seguir:

$$\frac{1024}{24} = 42{,}67 \cong 43$$

Ou seja, serão necessários 43 pixels para armazenar um pixel cifrado de uma imagem. Dessa forma, a imagem gerada é 43 vezes maior que a imagem original em relação à quantidade de pixels. Assim, cada número cifrado corresponde a 1032 bits $(43 * 24)$ de uma imagem.

Esses números cifrados de 1032 bits são separados em 129 blocos de números binários com 8 bits cada, pois o maior número representado por 8 bits é 255 que é o maior número que pode ser inserido em uma imagem do tipo RGB.

Desa forma, é possível gerar uma imagem cifrada, porém com 43 vezes a mais que seu tamanho em relação a pixels. A Figura 1 apresenta um exemplo de imagem a ser cifrada. Esta imagem tem resolução de 100 pixels de largura com mais 100 de comprimento, uma imagem com 10 mil pixels.

Fig. 1. Imagem Original 100 x 100

A Figura 2 é o resultado da cifragem, utilizando o método descrito. A imagem cifrada com resolução de 688 por 625, ou seja um total de 43 mil pixels, que como dito é 43 vezes maior que a imagem original de 10 mil pixels.

O tamanho da imagem original em bytes é de 30,8 KB (o formato utilizado é o JPG), já a imagem cifrada tem 1,26MB (o formato da imagem utilizado foi o PNG), nota-se que houve um aumento significativo na imagem.

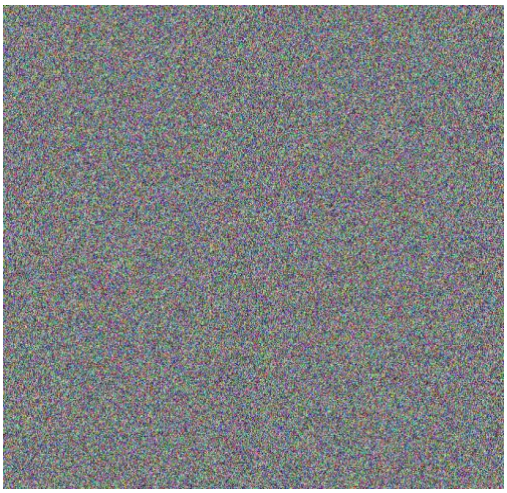

Figura 2: Imagem Cifrada 688 x 625

V. RESULTADOS

Este processo de criptografia por envolver muitos cálculos acaba se tornando um processo lento, pois são realizados vários cálculos com números muito grandes para que o processo funcione sem perda de informações. Além disso, o aumento do tamanho da imagem é um fator complicante.

Comparando a geração do arquivo de texto para a geração da imagem foi visto que gerar uma imagem era melhor que gerar o arquivo de texto.

A geração do arquivo de texto resultava em um arquivo maior do que a geração da imagem. uma imagem cifrada utilizando o método de gerar o arquivo de texto a cifragem tinha um resultado com 9MB de tamanho em disco, enquanto no método de gerar a imagem a mesma imagem cifrada tinha 1,26MB.

Além da questão de tamanho o tempo também foi diferente, isso ocorreu pela tática diferente de criptografia aplicada. No método do arquivo de texto, era cifrado cada banda de cada pixel da imagem, fazendo que para cada pixel ocorressem 3 cifragens e três gravações no arquivo de texto aumentando seu tempo de execução.

No método de gerar a imagem era cifrado pixel a pixel, fazendo com que fosse aproximadamente 3 vezes mais rápido que o método anterior.

Na Figura 3 é representado o gráfico comparativo de cifragem dos dois métodos, como dito o arquivo de texto utiliza mais tempo para terminar o processo do que o método que gera a imagem.

Já na Figura 4 é representado o gráfico comparativo de decifragem dos métodos.

