SEGURANÇA DE DADOS COM ESTEGANOGRAFIA E CRIPTOGRAFIA

DATA SECURITY WITH STEGANOGRAPHY AND CRYPTOGRAPHY

Evandro Cesar Estevam[1]

RESUMO: A internet se tornou o principal meio de comunicação para troca de informações. Com isso a segurança da informação se tornou prioridade para setores que utilizam a rede para trafegar seus dados de forma rápida, principalmente quando se trata de dados confidenciais. A proteção digital é constantemente explorada com o objetivo de buscar novos meios de garantir a segurança necessária no tráfego de dados pela internet. Visando demonstrar mais uma forma de segurança da informação, este trabalho apresenta um estudo de métodos e conceitos de esteganografia e criptografia como formas eficazes de garantir a inviolabilidade da informação. Para mostrar a utilização dessas técnicas foi desenvolvido um estudo de caso para ocultar informações criptografadas dentro de uma imagem digital. Para tal, foi utilizada a técnica de esteganografia Last Significant Bit juntamente com a criptografia dos dados baseada na criptografia simétrica com o algoritmo DES (*Data Encryption Standard*).

Palavras-chave: Segurança de dados. Esteganografia. Criptografia.

ABSTRACT*: *The internet has become the main means of communication for information exchange. With this, information security has become a priority for sectors that use the network to traffic their data quickly, especially when it comes to confidential data. Digital protection is constantly being explored in order to find new ways of guaranteeing the necessary security in internet data traffic. In order to demonstrate another form of information security, this paper presents a study of methods and concepts of steganography and cryptography as forms effective to ensure the inviolability of information. To show the

[1] Especialista em Análise de Sistemas, PUCCAMP, 2001.

use of these techniques a case study was developed to hide encrypted information within a digital image. For that, the Last Significant Bit steganography technique was used along with data encryption based on symmetric cryptography with the Data Encryption Standard (DES) algorithm.

***Keywords*:** *Data security*. *Steganography*. *Cryptography*.

1 Introdução

A internet, segundo POPA (1998) é um dos maiores acontecimentos dos últimos anos, e com seu rápido crescimento, ela se tornou o principal meio de comunicação e de troca de informações, seja por um usuário ou uma empresa que objetiva melhorar a condução dos seus negócios. Como consequência a esse crescimento, surge o interesse e a necessidade cada vez maior de proteger as informações para evitar que transações sejam interceptadas por pessoas não autorizadas (PUTTINI; SOUZA, 2000).

Segundo (KOBUSZEWSKI, 2004), a criptografia de dados, que é uma ciência que estuda os princípios, meios e métodos para assegurar a privacidade das informações, por meio da modificação do texto original, está sendo largamente aplicada na comunicação de dados. A criptografia surgiu a partir da real necessidade de assegurar a privacidade dos dados e também a veracidade de seu destinatário.

Outra técnica que adquiriu um vasto conjunto de métodos para mascaramento de dados ao longo da história e que vem chamando a atenção é a esteganografia. Diferentemente da criptografia, as técnicas de esteganografia consistem, em ocultar a existência de informações em outra informação aparentemente inócua de forma que não seja possível detectar sua existência, sendo imperceptível aos olhos humanos (KOBUSZEWSKI, 2004).

O uso de criptografia e esteganografia são requisitos de segurança, porém a união destas duas técnicas resulta no aumento da segurança dos dados e vêm de encontro aos interesses de vários setores como comércio eletrônico, sigilo dos sistemas de computação, detecção de informação oculta, urnas eleitorais digitais, etc.

O objetivo deste trabalho é desenvolver uma ferramenta utilizando a técnica de esteganografia LSB (*Last Significant Bit*) em imagens, juntamente com o método de criptografia simétrica com o algoritmo DES (*Data Encryption Standard*). Na ferramenta será possível realizar a inserção de informações de textos criptografados que serão codificados

em uma imagem digital e a extração das informações que foram ocultadas dentro dessa imagem digital.

Busca-se com este trabalho oferecer mais uma forma de proteção aos dados, que pode ser aplicada em qualquer área que necessite enviar e receber mensagens com alto grau de confiabilidade.

Nas próximas seções serão abordados os seguintes assuntos: Seção 2 apresenta uma revisão de conceitos e a fundamentação teórica para o desenvolvimento do projeto, a Seção 3 descreve a metodologia utilizada, e os resultados são analisados e discutidos na Seção 4, finalizando o trabalho com a conclusão seguida das referências utilizadas.

2 Fundamentação Teórica

Nesta seção descreve-se brevemente os conceitos utilizados na elaboração deste trabalho.

a. Segurança

A segurança em sua forma mais simples, serve para garantir que outras pessoas não consigam ler ou modificar mensagens enviadas para outros destinatários, assim como impedir que pessoas não autorizadas possam acessar serviços remotos (TANENBAUM, 2011).

b. Criptografia

Criptografia é a arte de escrever informações, inicialmente legíveis, utilizando códigos que as tornam totalmente incompreensíveis e que somente podem ser decodificadas através da utilização das regras utilizadas para codificação, a essas regras se dá o nome de chaves (LUCCHESI, 1986 apud JASCONE, 2003).

