Universidade de São Paulo

Instituto de Matemática e Estatística

Departamento de Ciência da Computação

Métodos de Esteganografia Aplicados a Imagens Médicas

Rafael de Assunção Sampaio

rsampaio@ime.usp.br

Orientador: Prof. Dr. Marcel P. Jackowski

mjack@ime.usp.br

Agradecimentos

Quero guardar neste trabalho sentimentos que tenho por esta Universidade. A Universidade de São Paulo não é somente um centro acadêmico de excelência reconhecido internacionalmente. A USP é uma cidade que reúne várias unidades, cada qual especialista e peculiar. Além destas, ela abriga o TUSP, Cinusp, Rádio USP, TV USP, Coral da USP, Jornal do Campus, Orquestra Sinfônica da USP (OSUSP). Que dizer, então, das maiores bibliotecas da América Latina? A Praça do Relógio, rodeada de espécies de Mata Atlântica. Os doze painéis, inspirados de Benedetto Croce, figuram o mundo da fantasia e o mundo da realidade. "Scientia vinces" – Vencerás pela Ciência – lê-se no brasão.

No Instituto de Matemática e Estatística, cresci intelectualmente. Mas também cresci como pessoa. Tenho a feliz oportunidade de ter cursado dois bacharelados: Matemática Pura e Ciência da Computação. De ter participado de diversas palestras, cursos, eventos e seminários. Aliás, de poder participar também de aulas que não faziam parte do meu currículo, com a facilidade de abrir a porta, sentar e aprender. As aulas, em geral, não são fáceis. Talvez a maior lição que aprendi é que leva tempo aprender a essência e incorporar alguns conceitos. Mas é imensurável a satisfação diária de ampliar o conhecimento e dividi-lo com outras pessoas.

Tive a rara oportunidade de ter aulas com excelentes Professores. Certamente, não todos. Mas aqueles que preparavam as aulas, que se importavam com as suas dúvidas, que se tornavam disponíveis fora do horário de aula... Esses realmente são Professores, e entendem a responsabilidade que têm para a formação de futuros pesquisadores. Obrigado a cada um de vocês.

Reservo um espaço para registrar o meu carinho por uma parte especial do IME – a Matema**teca**. Com o nobre objetivo de cativar as pessoas para a Matemática, apresentando a beleza desta ciência, a Matema**teca** reúne professores batalhadores, por quem eu tenho profunda admiração. Serei sempre grato pela oportunidade que tenho de colaborar com esse grupo e pela amizade que construímos.

Quero agradecer, sobretudo, aos meus verdadeiros amigos, que estiveram, da melhor maneira possível, próximos, acompanhando esta jornada. Em especial, agradeço à minha família, que me ensinou a importância de lutar e perseverar.

Finalmente, agradeço ao Professor Marcel Jackowski pela disponibilidade e atenção à minha orientação. Devo destacar a minha gratidão por ter podido escolher o tema desta monografia e trabalhar com grande liberdade. Obrigado pelos livros, as idéias, as sugestões, o tempo e a paciência!

Rafael Sampaio

Resumo

Todos os dias, pessoas comparecem a laboratórios, clínicas e hospitais para que sejam realizados exames médicos. Tais exames são essenciais para avaliação de tumores (câncer), condição óssea, estado de gestação etc. Os resultados desses exames, além do aspecto clínico, guardam informações confidenciais do paciente (nome, endereço, diagnóstico etc.), do local onde o exame foi realizado, dos aparelhos e responsáveis, entre outras. As imagens originadas desses exames podem inadvertidamente ser compartilhadas, expondo tais informações, sem que se possa verificar a autenticidade e o uso indevido. Isso é possível pois o padrão DICOM (*Digital Imaging and Communications In Medicine*) não dispõe de métodos de segurança, armazenando os dados em *tags* irrestritamente editáveis.

A Esteganografia é formada por um conjunto de técnicas que permitem escrever mensagens e ocultá-las, por exemplo, em imagens, de tal sorte que ninguém desconfie de sua existência. É diferente de Criptografia, que codifica uma mensagem para que apenas o emissor e o destinatário consigam ler o texto claro. Nesse sentido, a Criptografia ocupa-se da segurança da mensagem, enquanto a Esteganografia ocupa-se da segurança da mensagem e do canal de comunicação.

Este trabalho visa a estudar métodos de esteganografia aplicados a imagens médicas, que permitam agregar segurança e confidencialidade às informações contidas nas imagens médicas, minimizando perdas intrínsecas à manipulação dessas imagens, cujo uso em diagnósticos poderia ficar comprometido.

Sumário

Parte I

Objetiva

1 Introdução

O começo de todas as ciências é o espanto de as coisas serem o que são.

– Aristóteles (filósofo, 384 a.C. - 322 a.C.)

A palavra *esteganografia* tem origem nas palavras gregas *steganos*, que significa "encoberto", e *graphia*, que significa "escrita". A esteganografia é, assim, uma ciência que se ocupa de realizar comunicações *invisíveis*, isto é, a existência de mensagens secretas não deve ser detectada. O termo *esteganografia* foi utilizado pela primeira vez por Johannes Trithemius (1462-1516) na trilogia *Polygraphia* e em *Steganographia*.

A evidência mais remota de esteganografia, de acordo com [6], é atribuída a Heródoto, um géografo e historiador grego do século V a.C. Heródoto narra sobre um escravo que teria sido enviado por Histiaeus a Mileto com uma mensagem secreta tatuada na cabeça. O cabelo do escravo teria sido raspado e a tatuagem realizada; o escravo teria de esperar o cabelo crescer novamente para manter o segredo. O escravo viaja a Mileto e raspa a cabeça para revelar a mensagem ao governador Aristagoras. A mensagem encorajaria Aristagoras a iniciar a guerra contra o rei da Pérsia.

Outro episódio peculiar é o embate enxadrístico entre Viktor Korchnoi e Anatoly Karpov pelo Campeonato Mundial de Xadrez em 1978. Segundo [6], durante uma das partidas, um dos assistentes de Karpov traz um iugorte. A delegação de Korchnoi imediatamente protestou, alegando que, dependendo da cor do iogurte, isso poderia significar oferecer ou rejeitar um empate. Karpov passaria a poder consumir apenas um iugorte – sempre da mesma cor – num mesmo momento das partidas.

