Avaliação de Métodos Esteganográficos em Imagens Médicas

Rafael A. Sampaio[1], **Marcel P. Jackowski**[1]

[1]Departamento de Ciência da Computação
Instituto de Matemática e Estatística
Universidade de São Paulo, Brasil

{rsampaio, mjack}@ime.usp.br

Abstract. *Digital Imaging and Communications In Medicine (DICOM) is a well-established standard regarding storage, printing, and transmission of medical images. However, there are no security methods that preserve metadata confidentiality, nor image authenticity. This work assesses three steganographic methods – least significant bit insertion (LSB), division into blocks, mean change modified method (MCMM) – and verify their feasibility for clinical use in medical imaging. Integrating MCMM in DICOM standard would provide increased information security in medical imaging, deterring fraud, privacy invasion, while preserving diagnostic information.*

Resumo. *Digital Imaging and Communications In Medicine (DICOM) é um padrão bem estabelecido no que diz respeito ao armazenamento, impressão e transmissão de imagens médicas. Contudo, não existem mecanismos de segurança que garantam a confidencialidade dos metadados, nem a autenticidade da imagem. Este trabalho avalia três métodos esteganográficos – a inserção no bit menos significativo (LSB), divisão em blocos, método modificado da alteração da média (MMAM) – e verifica a aplicação destes em imagens médicas para uso clínico. A integração do MMAM no padrão DICOM propiciaria um grande avanço para a segurança da informação das imagens médicas, impedindo fraudes, invasão de privacidade, e preservando as informações de diagnóstico.*

1. Introdução

Digital Imaging and Communications In Medicine (DICOM) é um padrão bem estabelecido de armazenamento, impressão e transmissão da informação presente nas imagens médicas, haja vista que o armazenamento dos dados ocorre em *tags* irrestritamente editáveis. As imagens originadas desses exames podem inadvertidamente ser compartilhadas, expondo tais informações, sem que se possa verificar a autenticidade e o uso indevido.

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.

Este trabalho avalia três métodos esteganográficos conhecidos na literatura, e verifica a aplicabilidade destes a imagens médicas com finalidade clínica. A proposta é acrescentar segurança e confidencialidade à informação contida no DICOM, sem comprometer a qualidade da informação para diagnóstico.

1.1. Trabalhos relacionados

Enquanto a avaliação de autenticidade de imagens médicas pode ser encontrada na literatura [Kannammal and Rani 2011, Zain and Clarke 2007, Cao 2003, Kim Hyoungseop and Akiyoshi 2005], não se tem notícia de nenhuma pesquisa acerca da informação presente nas *tags* do DICOM ser incorporada nas suas respectivas imagens. Neste trabalho, exploram-se três métodos esteganográficos para incluir informação textual em imagens médicas: inserção no último bit significativo [Fridrich 2009]; divisão em blocos e alteração da média [Pouria Mortazavian and Fatemizadeh 2004]; e o método modificado de alteração da média [Pouria Mortazavian and Fatemizadeh 2004].

2. Imagens Médicas e DICOM

A Medicina moderna avançou bastante nos últimos anos e o mérito desse progresso deve ser compartilhado com outras ciências.

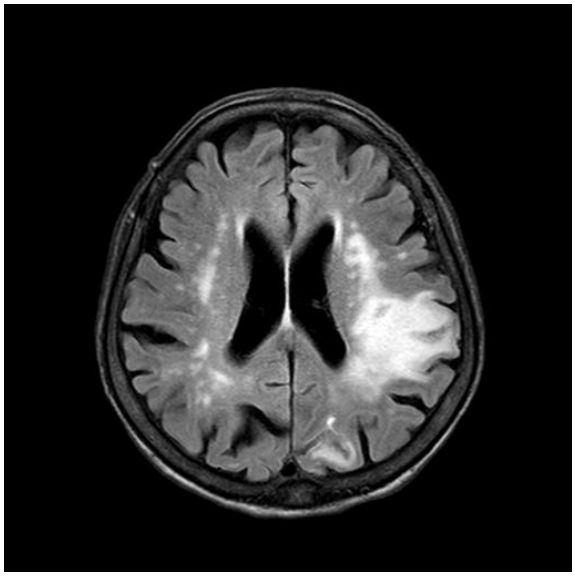

Figura 1. Imagem obtida por ressonância magnética de um cérebro humano, no qual as regiões hiperintensas indicam anormalidade de tecido.

Com o 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 [National Electrical Manufacturers Association 2011a].