A criptografia consiste na modificação do texto original, conhecida como textos simples, em textos cifrados de forma que não possa ser lido por pessoas não autorizadas. Quando um texto é criptografado, uma chave é gerada que será utilizada pelo destinatário para decodificar a informação. A princípio toda informação é pública, apenas a chave para acessá-la é privada (TANENBAUM, 2011).

A criptografia garante às pessoas autorizadas a segurança necessária das informações quanto a sua confiabilidade, autenticação, integridade e não repúdio para dados (MISAGHI, 2001 apud PETRI, 2004).

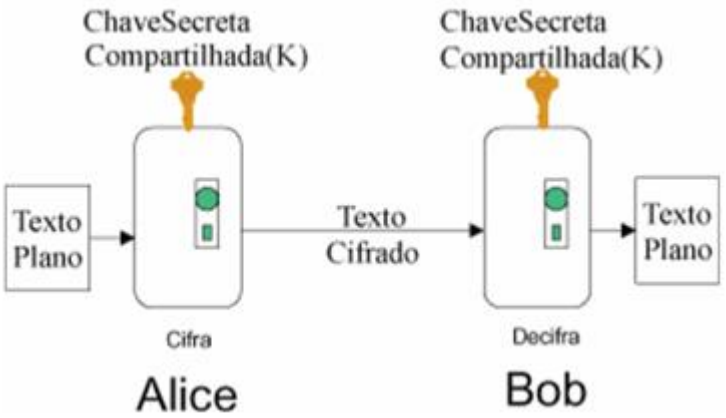
c. Criptografia Simétrica

Na criptografia simétrica a chave secreta é única, onde a mesma chave será utilizada para cifrar e decifrar as informações. Para criação da chave, deve haver um acordo entre o emissor e o receptor da informação, pois ela será utilizada em um mesmo algoritmo antes do início do envio e do recebimento das mensagens (PETRI, 2004).

O método de criptografia simétrica, também conhecida como criptografia convencional ou criptografia de chave secreta, é utilizado em aplicações limitadas que necessitam transmitir dados em ambientes não seguros e que precisam de autenticação das entidades. Para tal é necessário que o emissor e o destinatário tenham uma preparação antecipada para uso da chave (BRILHANTE, 2004).

A Figura 1 ilustra um modelo simplificado de criptografia convencional onde a mensagem original é cifrada com a chave compartilhada K e enviada por Alice através de um meio eletrônico. Como Bob possui a chave compartilhada K utilizada para cifrar a mensagem, poderá visualizar a mensagem recebida. Este método garante a confiabilidade da mensagem, desde que somente os interessados tenham conhecimento da chave K (MISAGHI, 2001, apud PETRI, 2004).

Figura 1. Modelo simplificado de criptografia



Fonte: (MISAGHI, 2001)

d. Algoritmo Criptográfico Simétrico DES (*Data Encription Standard*)

DES é um algoritmo simétrico, desenvolvido pela IBM na década de 70, com chave de 64 bits, dos quais 8 são de paridade. Desta forma, para cada chave, o algoritmo fornece uma permutação do texto original na ordem de 264 permutações possíveis aproximadamente 1,8 x 1019 letras (MORAES, 2004).

e. Esteganografia

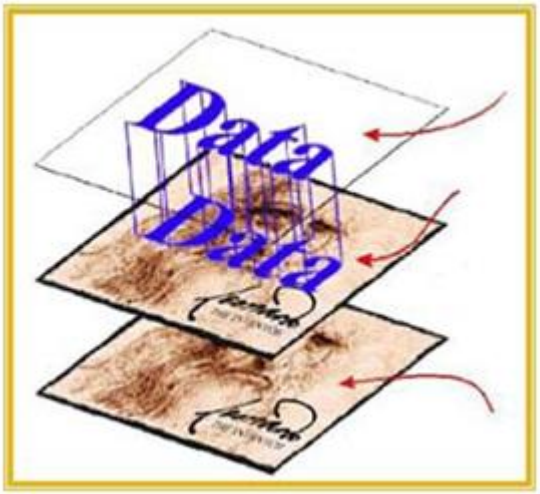
Esteganografia significa literalmente "escrita encoberta". É uma antiga art - ciência que consiste em ocultar uma mensagem secreta e codificada em objetos matemáticos, em outra informação aparentemente inócua de forma que não seja possível detectar a existência de uma mensagem escondida (JASCONE, 2003).

Segundo (PETITCOLAS ET AL., 1999), o conceito de esteganografia está dividido em três termos utilizados nesta área:

- Dado embutido (*embedded data*): mensagem que será enviada de maneira secreta para dentro de outra mensagem.
- Mensagem de cobertura (*cover-message*): identifica a mensagem que serve para mascarar o dado embutido, sendo que esta mensagem de cobertura pode ser de áudio (*cover-audio*), de texto (*cover-text*) ou imagem (*cover-image*). Após o término do processo de inserção da informação obtém-se o estego-objeto (*stego-object*)
- Estego-objeto (*stego-object*): identifica o objeto resultante após a inserção da informação na mensagem de cobertura.

A Figura 2 ilustra como a técnica de esteganografia em imagens pode ser interpretada. A informação escolhida pelo usuário é embutida dentro de uma imagem, gerando uma estego-imagem com as informações escondidas (JULIO ET AL., 2007).