No *The New York Times* de 11 de novembro de 2006, lê-se que Dhiren Barot, membro da Al Qaeda, realizou uma filmagem entre a *Broadway* e *South Street*, ocultando esse material numa cópia de *Die Hard: With a Vengeance*, com Bruce Willis. Esse vídeo teria sido utilizado nos ataques de 11 de setembro de 2001.

Do exposto, observa-se que a esteganografia pode ser aplicada em dife-

rentes formas de informação, com o objetivo de ocultar alguma mensagem. Neste trabalho, o foco será a utilização de imagens e nelas ocorrerá o armazenamento de dados sigilosos.

As imagens médicas foram as escolhidas, por oferecerem duas restrições importantes: i) carregar informações sigilosas relacionadas ao paciente, diagnóstico etc. num formato inseguro; e ii) qualquer modificação feita na imagem, visando a ocultar informação, deve manter alta a taxa de originalidade, para que a imagem continue a ter utilidade clínica.

A principal motivação deste trabalho é fornecer subsídios para que as imagens médicas ofereçam confidencialidade, bem como possam ser autenticadas quanto à veracidade de seus metadados. Assim, o objetivo central é propor uma extensão do protocolo DICOM utilizando-se métodos de esteganografia.

2 Imagens Médicas e DICOM

Não devemos ter medo de inventar seja o que for. Tudo o que existe em nós existe também na natureza, pois fazemos parte dela.

– Pablo Picasso (pintor, 1881-1973)

A medicina moderna tem avançado muito nos últimos anos. Em grande parte, o mérito desse avanço deve ser compartilhado com outras ciências, que lhe provêm subsídios. Aqui, destaca-se a importância das imagens médicas no auxílio do diagnóstico, da compreensão e da evolução de diversas patologias.

Em 1895, Wilhelm Conrad Röntgen descreveu o comportamento de um tipo de radiação eletromagnética, os raios X. Esse foi apenas o início do surgimento de diversas tecnologias que se seguiram: tomografia computadorizada (1960), ultrassom (1970), ressonância magnética (1980).[24]

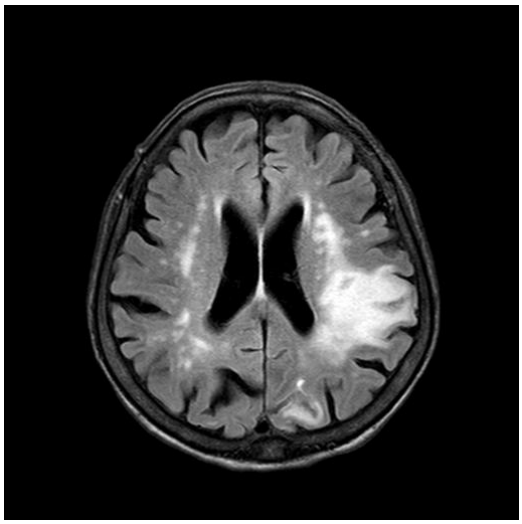

Figura 1: Ressonância magnética de um encéfalo – região esbranquiçada indica anomalia

Com a tomografia computadorizada e as outras tecnologias, associadas ao crescente uso dos computadores em aplicações clínicas, o *American College of Radiology* (ACR) e a *National Electrical Manufacturers Association* (NEMA) reconheceram a necessidade de se estabelecer um padrão para a

transferência das imagens e da informação relacionada entre os vários dispositivos. Assim, em 1983, o ACR e a NEMA decidiram desenvolver um padrão que viabilizasse a transmissão das imagens médicas, facilitasse a evolução dos sistemas de armazenamento das imagens para a integração destes com as demais informações hospitalares, e tornasse possível a criação de um banco de dados que cresceria além das fronteiras geográficas.

Em 1985, ACR-NEMA publicam a versão 1.0 daquele que viria a ser conhecido como padrão DICOM – *Digital Imaging and Communications in Medicine*. Hoje, o DICOM é um padrão bem estabelecido de armazenamento, impressão e transmissão da informação presente nas imagens médicas. [2]

Os arquivos .DCM, estruturados para o formato DICOM, possuem duas componentes: cabeçalho (*header*), em que se encontram diversas informações confidenciais do paciente, do local onde o exame foi realizado, dos aparelhos e responsáveis, entre outras; matriz, em tons de cinza, que representa a imagem obtida pelo aparelho. O cabeçalho é composto por um conjunto de *tags* que, atualmente, já somam mais de 3300 distintas. A listagem pode ser encontrada nas referências [1, 8].

0008-0070	Manufacturer	LO	Philips Medical Systems
0008-0080	InstitutionName	LO	INSTITUTO DE RADIOLOGIA
0008-0090	ReferringPhysicianName	PN	.^NAO LOCALIZADO^^^
0008-0100	CodeValue	SH	
0008-0102	CodingSchemeDesignator	SH	DCM
0008-0104	CodeMeaning	LO	
0008-1010	StationName	SH	ACHIEVA
0008-1030	StudyDescription	LO	R.M. ENCEFALO

Figura 2: Algumas *tags* referentes ao exame

Considerando a relevância do padrão DICOM para a disseminação das imagens médicas, é importante destacar que o DICOM *não* oferece segurança na transmissão, nem proteção dos dados. Em outras palavras, é possível adquirir uma imagem de forma ilegal e alterá-la, sem que se possa detectar

0010-0010	PatientName	PN	Morris^Rachel^B^^^
0010-0020	PatientID	LO	02005A46
0010-0030	PatientBirthDate	DA	19270127
0010-0040	PatientSex	CS	F
0010-1000	OtherPatientIDs	LO	204175157280003
0010-1030	PatientWeight	DS	49
0010-21C0	PregnancyStatus	US	4

Figura 3: Algumas *tags* referentes ao paciente

o uso indevido, a autenticidade da imagem, tampouco validar as informações nas *tags*. A referência [16] ilustra quão frágil é a segurança, utilizando um editor de texto tradicional para alterar algumas *tags*; no final, cita algumas técnicas de criptografia[1] para acrescentar alguma segurança.