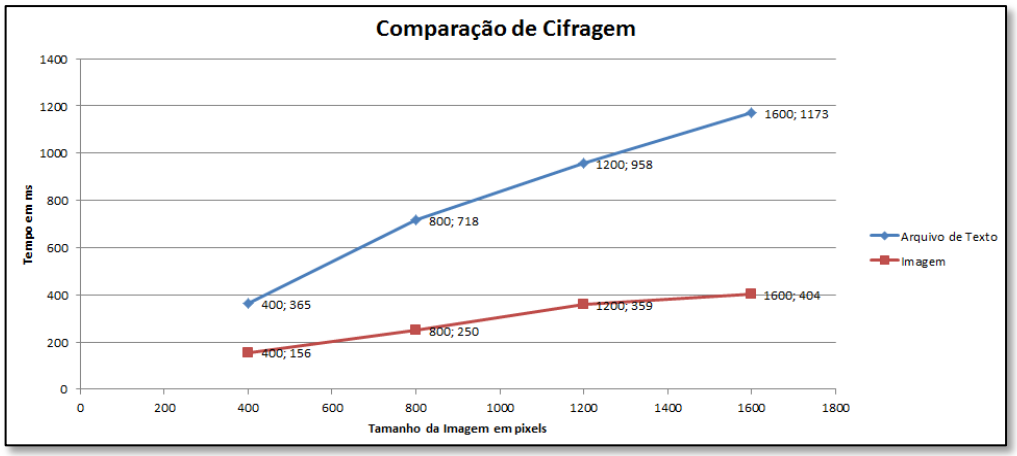

Fig. 3. Gráfico Comparação de Cifragem

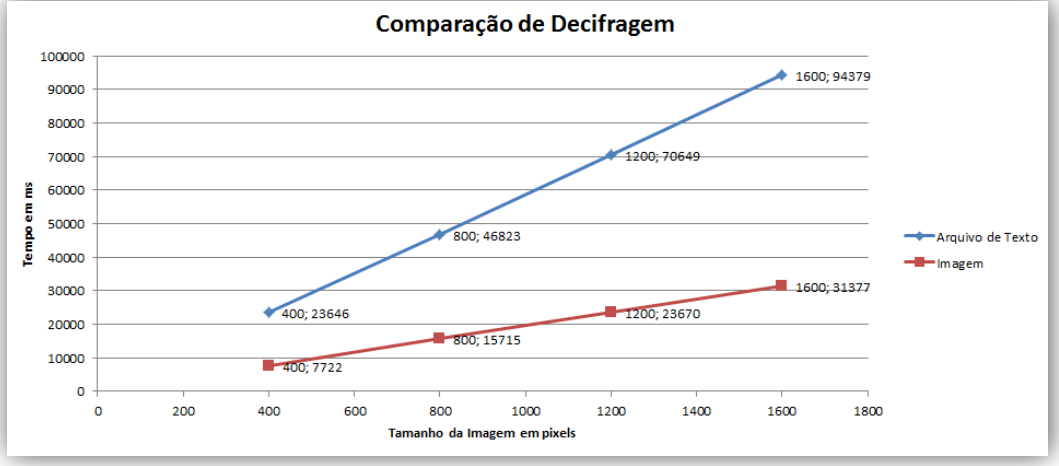

Fig. 4. Gráfico Comparação de Decifragem

Observando a Figura 4, também é possível verificar que o processo de decifragem utilizando o arquivo de texto foi mais lento que o de gerar a imagem.

VI. CONCLUSÃO

Neste artigo foi apresentada a técnica de criptografia RSA aplicada em imagens. Foram utilizadas duas abordagens diferentes de cifragem. A primeira consistia em gerar um arquivo de texto com os números cifrados, e a segunda consistia em gerar uma imagem cifrada.

Os dois métodos foram testados e comparados com o objetivo de corroborar a decisão do melhor método a ser utilizado. Foram realizados testes de tempos e tamanho que são os que mais afetam na eficiência da criptografia.

Conclui-se que o segundo método que, além de permitir retornar uma imagem como resposta, obteve maior eficiência, enquanto o método que gerava o arquivo de texto teve alguns problemas em relação ao tamanho, o tempo gasto também foi maior, pelo fato de que era cifrada a intensidade de cada banda no lugar de cada pixel.

Outro aspecto que também obteve vantagem na utilização da geração da imagem, é que o arquivo criptografado era igual ao arquivo original, ou seja, ambos são imagens, já no arquivo de texto o arquivo original era imagem e o resultado um arquivo de texto.

Mesmo conseguindo gerar a imagem, alguns problemas de tempo e tamanho, precisam ser resolvidos. O arquivo cifrado tem um aumento com relação ao original. Também é gasto muito tempo para que o processo seja realizado, esses são problemas a serem resolvidos ainda. Pretende-se investigar outras técnicas de criptografia de forma a resolver esses problemas.

AGRADECIMENTOS

Agradecimento ao CNPq pelo auxílio financeiro para a realização deste trabalho.

REFERÊNCIAS

[1] D. R. Stinson, Cryptography: theory and practice. CRC press, 2006.

[2] H. G. de Melo, “Consulta a base de dados cifrada em computação as nuvens,” Master’s thesis, Universidade Federal de Uberlândia, 2011.

[3] E.V.P. da Silva, “Introdução à criptografia RSA”, Universidade Estadual Paulista–UNESP. Escola de engenharia de Ilha Solteira, 2006.

[4] O.M. Filho, H.V. Neto, “Processamento Digital de Imagens”. Rio de Janeiro: Brasport, 1999. ISBN 8574520098.