Figura 2. Técnica de esteganografia em imagens



i) A mensagem de texto ou dado a ser embutido (*embedded data*)

ii) Os dados são embutidos na imagem a partir de uma chave (*cover-message*)

iii) A estego-imagem é criada contendo a informação escondida (*stego-object*)

Fonte: (JULIO, 2007)

f. Esteganografia em Imagens

Esta técnica de esteganografia consiste em embutir informações dentro de imagens digitais de forma que não irá comprometer a aparência das mesmas. Ela aproveita das fraquezas e limitações do HVS (sistema visual humano) que não é capaz de perceber as mudanças ocorridas devido a variações das cores em uma imagem esteganografada (ZANELLHA, 2002).

g. Imagem Digital

Imagem digital é uma matriz onde os índices das linhas e colunas identificam um ponto na imagem. Esses pontos são conhecidos como “pixels”, abreviação de “*picture elements*” (elementos da imagem, elementos da figura), que é a menor unidade de uma imagem digital. Em cada ponto é possível identificar alguma propriedade, como tom de cor, brilho e contraste. Quanto mais pixel uma imagem possuir, maior será sua resolução e qualidade. A Figura 3 ilustra a convenção dos eixos adotada para representação de uma imagem digital.

Figura 3. Conversão dos eixos

Fonte: Marques Filho e Vieira Neto (1999).

Para classificar a resolução de cor de uma imagem digital basta saber a quantidade de bits usados para representar um pixel. Esta classificação é chamada de profundidade da imagem, atualmente as resoluções de cores mais usadas são 1, 2, 4, 8, 16, 24, 32 bits. Por exemplo, uma imagem 800 x 600 com 256 cores (800 colunas por 600 linhas e com 8 bits de profundidade) possui 480.000 pixels, cada um representado por uma sequência de 8 bits (ZANELLA, 2002).

h. Inserção no Bit Menos Significativo (*Last Significant Bit*)

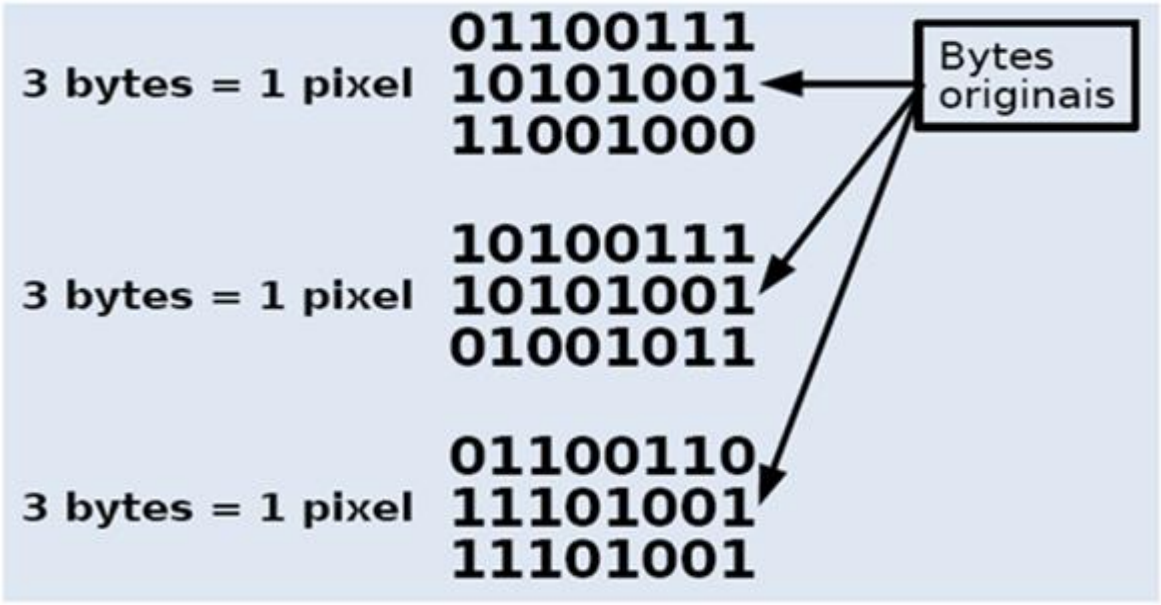
A técnica LSB é a mais comum na utilização de esteganografia em imagens. Nesta técnica a informação é inserida no bit menos significativo de cada byte formando o conjunto de bits que compõem o dado embutido (JASCONE, 2003).

É uma técnica considerada frágil porque por meio de um simples processo computacional de compressão de imagem, por exemplo de um formato bitmap (mapa de bits) para um formato JPEG (*Joint Photography Experts Group*), pode ocorrer perda de dados embutidos ou até mesmo a destruição inteira da informação, isto porque os algoritmos

que fazem a compressão geralmente descartam os bits menos significativos para diminuir o tamanho da imagem (ROCHA, 2003).

Para ilustrar o método, vamos supor que desejamos embutir a letra “a” dentro de uma imagem que possui os valores em pixel, conforme ilustra a Figura 4.