No que se segue, percorrer-se-á outro caminho: a utilização de métodos de esteganografia aplicados a imagens médicas, que permitam agregar segurança e confidencialidade às informações contidas nas imagens médicas, minimizando perdas intrínsecas à manipulação dessas imagens, cujo uso em diagnósticos poderia ficar comprometido.

[1]Codificar uma mensagem para que apenas o emissor e o destinatário consigam ler o texto claro é o que faz a Criptografia. Nesse sentido, a Criptografia ocupa-se da segurança da mensagem, enquanto a Esteganografia ocupa-se da segurança da mensagem e do canal de comunicação.

3 Esteganografia

No Egito, as bibliotecas eram chamadas 'tesouro dos remédios da alma'. De fato é nelas que se cura a ignorância, a mais perigosa das enfermidades e a origem de todas as outras.

– Jacques Bossuet (teólogo, 1627-1704)

A Esteganografia é uma ciência que se ocupa de realizar comunicações *invisíveis*, isto é, a existência de mensagens secretas não deve ser detectada nessas comunicações. Trata-se de uma ferramenta a favor da privacidade. Assim, é natural que o ser humano tente atacá-la. Por essa razão, desenvolvem-se métodos para detectar a presença de mensagens secretas e, eventualmente, extraí-las. Tais técnicas deram origem à *Esteganálise*.

A principal propriedade de um sistema esteganográfico é ser estatisticamente indetectável, isto é, é impossível para um interceptador afirmar que *Alice* e *Bob*[2] estão se comunicando e utilizam esteganografia.

Em [6], lê-se a formulação do problema dos prisioneiros aplicado à esteganografia:

> Alice e Bob estão presos em celas separadas e desejam traçar um plano de fuga. É permitido que eles se comuniquem, mas essa comunicação é monitorada pelo guarda *Eve*[3]. Se Eve desconfiar que os prisioneiros estão secretamente trocando mensagens, ele suspenderá o canal de comunicação e colocará os prisioneiros em confinamento solitário. Assim, os prisioneiros recorrem à esteganografia para que consigam discutir os detalhes da fuga.

Observe-se que Eve precisa apenas detectar a presença de mensagens secretas, e não conhecer o conteúdo delas. Em outras palavras, quando Eve descobre que Alice e Bob estão se comunicando secretamente, o sistema esteganográfico é considerado *quebrado*. Comparando-se com a criptografia,

[2]Em geral, Alice desejar enviar uma mensagem para Bob. A escolha desses nomes é clássica, considerando o artigo de 1978 de Ron Rivest, em que o algoritmo de criptografia RSA foi apresentado.[23]

[3]Do inglês, *eavesdropper*, é normalmente alguém que pode interceptar as mensagens trocadas.

um ataque é bem-sucedido quando o conteúdo decriptografado é conhecido ou a chave de criptografia é parcialmente recuperada.

A segurança da esteganografia está em Eve não conseguir decidir e provar que um dado objeto de comunicação transmite uma mensagem secreta.

A seguir, estudar-se-ão três métodos de esteganografia, com vistas à aplicação em imagens médicas.

3.1 Inserção no Bit Menos Significativo

A informação em imagens digitais 24-bit é representada por uma matriz de triplas, e essas triplas correspondem a intensidades das cores vermelho, verde e azul (modelo RGB). Cada pixel da imagem pode ser descrito por uma tripla de valores associados a cada uma das cores. No caso de imagens 8-bit, em tons de cinza, padrão de imagens médicas, a imagem é representada por uma matriz de valores, em que cada elemento varia de 0 a 255, isto é, existem 256 tons possíveis para cada pixel.

O método de inserção no bit menos significativo é o mais óbvio e também o mais conhecido para ocultar informação em imagens. Como o próprio nome sugere, a informação é colocada no bit menos significativo de cada pixel. A ideia é que a alteração do bit menos significativo provoque uma alteração pouco perceptível.

Considere-se a representação binária da informação S a ser ocultada. O bit menos significativo de cada pixel da imagem será sobrescrito por $S_i \in \chi = 0, ..., 2^{n_c} - 1$, para $1 \leq i \leq |S|$ e n_c o número de bits da paleta gráfica. Assim,

$$S_i = \sum_{k=1}^{n_c} b[i,k] \cdot 2^{n_c - k},$$

em que $(b[i,1], ..., b[i,n_c])$ é a representação binária de S_i, sendo $b[i,n_c]$ o bit menos significativo.

Exemplo: A letra A é representada por 65 na tabela ASCII, cuja representação binária é 1000001. Para esteganográ-la na seguinte sequência de pixels de uma imagem 8-bit: 10000000, 10100100, 10110101, 10110101, 11110011, 10110111, 11100111, as seguintes alterações ocorrem: 1000000**1**,

10100100, 10110100, 10110100, 11110010, 10110110, 11100111.

3.1.1 Análise

No caso de imagens 24-bit, a modificação é mínima e praticamente imperceptível ao olho humano quando $|S|$ é razoável. As imagens 8-bit, porém, sofrem alterações relevantes e são facilmente detectadas com ataques de histograma, em que as frequências das intensidades dos pixels têm a sua distribuição modificada [6].

Esse método é bastante vulnerável a transformações geométricas e filtros, bem como esquemas de compressão (por exemplo, JPEG), pois tais técnicas implicam alterações nos bits menos significativos e a informação esteganografada é destruída.

Outro ponto fraco é a fácil recuperação da informação que se pretende ocultar. Em [6], é proposto que ocorra uma permutação dos bits, a partir de uma sequência de números pseudo-aleatórios gerada por meio de uma chave[4] compartilhada entre Alice e Bob. Ainda assim, o ataque via histograma seria bem-sucedido.

3.2 Divisão em Blocos e Alteração da Média

Outra abordagem é dividir a imagem em blocos de dimensão "suficientemente grande". Em outras palavras, tais blocos devem ser capazes de armazenar a informação S e não provocar diferença aparente antes e depois da esteganografia.

Seja B um bloco de dimensão $m \times n$ da imagem, o valor médio desse bloco será alterado de modo a representar o k-ésimo bit de S. Para tanto, [17] descreve este processo de tomada de decisão: calcula-se o valor médio M_i dos pixels do bloco B; calcula-se $M_{S_i}(j)$, que corresponde ao j-ésimo centro do espectro das médias com o símbolo S_i; calcula-se a nova média

$$M_d(i) = \underset{j=1,2,3,\ldots}{\arg\min} \left| M_{S_i}(j) - M_i \right|.$$

[4]Essa chave realizaria o papel de semente para a geração dos números aleatórios.