Tag	Descrição	Tipo	Valor
0008-0022	AcquisitionDate	DA	20110913
0008-0070	Manufacturer	LO	Philips Medical System
0008-0080	InstitutionName	LO	INSTITUTO DE RADIOLOGIA
0008-0090	ReferringPhysicianName	PN	.^NAO LOCALIZADO^^^
0008-0102	CodingSchemeDesignator	SH	DCM
0008-1010	StationName	SH	ACHIEVA
0008-1030	StudyDescription	LO	R.M. ENCEFALO
0008-103E	SeriesDescription	LO	AXIAL FLAIR
0008-1040	InstitutionalDepartmentName	LO	RESSONANCIA MAGNETICA

Tabela 1. Um subconjunto de *tags* relacionadas a informações clínicas

Tag	Descrição	Tipo	Valor
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

Tabela 2. Um subconjunto de *tags* relacionadas a informações do paciente

Os arquivos DICOM possuem duas componentes: um cabeçalho (*header*), em que se encontram diversas informações confidenciais do paciente, do local onde o exame foi realizado, dos aparelhos e responsáveis, entre outras; e uma matriz em tons de cinza, que representa as intensidades da imagem. O cabeçalho é composto por um conjunto de *tags* que, atualmente, já somam mais de 3300 distintas. A listagem pode ser encontrada nas referências [National Electrical Manufacturers Association 2011b, Lawrence Berkeley National Laboratory Visualization Group 2005]. Veja exemplos nas tabelas 1 e 2.

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 [Pianykh 2008]. Em outras palavras, é possível adquirir uma imagem de forma ilegal e alterá-la, sem que se possa detectar o uso indevido, a autenticidade da imagem, tampouco validar as informações nas *tags*. Pianykh ilustra quão frágil é a segurança, utilizando um editor de texto tradicional para alterar algumas *tags*. Algumas técnicas de criptografia foram, então, acrescentadas visando a oferecer segurança.

3. Esteganografia

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. Por se tratar de uma ferramenta a favor da privacidade é natural que o ser humano tente atacá-la. Por essa razão, desenvolveram-se métodos para detectar a presença de mensagens secretas e, eventualmente, extraí-las.

A principal propriedade de um sistema esteganográfico é ser estatisticamente in-

detectável, isto é, deve ser impossível para um interceptador afirmar que *Alice* e *Bob*[1] estão se comunicando.

Fridrich formula o 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*[2]. 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*. A segurança da esteganografia está em Eve não conseguir decidir e provar que um dado objeto de comunicação transmite uma mensagem secreta.

Três métodos de esteganografia são descritos a seguir e, posteriormente, serão avaliados quanto à aplicabilidade a imagens médicas.

3.1. Inserção no bit menos significativo

Neste método, assume-se que 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, a imagem é representada por uma matriz de valores de tons de cinza.

O método de inserção no bit menos significativo é o mais óbvio e também o mais conhecido para ocultar informação em imagens. A alteração no bit menos significativo de cada pixel da imagem deve causar uma mudança visual quase imperceptível.

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.

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 [Fridrich 2009].

[1]Em geral, Alice desejar enviar uma mensagem para Bob. A escolha dos nomes é clássica após o artigo de 1978 de Ron Rivest, em que o algoritmo de criptografia RSA foi apresentado [Schneier 1996].

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

Este 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. Fridrich propôs uma permutação dos bits a partir de uma sequência de números pseudo-aleatórios gerada por meio de uma chave 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, Mortazavian et al. descrevem 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

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

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 3 encontrada em [Pouria Mortazavian and Fatemizadeh 2004] 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	$\cdots$

Tabela 3.

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, $K = 2$.

Finalmente, os elementos

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

são alterados, sendo que $[.]$ representa o arredondamento para o inteiro mais próximo de $\Delta M(i)$. Embora esse método ofereça melhores resultados que a inserção no bit menos significativo, alguns pontos de atenção são destacados por Mortazavian et al. em [Pouria Mortazavian and Fatemizadeh 2004]:

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 modificado de alteração da média

Visando a aperfeiçoar o algoritmo proposto na subseção anterior, Mortazavian et al. propuseram uma técnica que embaralha os pixels da imagem (*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) as intensidades dos tons de cinza dos pixels a serem modificados até que a média objetivada seja alcançada. No entanto, o algoritmo deve impedir que se altere substancialmente certa região. Para isso, existe uma decisão (*switch mode*), em que, após ultrapassado certo limite, o algoritmo não irá reduzir a paleta de tons de cinza para atingir a média se isso degradar a imagem, e sim aumentar as intensidades de cada pixel, de modo que alteração total necessária seja alcançada.

3.4. Pseudocódigo

Mortazavian et al. definem em [Pouria Mortazavian and Fatemizadeh 2004]:

- 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*.

Descrevemos a seguir o algoritmo para codificação de conteúdo, por meio de esteganografia, e o algoritmo correspondente de extração.

Esteganografia via MMAM:

1. Codifico a mensagem em representação binária (vide Inserção no Bit Menos Significativo);
2. Sorteio números pseudo-aleatórios utilizando a chave como semente e reordeno 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:
    (a) 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:
    (a) Calculo $M_{d2}(i) = M_d(i) + 2K$, em que K é a largura do espectro, tolerância aceita;
    (b) Calculo $N2$;
    (c) Calculo $\Delta G_{T2} = N2 \cdot \Delta M_2(i)$, com $\Delta M_2(i) = 2K - |\Delta M(i)|$;
    (d) 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 será repetida, o que permitirá a extração correta de cada bit esteganografado.