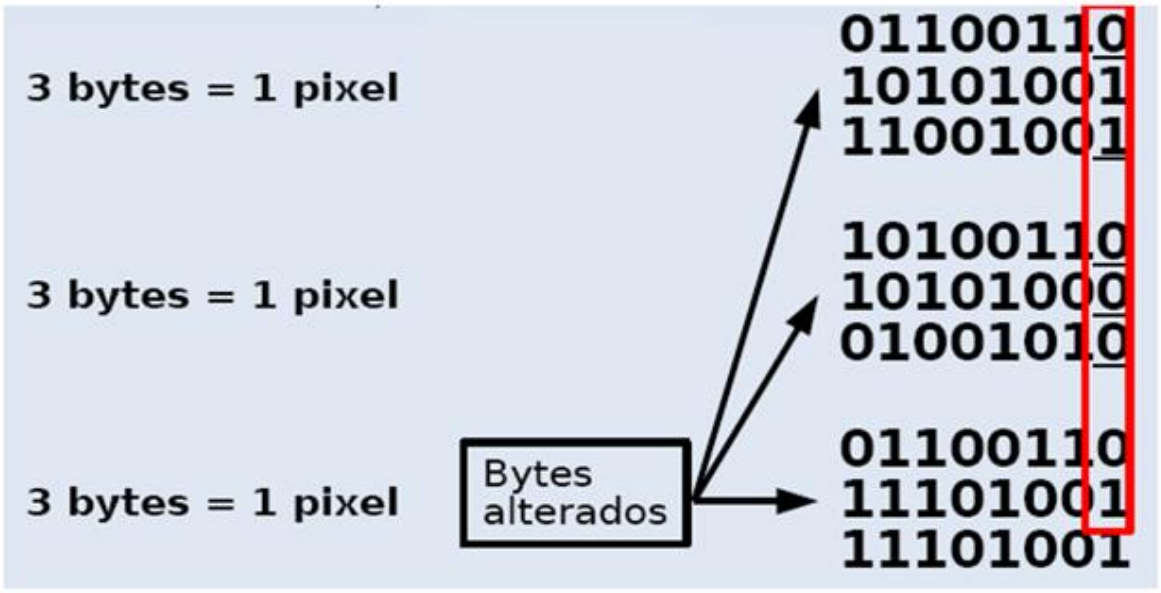
Figura 4. Pixel de uma imagem original



Fonte: Produzida pelo autor.

Para embutir na imagem é necessário saber qual o valor binário respectivo a letra “a” que é o código 97 da tabela ASCII (*American Standard Code for Information Interchange*), portanto o valor binário respectivo é 1 1 0 0 0 0 1. Colocando esse valor binário, bit a bit dentro da imagem utilizando a técnica LSB, vamos ter um conjunto de pixel da imagem resultante alterada conforme ilustra a Figura 5.

Figura 5. Pixel de uma imagem resultante após a inserção de uma dado



Fonte: Produzida pelo autor.

Os bits destacados foram os que sofreram as alterações causando uma mudança na imagem totalmente imperceptível ao olho humano.

Para identificarmos a quantidade de informações que podemos embutir em uma imagem, vamos tomar como exemplo uma imagem com tamanho 800 x 600 pixels que no total possui 480.000 pixels. Se utilizarmos uma imagem com profundidade de 32 bits, onde cada pixel possui um conjunto de 4 bytes, podemos esconder 240.000 bytes de informação.

i. Linguagem Java

Linguagem de programação baseada em C e C++ completamente orientada a objetos desenvolvida por James Grosling juntamente com sua equipe da Sun Microsystems e hoje mantida pela Oracle.

Java é uma linguagem interpretada, então para que um programa seja executado é necessário a utilização de um carregador de classes que transfere o programa para a memória. Este carregador possui o nome de *Java Virtual Machine*, ou JVM – a máquina virtual Java tem como principal função interpretar o bytecodes gerados na compilação dos programas java e codificá-los de forma que a CPU possa entende-los e executá-los (DEITEL, 2010).

A Figura 6 ilustra o funcionamento do ambiente Java

Figura 6. Funcionamento do ambiente Java

Fonte: Produzida pelo autor.

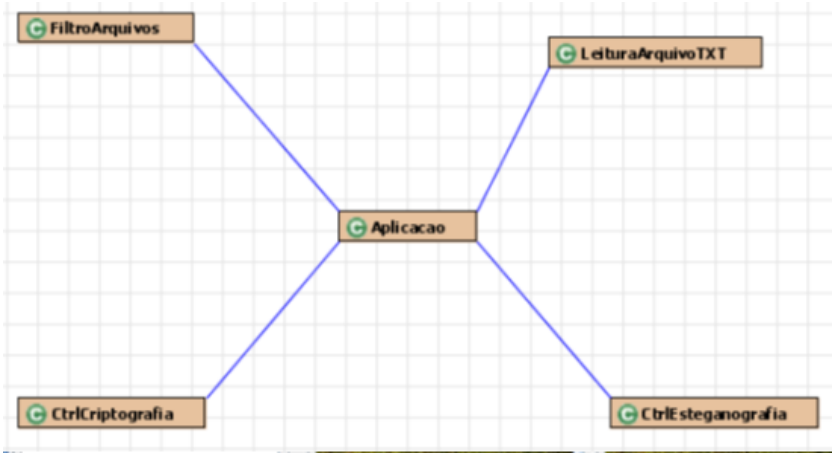
3 Metodologia

Para a exposição da metodologia utilizada no desenvolvimento deste trabalho, o processo foi dividido em duas etapas que serão melhor detalhadas nas próximas subseções: modelagem do diagrama de classes utilizando a notação UML (Unified Modeling Language) e Elaboração da aplicação que demonstra a utilização de esteganografia, utilizando o método de inserção da informação no bit menos significativo, em conjunto com a criptografia com algoritmo DES.

a. Diagrama de Classe

Para o desenvolvimento da aplicação foram criadas cinco classes. Para visualizar seus relacionamentos foi desenvolvido um diagrama de classe do estudo proposto, conforme ilustra a Figura 7.