Define-se $\Delta M(i) = M_d(i) - M(i)$, que corresponde à alteração a ser produzida em cada pixel do bloco B, para obter a média que provoque a menor degradação possível na imagem e, além disso, aponte para o bit que guarda a informação S_i. A tabela abaixo ilustra alguns valores:

Tabela de Tomada de Decisão					
Espectro das médias	0 **1** 2	2 **3** 4	4 **5** 6	6 **7** 8	$\cdots$
Valor binário S_i	0	1	0	1	$\cdots$

De outra forma, cada bit 0 é obtido da equação $K/2 + 2Kt$ e cada bit 1 é obtido de $3K/2 + 2Kt$, em que K é a largura do espectro e $t \in \mathbb{N}$. Na tabela, adotou-se $K = 2$.

Finalmente, os elementos

$$B_{ij} \leftarrow B_{ij} + [\Delta M(i)]$$

são alterados, sendo que [.] representa o arredondamento para o inteiro mais próximo de $\Delta M(i)$.

3.2.1 Análise

Embora esse método ofereça melhores resultados que a inserção no bit menos significativo, alguns pontos de atenção são destacados em [17]:

1. o efeito do bloco é aparente nas regiões uniformes da imagem, ainda que a dimensão tenha sido bem escolhida;

2. o valor de $\Delta M(i)$ é arredondado para um inteiro próximo, o que pode alterar o valor médio esperado;

3. é necessário um pré-processamento da imagem para definir o intervalo de tons de cinza, o que pode causar alteração do brilho da imagem ou eliminar pequenos detalhes;

4. a alteração não é ótima: todos os pixels são alterados, o que torna a mudança mais perceptível. A alteração de menos pixels pode oferecer resultados melhores.

3.3 Método de Alteração da Média Modificado

Visando a aperfeiçoar o algoritmo proposto na subseção anterior, os autores de [17] propuseram algumas mudanças.

Inicialmente, os pixels da imagem devem ser embaralhados (*shuffling*) antes que a esteganografia ocorra. Isso minimiza o efeito causado pela alteração direta num determinado bloco, e acrescenta segurança: o gerador de números pseudo-aleatórios embaralha os pixels segundo determinada *semente*. Essa semente pode ser vista como uma *chave* compartilhada entre Alice e Bob.

Ademais, o algoritmo deve reduzir (ou elevar) os tons de cinza dos pixels a serem modificados até que a média objetivada seja alcançada; no entanto, o algoritmo impede que se altere *muito* certa região. Para isso, existe uma decisão (*switch mode*), em que, ultrapassado certo limite, o algoritmo não irá reduzir os tons de cinza para atingir a média sempre que isso degradar a imagem, e sim aumentar os tons de cada pixel, de modo que alteração total necessária seja alcançada.

Os autores de [17] definem:

- N1: número de pixels com valores superiores a $\Delta M(i)$, isto é, os que serão modificados;
- ΔG_T: alteração total necessária para que a média do bloco aproxime-se de $M_d(i)$, dada por $\Delta G_T = |\Delta M(i)| \cdot N$, em que N é o número total de pixels;
- $M_{d2}(i)$, $\Delta M_2(i)$, $N2$ e ΔG_{T2} são definidos de forma equivalente a $M_d(i)$, $\Delta M(i)$, $N1$ e ΔG_T sempre que o algoritmo entrar em *switch mode*.

Essas grandezas encontrarão espaço na descrição a seguir.

3.3.1 Pseudocódigo

No que se segue, descrever-se-á o algoritmo para esteganografia de conteúdo e sua consequente extração. Sempre que possível, detalhes serão acrescentados

ao apresentado em [17].

Esteganografia via MAMM:

1. Codifico a mensagem em representação binária (vide Inserção no Bit Menos Significativo);
2. Sorteio números pseudo-aleatórios utilizando a semente (chave) e re-ordeno os pixels da imagem;
3. Tomo $i = 1$;
4. Seleciono N pixels, de $(i-1) \times N+1$ a $i \times N$, que armazeno em $CB(i)$;
5. Calculo $M(i)$;
6. Calculo $M_d(i)$ – tomada de decisão (vide Divisão em Blocos e Alteração da Média);
7. Calculo $N1$;
8. Calculo ΔG_T;
9. Se $\Delta M(i) < 0$, então:
   - 9.1. s = 1 – definição da operação a ser executada em *switch mode*;
10. Caso contrário: s = -1;
11. Se $\Delta G_T > 2K \times N1$, então:
    - 11.1. Calculo $M_{d2}(i) = M_d(i) + 2K$, em que K é a largura do espectro, tolerância aceita;
    - 11.2. Calculo $N2$;
    - 11.3. Calculo $\Delta G_{T2} = N2 \cdot \Delta M_2(i)$, com $\Delta M_2(i) = 2K - |\Delta M(i)|$;
    - 11.4. Somo $1 \times s$ unidades, ΔG_{T2} vezes, aos pixels de $CB(i)$, cujos valores sejam menores que 255;

12. Caso contrário: Somo $-1 \times s$ unidades, ΔG_T vezes, aos pixels de $CB(i)$, cujos valores são maiores que 0;

13. Escrevo $CB(i)$ na imagem embaralhada;

14. Enquanto houver bits a serem esteganografados, incremento i e repito o processo a partir de 4;

15. Desembaralho a imagem que possui os blocos esteganografados para obter a imagem final.

O algoritmo de extração é, essencialmente, o caminho inverso do que foi descrito anteriormente. Utilizando-se a chave compartilhada será possível gerar a sequência de números pseudo-aleatórios novamente. Consequentemente, a tomada de decisão poderá ser repetida, o que permitirá a extração correta de cada bit esteganografado.