Figura 7. Diagrama de classe da aplicação



Fonte: Produzida pelo autor.

As classes de controle desenvolvidas no estudo de caso são:

- Aplicação: classe responsável pela interação com o usuário;
- FiltroArquivos: classe que restringe a utilização de arquivos texto e imagens bitmap;
- LeituraArquivoTXT: classe que lê um arquivo texto para apresentar ao usuário o que vai ser ocultado e o que foi extraído da imagem;
- CtrlCriptografia: classe que possui os métodos para cifrar e decifrar as informações embutidas e extraídas na imagem; e
- CtrlEsteganografia: classe que possui os métodos para embutir e extrair as informações na imagem e criação dos arquivos gerados a partir da codificação e decodificação.

b. Elaboração da Aplicação

A ferramenta desenvolvida se baseia em 2 etapas que são:

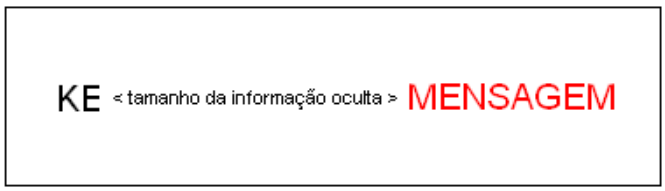
- Realização da criptografia de um determinado texto e na esteganografia do texto criptografado em uma imagem digital selecionada; e
- Realização da extração da informação de uma imagem digital assim como a descriptografia do texto extraído.

Para a realização da primeira etapa, inicialmente as informações do arquivo texto selecionado são carregadas e expostas em tela para validação. Após a exposição das informações, é gerado uma chave secreta que será utilizada para cifrar e decifrar as informações. A criptografia dos dados é realizada em seguida juntamente com a codificação dos dados criptografados para o método de conversão *base64*.

Ainda na primeira etapa, finalizado a fase de criptografia do texto, inicia-se a fase da esteganografia onde será realizado tratamento da imagem para seu processamento pixel a pixel. A inserção do texto criptografado na imagem será feita caractere por caractere. Como cada caractere ocupa dois bytes, serão necessários seis pixels por caractere. Nos primeiros pixels da imagem esteganografada serão gravadas marcas, representadas pela letra (“K”) e a

letra (“E”), que indicam a existência de informações ocultas na imagem e também será gravado o tamanho da informação contida na imagem conforme ilustra a Figura 8. Após o término da alteração dos primeiros pixels para inserção das marcas iniciais, serão alterados os demais pixels para inserção dos dados de acordo com a quantidade de caracteres contidos na mensagem.

Figura 8. Estrutura que identifica a existência de informação oculta na imagem



Fonte: Produzida pelo autor.

Para a realização da segunda etapa, inicialmente a imagem que contém a informação oculta e que foi selecionada será exposta em tela para validação. Após a exposição da imagem, será verificada a existência das marcas utilizadas no processo de esteganografia das informações para validar o processo de extração. Caso a imagem esteja de acordo com as regras definidas, será extraída a quantidade de informação que está embutida na imagem.

Ainda na segunda etapa, finalizado o processo de extração dos dados ocultos na imagem, inicia-se a fase de descriptografia dos dados, que inicialmente será verificada a validade da chave secreta gerada na encriptação. Após a validação da chave, os dados serão decodificados da *base64* e convertido em texto decifrado.

4 Análise e Discussão dos Resultados

Para demonstrar a técnica LSB, serão mostrados os resultados obtidos na inserção da palavra “KELVIN” em uma imagem.

Primeiramente os dados serão formatados com as marcações necessárias para identificar a existência da informação na imagem e possibilitar sua decodificação. Desta forma a informação a ser embutida ficará representada sob a seguinte formatação KE6KELVIN sendo que seu respectivo código binário é “01001011 01000101 00000110 01001011 01000101 01001100 01010110 01001001 01001110”. Essa sequência binária que será inserida nos bits menos significativos de cada pixel.

A Figura 9 ilustra a modificação nos bits com a inserção das marcas “KE”, do tamanho da informação “6” e da mensagem KELVIN.