Extração do MAMM:

1. Gero a Tabela de Tomada de Decisão (TTD);

2. Gero os índices de embaralhamento a partir da sequência de números pseudo-aleatórios e a chave compartilhada;

3. Embaralho a imagem esteganografada;

4. Tomo $i = 1$;

5. Seleciono N pixels, de $(i-1) \times N+1$ a $i \times N$, que armazeno em $SB(i)$;

6. Determino M_{SB}, o valor médio de $SB(i)$;

7. Determino $b(i)$ associado a um intervalo do espectro das médias, no qual M_{SB} se encontra, utilizando a TTD;

8. Se ainda houver conteúdo a ser decodificado, incremento i e repito o processo a partir de 5;

9. Revelo o conteúdo armazenado com a esteganografia.

3.3.2 Implementação

A implementação do algoritmo MAMM de esteganografia foi realizada em MATLAB 7 pelo autor deste trabalho.

```
info = dicominfo('imagem_medica.dcm');
I = dicomread(info);
minimo = min(I(:));
maximo = max(I(:));
dimensao = 512
figure, imshow(I,[minimo maximo])

% Mensagem a ser codificada na imagem
msg = 'INSTITUTO DE RADIOLOGIA';
msg_codificada = reshape(dec2bin(msg, 7)', 1, []);

% Segredo utilizado para codificação
chave = 'IME USP';
rand('seed', sum(bin2dec(dec2bin(chave))));
CI = [];
for i = 1:dimensao
    r = randperm(dimensao);
    CI = [CI ; I(i, r)];
end

% Recomendações do artigo
N = 64; % Considerar-se nesta implementação que dimensao mod N == 0,
K = 2;  % e que K é sempre múltiplo de 2.
blocos = length(msg_codificada);

if (blocos * N > dimensao^2)
    error ('O payload é superior à capacidade de armazenamento da imagem.')
end
```

```
z = 1;
CB = zeros(blocos, N);
for i = 1:dimensao
    for j = 1:N:(dimensao-N+1)
        CB(z,:) = CI(i, j:(j+N-1));
        z = z + 1;
        if (z > blocos), break, end
    end
    if (z > blocos), break, end
end

z = z - 1;

% Espectros das médias
% 0 :   K/2 + 2*K*t
% 1 : 3*K/2 + 2*K*t,
% com t um inteiro positivo.

M   = [];
Md  = [];
Md2 = [];
Delta_M  = [];
Delta_M2 = [];
v = [];

for i = 1:z
    M(i) = mean(CB(i,:));

    if msg_codificada(i) == 0
        t0 = K/2;
    else
```

```
    t0 = 3*K/2;
end

minimo = 1000;

for t = 1:256/(2*K)
    v(t) = abs(t0 + 2*K*(t-1) - M(i));
    if minimo > v(t)
        minimo = v(t);
        t_minimo = t;
    end
end

Md(i) = t_minimo;
Delta_M(i) = Md(i) - M(i);

N1 = sum(CB(i) > Delta_M(i));
Delta_Gt = abs(Delta_M(i)) * N1;

if Delta_M(i) < 0
    sinal = 1;
else
    sinal = -1;
end

if Delta_Gt > 2*K * N1
    Md2(i) = Md(i) + 2*K;
    Delta_M2(i) = 2*K - abs(Delta_M(i));
    N2 = sum(CB(i,:) > Delta_M2(i));
    Delta_Gt2 = N2 * Delta_M2(i);
    CB(i, CB(i,:) < 255) = CB(i, CB(i,:) < 255) + sinal * Delta_Gt2;
else
```

```
        CB(i, CB(i,:) > 0) = CB(i, CB(i,:) > 0) - sinal * Delta_Gt;
    end

end

% Substituir os blocos modificados na imagem
z = 1;
for i = 1:dimensao
    for j = 1:N:(dimensao-N+1)
        CI(i, j:(j+N-1)) = CB(z,:);
        z = z + 1;
        if (z > blocos), break, end
    end
    if (z > blocos), break, end
end

% Unshuffle
rand('seed', sum(bin2dec(dec2bin(chave))));
SI = [];
for i = 1:dimensao
    r = randperm(dimensao);
    ir(r) = 1:dimensao;
    SI = [SI ; CI(i,ir)];
end

% Grava a imagem
dicomwrite(SI,'nova_imagem_medica.dcm', info);
```

3.3.3 Análise

O Método de Alteração da Média Modificado de [17] combate cada um dos pontos fracos dos algoritmos anteriores: a perceptibilidade da esteganogra-

fia causada pelo efeito do bloco; a alteração não desejada da informação armazenada, por meio da Tabela de Tomada de Decisão; a degradação da imagem, impondo limites de alteração.

Os autores de [17] realizaram testes quantitativos, utilizando várias coleções de imagens, e qualitativos, por meio de entrevistas com pessoas que pudessem opinar quanto a mudanças perceptíveis nas imagens. A conclusão de [17] quanto à utilização do método em imagens médicas é positiva, o que corrobora os resultados apresentados na próxima seção deste trabalho.

4 Métricas e Resultados

A maioria pensa com a sensibilidade, eu sinto com o pensamento. Para o homem vulgar, sentir é viver e pensar é saber viver. Para mim, pensar é viver e sentir não é mais que o alimento de pensar.

– Fernando Pessoa (escritor, 1888-1935)

Para avaliar os resultados dos métodos de esteganografia, duas abordagens serão adotadas: a qualitativa, que se ocupa da alteração visual significativa – para utilização clínica da imagem –, e quantitativa, em que se objetiva medir o grau de similaridade entre a imagem antes e depois de aplicado o método de esteganografia.

4.1 Análise qualitativa

Para esta análise, as imagens de diferença foram computadas por meio do *software* `ImageMagick` v6 [7].

Utilizando-se o método de Inserção no Bit Menos Significativo, os resultados para imagens médicas são insatisfatórios. A região de anomalia é agravada, como se observa abaixo:

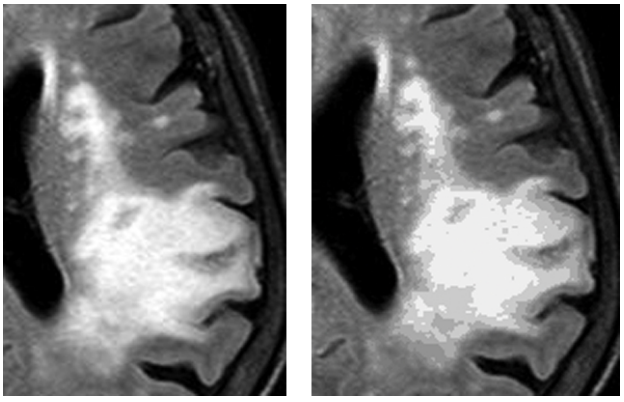

Figura 4: À esquerda, a imagem original. À direita, a imagem após LSB.

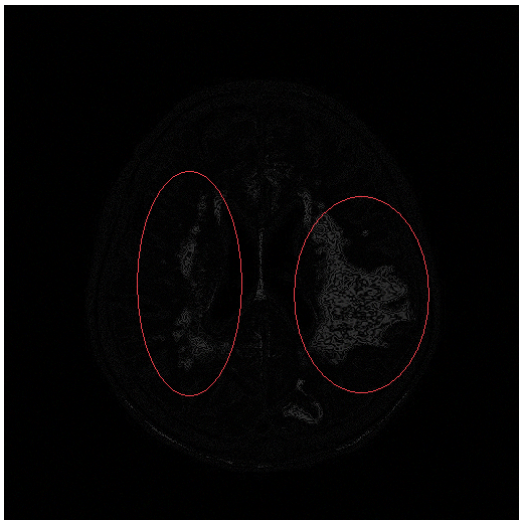

Figura 5: Diferença entre as imagens

O método de Divisão em Blocos e Alteração da Média provoca efeitos indesejados na imagem, bem como na segurança do método. Observe-se o efeito do bloco na comparação abaixo:

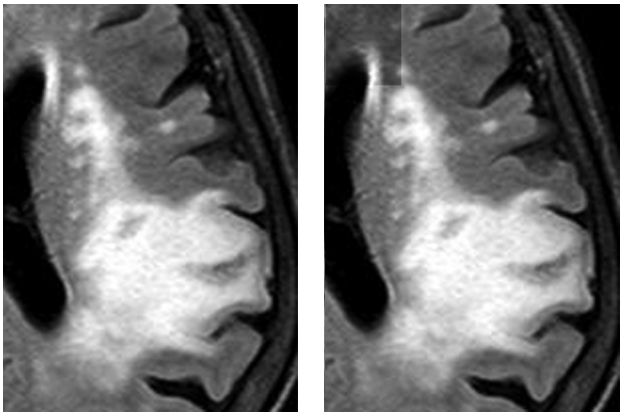

Figura 6: À esquerda, a imagem original. À direita, a imagem após aplicação do método de Divisão em Blocos.

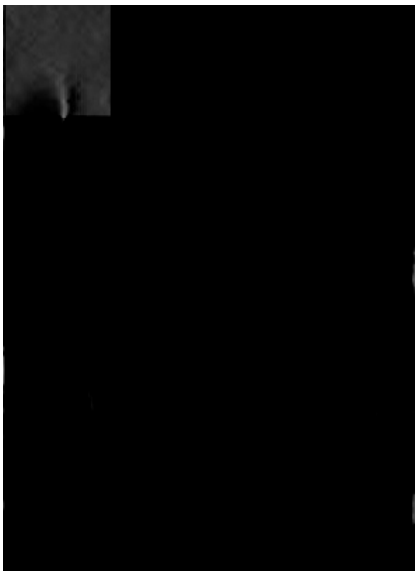

Figura 7: Diferença entre as imagens

O método de Alteração da Média Modificado é o que produz o melhor resultado visual em relação à degradação da imagem médica. Verifique a seguir:

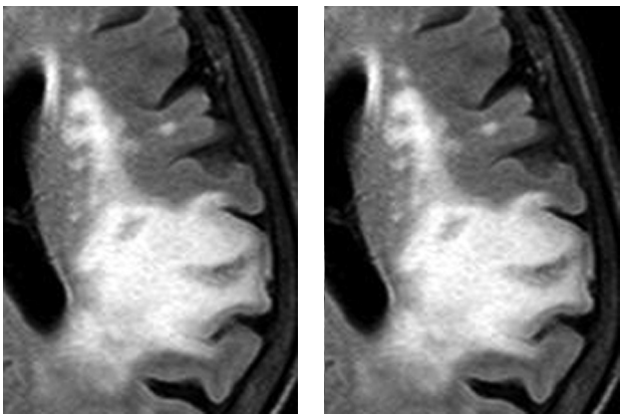

Figura 8: À esquerda, a imagem original. À direita, a imagem após aplicação do MAMM.

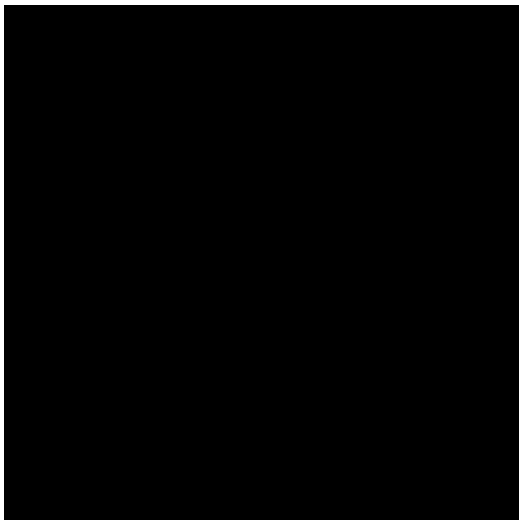

Figura 9: Diferença entre as imagens

4.2 Análise quantitativa

Para esta análise serão considerados três critérios sugeridos para imagens médicas em [22]. Sejam A a matriz que corresponde à imagem original e B a matriz da imagem obtida após a aplicação do método esteganográfico.

Definem-se:

1. Soma dos Quadrados das Diferenças (SSD):

$$SSD = \frac{1}{N} \sum_{i,j} |A_{ij} - B_{ij}|^2$$

2. Soma das Diferenças Absolutas (SAD):

$$SAD = \frac{1}{N} \sum_{i,j} |A_{ij} - B_{ij}|$$

3. Máxima Diferença Absoluta (MAD):

$$MAD = \frac{1}{N} \max |A_{ij} - B_{ij}|$$

A seguir, comparamos cada um dos métodos de esteganografia utilizando-se as métricas anteriores, a partir do mesmo conjunto de imagens médicas[5].