Figura 9. Inserção do dado KE6KELVIN utilizando a técnica *Last Significant Bit*

Pixel	Caratere	Código binário	Binário no formato original	Binário no formato estegano
1	K	00000000 01001011	11111111 11111110 11111110 11111110	11111111 11111110 11111110 11111110
2			11111111 11111110 11111110 11111110	11111111 11111110 11111110 11111110
3			11111111 11111110 11111110 11111110	11111111 11111110 11111110 11111110
4			11111111 11111111 11111110 11111111	11111111 11111111 11111110 11111110
5			11111111 11111110 11111110 11111111	11111111 11111111 11111110 11111111
6			11111111 11111111 11111110 11111110	11111111 11111111 11111110 11111110
7	E	00000000 01000101	11111111 11111110 11111110 11111110	11111111 11111110 11111110 11111110
8			11111111 11111110 11111110 11111110	11111111 11111110 11111110 11111110
9			11111111 11111110 11111110 11111110	11111111 11111110 11111110 11111110
10			11111111 11111111 11111110 11111111	11111111 11111111 11111110 11111110
11			11111111 11111110 11111111 11111110	11111111 11111110 11111111 11111110
12			11111111 11111110 11111110 11111110	11111111 11111111 11111110 11111110
13	6	00000000 00000110	11111111 11111110 11111110 11111111	11111111 11111110 11111110 11111110
14			11111111 11111110 11111110 11111110	11111111 11111110 11111110 11111110
15			11111111 11111110 11111111 11111111	11111111 11111110 11111110 11111110
16			11111111 11111111 11111111 11111111	11111111 11111110 11111110 11111110
17			11111111 11111110 11111111 11111110	11111111 11111110 11111111 11111111
18			11111111 11111111 11111110 11111110	11111111 11111110 11111110 11111110
19	K	00000000 01001011	11111111 11111110 11111110 11111110	11111111 11111110 11111110 11111110
20			11111111 11111110 11111110 11111110	11111111 11111110 11111110 11111110
21			11111111 11111110 11111110 11111110	11111111 11111110 11111110 11111110
22			11111111 11111110 11111110 11111110	11111111 11111111 11111110 11111110
23			11111111 11111111 11111110 11111111	11111111 11111111 11111110 11111111
24			11111111 11111101 11111100 11111100	11111111 11111101 11111100 11111100
25	E	00000000 01000101	11111111 11111100 11111100 11111100	11111111 11111100 11111100 11111100
26			11111111 11111100 11111100 11111100	11111111 11111100 11111100 11111100
27			11111111 11111110 11111110 11111110	11111111 11111110 11111110 11111110
28			11111111 11111111 11111111 11111110	11111111 11111111 11111110 11111110
29			11111111 11111110 11111110 11111111	11111111 11111110 11111111 11111110
30			11111111 11111111 11111110 11111110	11111111 11111111 11111110 11111110
31	L	00000000 01001100	11111111 11111110 11111110 11111110	11111111 11111110 11111110 11111110
32			11111111 11111110 11111110 11111110	11111111 11111110 11111110 11111110
33			11111111 11111110 11111110 11111110	11111111 11111110 11111110 11111110
34			11111111 11111110 11111111 11111111	11111111 11111111 11111110 11111110
35			11111111 11111111 11111110 11111111	11111111 11111111 11111111 11111110
36			11111111 11111110 11111110 11111110	11111111 11111110 11111110 11111110
37	V	00000000 01010110	11111111 11111110 11111110 11111110	11111111 11111110 11111110 11111110
38			11111111 11111110 11111110 11111110	11111111 11111110 11111110 11111110
39			11111111 11111110 11111110 11111110	11111111 11111110 11111110 11111110
40			11111111 11111111 11111110 11111111	11111111 11111111 11111110 11111111
41			11111111 11111111 11111111 11111110	11111111 11111110 11111111 11111111
42			11111111 11111110 11111110 11111110	11111111 11111110 11111110 11111110

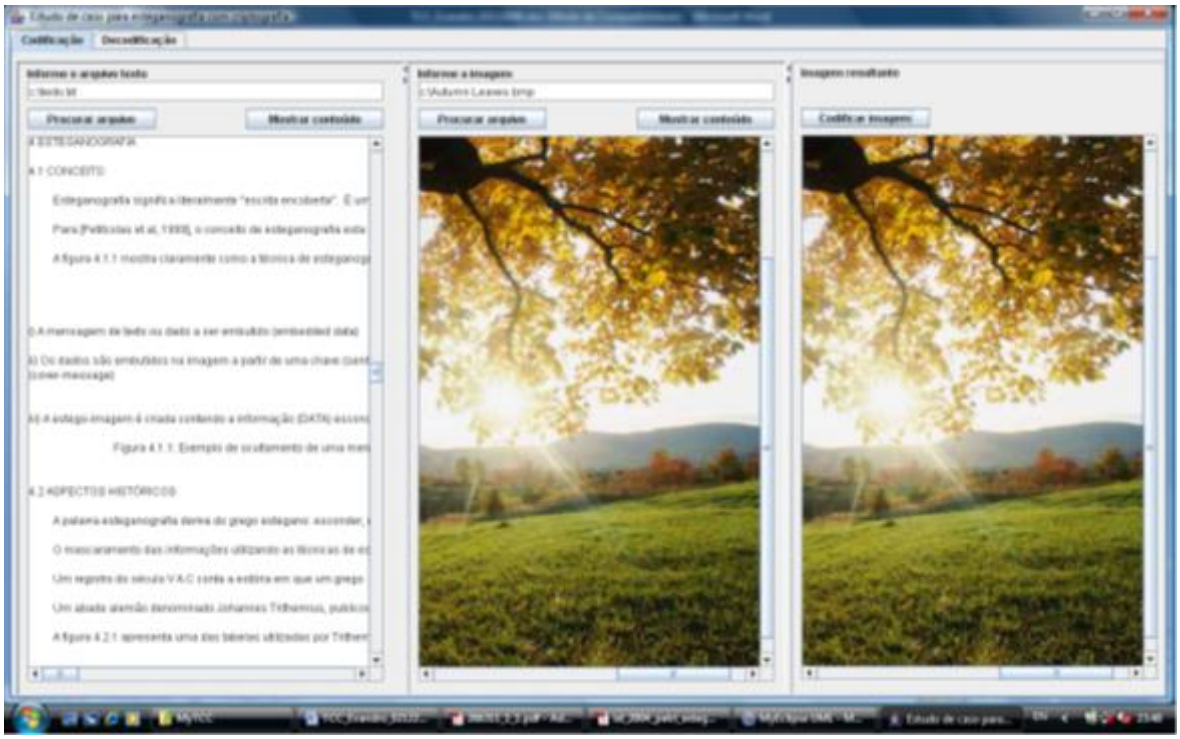
43	I	00000000 01001001	11111111 11111110 11111110 11111110	11111111 11111110 11111110 11111110
44			11111111 11111110 11111110 11111110	11111111 11111110 11111110 11111110
45			11111111 11111110 11111110 11111110	11111111 11111110 11111110 11111110
46			11111111 11111111 11111111 11111111	11111111 11111111 11111110 11111110
47			11111111 11111110 11111111 11111110	11111111 11111111 11111110 11111110
48			11111111 11111110 11111110 11111110	11111111 11111111 11111110 11111110

49	N	00000000 01001110	11111111 11111100 11111100 11111100	11111111 11111100 11111100 11111100
50			11111111 11111100 11111100 11111100	11111111 11111100 11111100 11111100
51			11111111 11111110 11111110 11111110	11111111 11111110 11111110 11111110
52			11111111 11111111 11111111 11111111	11111111 11111111 11111110 11111110
53			11111111 11111111 11111110 11111110	11111111 11111111 11111111 11111111
54			11111111 11111110 11111110 11111110	11111111 11111110 11111110 11111110

Fonte: Produzida pelo autor.

Para a validação do resultado da aplicação na primeira etapa, foi selecionado um texto que possui 239 linhas, que foi criptografado e ocultado dentro de uma imagem sem qualquer alteração em seus *pixels*. Após a geração da imagem resultante, que poderá ser gravada em qualquer dispositivo de armazenamento de dados, pode-se notar a impossibilidade de identificar, aos olhos humanos, a presença de qualquer vício que comprometa a qualidade da imagem, conforme ilustra a Figura 10.

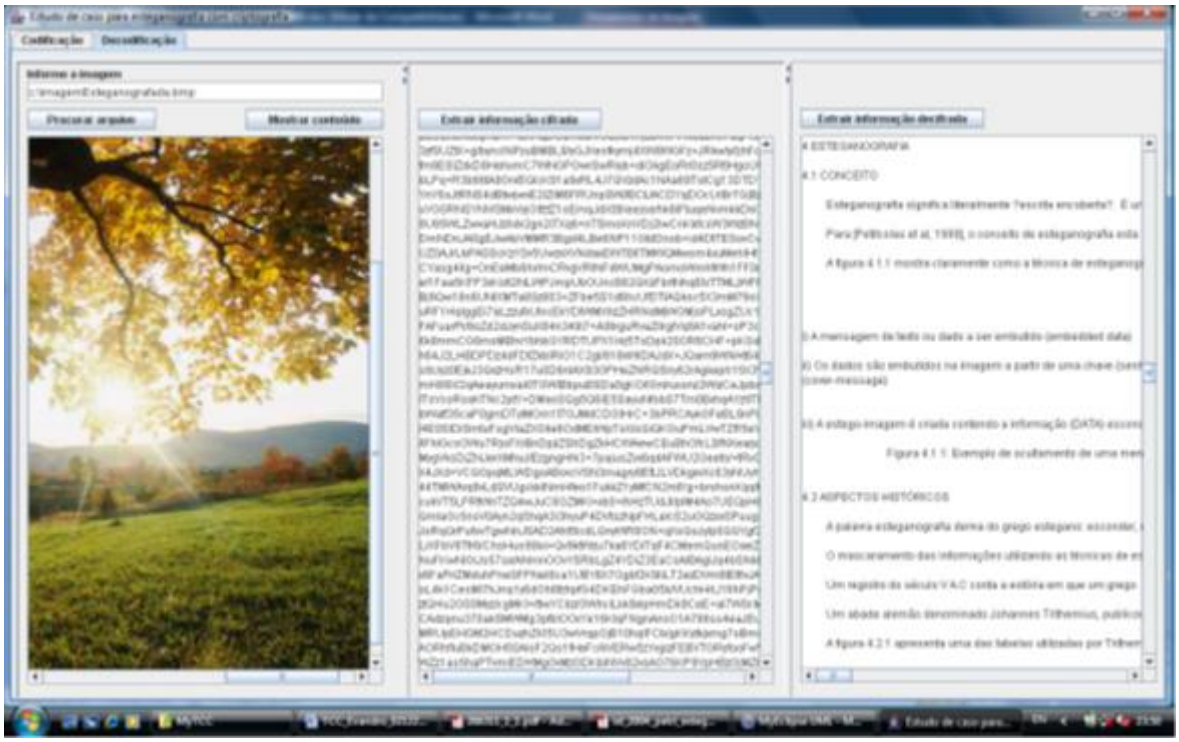
Figura 10. Recursos para encriptação dos dados e geração da imagem resultante



Fonte: Produzida pelo autor.