Tabela de Comparação dos Métodos			
	Inserção LSB	Divisão em Blocos	MAMM
SSD	1449	109	14
SAD	18	4	2
MAD	$2,14 \cdot 10^{-3}$	$9,16 \cdot 10^{-4}$	$5,29 \cdot 10^{-4}$

Tal como observado na análise qualitativa, o Método de Alteração da Média Modificado é o que apresenta a maior similaridade significativa entre as imagens antes e depois da aplicação da esteganografia, considerando as métricas SSD, SAD e MAD.

[5]A saber BU001015-V01 (13.95 MB), MR (32.63 MB), CT (255.02 kB), chest (3.72 MB), mammo (3.29 MB), skull (6.12 MB), disponibilizadas gratuitamente no sítio do MicroDicom.

5 Conclusões

Se queres compreender a palavra 'felicidade', indispensável se torna entendê-la como recompensa e não como fim.

– Antoine de Saint-Exupéry (aviador e escritor, 1900-1944)

O padrão DICOM está bem estabelecido quanto ao armazenamento, impressão e transmissão de imagens médicas. No entanto, não dispõe de métodos de segurança que preservem a confidencialidade dos dados na imagem, tampouco a autenticidade destes.

O estudo realizado neste trabalho mostra que o Método de Alteração da Média Modificado fornece uma técnica para ocultar a informação de interesse nos pixels da imagem. Esse método não provoca degradação aparente nesta, viabilizando a utilização clínica da imagem. Dessa forma, a partir de uma chave compartilhada entre o remetente e o destinatário da imagem, é possível que aquele esteganografe as *tags* confidenciais e este faça a extração delas. Qualquer alteração intencional ou acidental nas *tags* não irá interferir na informação esteganografada, o que garante a autenticidade delas.

A integração do MAMM ao padrão DICOM propiciaria um grande avanço para a segurança da informação em imagens médicas, coibindo fraudes e invasão de privacidade.

Referências

[1] Dicom tag list, 2005. URL: http://www.dicomtags.com.

[2] National Electrical Manufacturers Association. Digital imaging and communications in medicine - part 1: Introduction and overview, 2011. URL: http://medical.nema.org/Dicom/2011/11_01pu.pdf.

[3] Bjorn De Sutter Bertrand Anckaert and Koen De Bosschere. Steganography for executables. 2004. URL: http://escher.elis.ugent.be/publ/Edocs/DOC/R104_003.pdf.

[4] Dominique Chanet Bertrand Anckaert, Bjorn De Sutter and Koen De Bosschere. Steganography for executables and code transformation signatures. 2005. URL: http://escher.elis.ugent.be/publ/Edocs/DOC/P105_052.pdf.

[5] Abbas Cheddad. *Digital Image Steganography*. VDM Verlag Dr. Müller, December 2009. URL: http://www.abbascheddad.net/.

[6] Jessica Fridrich. *Steganography in Digital Media*. Cambridge University Press, November 2009. URL: http://ws2.binghamton.edu/fridrich/.

[7] ImageMagick. Image comparing. URL: http://www.imagemagick.org/Usage/compare/.

[8] Medical Imaging in IDL. Dicom attributes, 2005. URL: http://star.pst.qub.ac.uk/idl/DICOM_Attributes.html.

[9] Neil F. Johnson. Information hiding: Steganography & digital watermarking. URL: http://www.jjtc.com/Steganography/.

[10] Stefan Katzenbeisser. *Information hiding techniques for steganography and digital watermarking*. Artech House, 1999. URL: http://www.petitcolas.net/fabien/publications/book99-ih/index.html.

[11] Gary C. Kessler. Steganography: Hiding data within data. *Windows & .NET Magazine*, April 2002. URL: http://www.garykessler.net/library/steganography.html.

[12] Gary C. Kessler. An overview of steganography for the computer forensics examiner. *FBI Forensic Science Communications*, July 2004. URL: http://www.garykessler.net/library/fsc_stego.html.

[13] Husrev T. Sencar Mehdi Kharrazi and Nasir Memon. Image steganography: Concepts and practice, April 2004. URL: http://isis.poly.edu/~steganography/pubs/ims04.pdf.

[14] Mazleena Salleh Muhalim Mohamed Amin, Subariah Ibrahim and Mohd Rozi Katmin. Information hiding using steganography. 2003. URL: http://eprints.utm.my/4339/1/71847.pdf.

[15] Nick Nabavian. Image steganographic. November 2007. URL: http://www1.chapman.edu/~nabav100/ImgStegano/download/ImageSteganography.pdf.

[16] Oleg S. Pianykh. *Digital Imaging and Communications in Medicine: A Practical Introduction and Survival Guide*. Springer, July 2008. URL: http://cs.jhu.edu/~sdoshi/jhuisi650/papers/dicomsecuritychap11.pdf.

[17] Mohammad Jahangiri Pouria Mortazavian and Emad Fatemizadeh. A low-degradation steganography model for data hiding in medical images. *4th IASTED International Conference*, pages 914–920, September 2004. URL: http://www.commsp.ee.ic.ac.uk/~jahangiri/Papers/IASTED.pdf.

[18] Niels Provos and Peter Honeyman. Detecting steganographic content on the internet. 2001. URL: http://niels.xtdnet.nl/papers/detecting.pdf.

[19] Niels Provos and Peter Honeyman. Hide and seek: An introduction to steganography. *IEEE Security and Privacy*, pages 32–44, May / June 2003. URL: `http://niels.xtdnet.nl/papers/practical.pdf`.

[20] Deborah Radcliff. Quickstudy: Steganography: Hidden data. *Computerworld*, June 2002. URL: `http://www.computerworld.com/s/article/71726/Steganography_Hidden_Data`.

[21] Anderson Rocha and Siome Goldenstein. Steganography and steganalysis in digital multimedia: Hype or hallelujah? *RITA*, XV(1):83–110, 2008. URL: `http://www.ic.unicamp.br/~siome/papers/Rocha-Rita08.pdf`.

[22] J. N. Ulysses and A. Conci. Measuring similarity in medical registration. *IWSSIP 2010 - 17th International Conference on Systems, Signals and Image Processing*, 2010. URL: `http://www.ic.uff.br/iwssip2010/Proceedings/nav/papers/paper_189.pdf`.