Para a validação do resultado da aplicação na segunda etapa, foi selecionada a imagem, na qual as informações foram inseridas. Foi realizado um processamento nesta imagem para identificar a existência de informações ocultas e após esta validação foi feito a extração de todas as informações, que a princípio estão criptografadas. Após o término da extração foi realizado o processo de descriptografia dos dados, que foi possível devido ao conhecimento da chave secreta. Finalizado todo o processo, pode-se notar que toda a informação resultante está completamente legível, conforme ilustra a Figura 11.

Figura11. Recursos para extração de dados da imagem e decriptação dos dados extraídos



Fonte: Produzida pelo autor.

5 Conclusão

Dentro de uma organização, existem muitos meios de trafegar dados utilizando recursos tecnológicos, e garantir a segurança da informação é uma grande preocupação, pois um vazamento de informação pode colocar tudo a perder dentro de um projeto estratégico. Com isto o desenvolvimento deste trabalho vem de encontro a necessidade que as organizações possuem de garantir a segurança de suas informações durante a transações realizadas. Portanto este trabalho resultou em uma aplicação que faz a proteção dos dados

para evitar que pessoas não autorizadas possam acessá-los, garantindo sua confidencialidade. Para melhorar a segurança dos dados, a aplicação combina técnicas de criptografia e esteganografia, dificultando o acesso a informações sigilosas por pessoas estranhas. Outro ponto positivo da aplicação é a não existência de custos diretos, uma vez que só foram utilizadas soluções de softwares gratuitas e de livre distribuição.

Como trabalho futuro nesta área pode-se propor a possibilidade de utilização de algoritmos assimétricos na encriptação e decriptação das informações assim como a utilização de outras mídias para utilização das técnicas de esteganografia, como áudio e vídeo.

Referências

DEITEL, H. M. **Java Como Programar.** 8 ed.. Porto Alegre: Bookman, 2010.

TANENBAUM, Andrew S. **Redes de Computadores.** 5 ed.. Rio de Janeiro: Campus, 2011.

MISAGHI, Mehran. Avaliação de Modificações do Cifrador Caótico de Roskin. Florianópolis, 2001. Dissertação (Mestrado em Ciência da Computação) – Centro Tecnológico, Universidade Federal de Santa Catarina.

PUTTINI, Ricardo S.; SOUSA, Rafael T. de. Criptografia e segurança de redes de computadores, Brasília, dez. 2000.

Disponível em: http://www.redes.unb.br/security/criptografia/rsa/rsa.html

POPA, R. An analysis of steganography techniques. Master's thesis, Department of Computer Science and Software Engineering of The "Polytechnic" University of Timisoara, Timisoara, Romênia, 1998.

JASCONE, Fábio Luis Tavares. Protótipo de Software para Ocultar Texto Criptografado em Imagens Digitais. Blumenau, 2003.

Disponível em: http://www.inf.furb.br/~pericas/orientacoes/Esteganografia2003.pdf

PETRI, Marcelo. Esteganografia, Joinville, dez. 2004.

Disponível em: http://www.mlaureano.org/aulas_material/orientacoes2/ist_2004_petri_esteganografia.pdf

[PETITCOLAS ET AL., 1999] Petitcolas, F. A., Anderson, R. J., and Kuhn, M. G. (1999).

Information hiding - a survey. In Proceedings of IEEE. Special issue on Protection on multimedia content.

Disponível em: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.21.4574

ZANELLA, Daniel. Protótipo de software para inserção e extração de mensagens em arquivo raster através de esteganogtrafia. Blumenau, nov 2002.

Disponível em: http://dsc.inf.furb.br/arquivos/tccs/monografias/2002-2danielzanellavf.pdf

JULIO, Eduardo Pagani, Brazil, Wagner Gaspar e Albuquerque, Célio Vinicius Neves (2007), "Esteganografia e Suas Aplicações",

Disponível em: http://sbseg2007.nce.ufrj.br/Minicurso-PDF.htm

MARQUES FILHO, M.; VIEIRA NETO, H. Processamento digital de imagens. Rio de

Janeiro: Brasport, 406p, ISBN 8574520098, 1999.

ROCHA, Anderson Rezende. Randomização Progressiva para Esteganálise , Campinas, fev. 2006.

Disponível em: <http://www.ic.unicamp.br/~rocha/msc/project/dissertacaoMestrado-AndersonRocha.pdf>

KOBUSZEWSKI, André. Protótipo de Software para Ocultar Textos Compactados em Arquivos de Áudio Utilizando Esteganografia. Blumenau, fev. 2004

Disponível em: http://www.inf.furb.br/~pericas/orientacoes/Esteganografia2004.pdf