[23] Wikipedia. Alice and bob. URL: `http://en.wikipedia.org/wiki/Alice_and_Bob`.

[24] Wikipedia. Medical radiography. URL: `http://en.wikipedia.org/wiki/Medical_radiography`.

Parte II

Subjetiva

1 Desafios e frustrações

Dividirei esta seção em duas partes, em que tratarei dos desafios e frustrações encontrados no BCC e no desenvolvimento deste trabalho.

Certa vez, ao conversar com o Prof. Eduardo Colli, observamos que um aluno de graduação, e mesmo de pós-graduação, recebe um grande desafio: *aprender a estudar*. Num primeiro momento, tal afirmação pode parecer muito nítida, mas retém implícita a responsabilidade solitária de descobrir o que é mais eficaz para o aprendizado. Há muitas aulas que são essenciais; em outras muitas ocasiões, é preciso digerir o assunto com muita leitura, exercícios e reflexão. Em todos os casos, no entanto, é preciso descobrir o que funciona melhor para *você*, desde a escolha da bibliografia, o lugar para estudar, o tipo de anotações, a organização e planejamento para a entrega de trabalhos nos prazos e preparo para provas. É certamente um desafio que, por consequência, traz um grande aprendizado.

Quanto ao desenvolvimento deste trabalho, o maior desafio foi lidar com uma bibliografia escassa. Esteganografia é uma área específica e, talvez por essa razão, discutida principalmente em artigos. Nem sempre esses artigos tratam com rigor científico as suas abordagens. Muitas referências encontradas na internet são imprecisas, apresentando esteganografia e técnicas para marcas d'água indistintamente.

A principal autora contemporânea de Esteganografia é a Profa. Jessica Fridrich, da Universidade de Binghamton no Estado de Nova Iorque. Os livros-texto dela propiciaram um norte para este trabalho, principalmente para o entendimento de conceitos presentes no artigo de interesse [17]. No entanto, ao procurar o principal autor desse artigo, para ter detalhes de certos pontos que não estão claros no texto, não houve retorno. Isso foi um pouco frustrante.

2 Aprendizados

Desenvolver um trabalho ao longo de um ano propicia grandes aprendizados, pois existe tempo para administrá-lo – *planejar, organizar, dirigir, executar e controlar*. Recorrentemente, cada uma das partes do trabalho se insere nessa cadeia de processos.

2.1 Acadêmicos

Escrever a monografia é extrair o cerne do que foi absorvido ao longo de todo o trabalho.

Seguramente, a experiência de ler artigos científicos e, sobretudo, preencher as várias lacunas deixadas pelos autores é um dos maiores aprendizados, pois são poucas as disciplinas que oferecem esse espaço na graduação e, em geral, são optativas eletivas.

Outro aprendizado, provindo do contato com o autor [17], é que a produção de qualquer trabalho científico predispõe *continuação*. Todos os anos, o BCC do IME produz dezenas de trabalhos interessantes[6]. Manter-se disponível e colaborar para que alguém no futuro possa dar continuidade à pesquisa é importante.

2.2 Tecnologias

Desde o início, foi criado o sítio e um *blog*, para manter atualizada e centralizada a evolução do trabalho, exercitando-se a criatividade para *web design*.

A edição desta monografia, bem como a do pôster e a dos slides, foi possível graças à existência do LaTeXe da classe Beamer. Certamente, os resultados valeram as várias horas empregadas para o aprendizado da sintaxe *peculiar* dessa linguagem de edição de textos.

Além disso, para a implementação dos algoritmos e comparações qualitativas das imagens, foram utilizados o Matlab 7 e o ImageMagick v6, que propiciariam momentos de experiência com programação matemática.

[6] Atualmente, disponibilizados aqui.

3 Disciplinas relevantes

Ter cursado a disciplina de Introdução à Computação Gráfica (MAC 420), ministrada pelo Prof. Marcel P. Jackowski, foi muito importante, pois até então o meu conhecimento de edição de imagens não era formal, apenas técnica, apoiada no Adobe Photoshop. Além disso, o contato com as estruturas de dados gráficas, paletas de cores e técnicas de modelagem foram muito importantes.

Nas disciplinas de Inteligência Artificial (MAC 425), ministrada pelo Prof. Flávio S. Corrêa, e Armazenamento e Recuperação de Informação (MAC 333), ministrada pelo Prof. Alair Pereira do Lago, tive contato com a leitura de artigos científicos, visando a implementação de um exercício-programa naquela e um artigo nesta.

Destaco também outras disciplinas que contribuíram para ampliar a minha visão de Ciência da Computação – Análise de Algoritmos (MAC 338), ministrada pelo Prof. José Augusto R. Soares, e Conceitos Fundamentais de Linguagens de Programação (MAC 316), ministrada pela Profa. Ana Cristina V. de Melo.

Por fim, as minhas professoras de Cálculo Integral e Diferencial – Profa. Heloísa Borsari, Profa. Lucília Borsari, Profa. Zara Issa Abud – e os meus professores de Álgebra – Prof. Francisco César Polcino e Profa. Heloísa Borsari – foram responsáveis por disciplinas que contribuíram para o meu amadurecimento matemático, principalmente a abstração, sem os quais nenhuma ciência exata pode ser verdadeiramente compreendida.

4 Pesquisa futura

Este trabalho pode ainda evoluir nas seguintes direções:

- Como garantir que *sempre* ocorrerá um embaralhamento (*shuffling*) conveniente dos pixels da imagem?
- Aumento do *payload*[7] com a utilização de vários cortes[8] de imagens médicas, de modo que nenhuma imagem carregue muita informação, reduzindo a perceptibilidade das alterações;
- Códigos corretores de erros, para garantir que os bits armazenados na imagem, se danificados por ruído, ainda possam ser recuperados;
- OCR[9] para ocultação de informação na superfície das imagens;
- A combinação de Esteganografia e Criptografia é boa? Não existe consenso entre os autores lidos.

[7] Informação que se deseja esteganografar numa imagem.

[8] Durante a realização de um exame médico, centenas de imagens são geradas. Cada uma delas é um *corte* de determinado órgão sob certo ângulo.

[9] Do inglês, *Optical Character Recognition*, é o reconhecimento de caracteres textuais numa imagem.