Extração do MMAM:

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.

O Método Modificado de Alteração da Média combate cada um dos pontos fracos dos algoritmos anteriores: a perceptibilidade da esteganografia 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.

Implementamos o algoritmo MMAM aqui descrito – o código-fonte pode ser disponibilizado contatando-nos.

4. Resultados

Duas abordagens foram adotadas para avaliar os resultados dos métodos de esteganografia: qualitativa, que avalia o quanto as alterações na imagem podem ser visualmente identificáveis – e quantitativa, que mede o grau de similaridade entre a imagem antes e depois de aplicado o método de esteganografia, para ocultar todas as *tags* não-vazias de uma imagem médica no padrão DICOM.

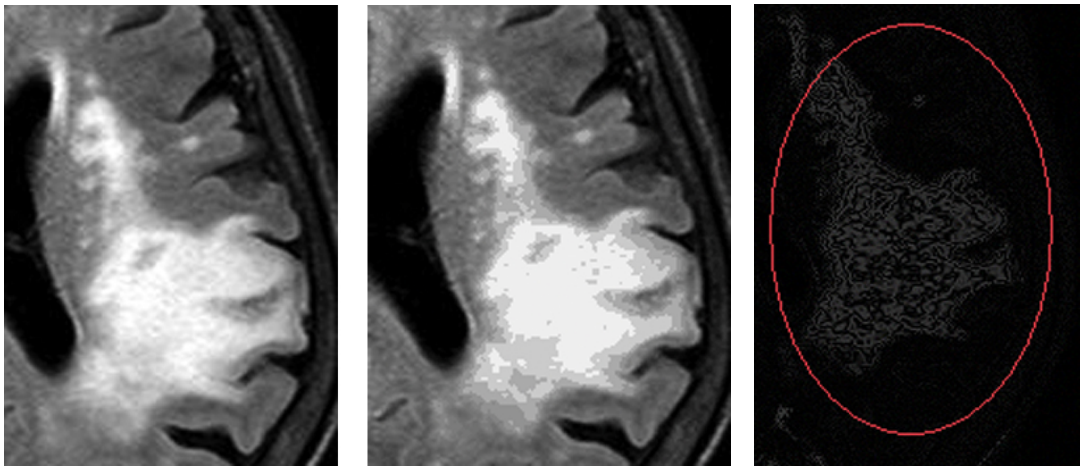

Figura 2. (a) Imagem original. (b) Imagem depois do LSB. (c) Imagem diferença.

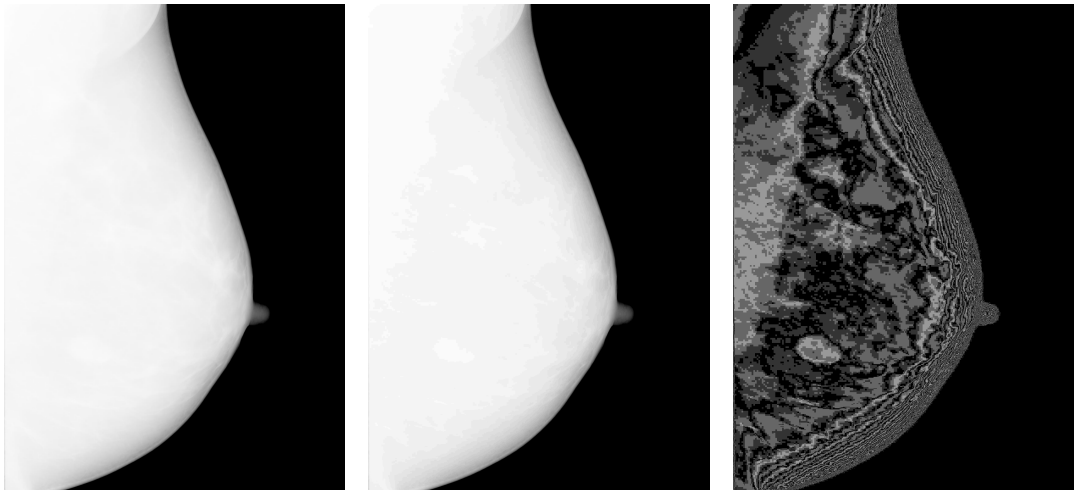

Figura 3. (a) Imagem original. (b) Imagem depois do LSB. (c) Imagem diferença.

4.1. Análise qualitativa

Estudaremos uma imagem de ressonância magnética de um cérebro humano, cedida pelo Medical Imaging Group do IME-USP, e uma imagem de mamografia disponibilizada livremente em [MicroDicom]. Nesta análise, as imagens de diferença foram computadas pelo *software* `ImageMagick` v6.

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 na Figura 2, em que se vê a ressonância magnética de um cérebro humano.

Também pode-se observar a perda de detalhes quando se uma observa o resultado do LSB aplicado a uma mamografia, tal como na Figura 3.

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 imagem de ressonância magnética de um cérebro humano (Figura 4).

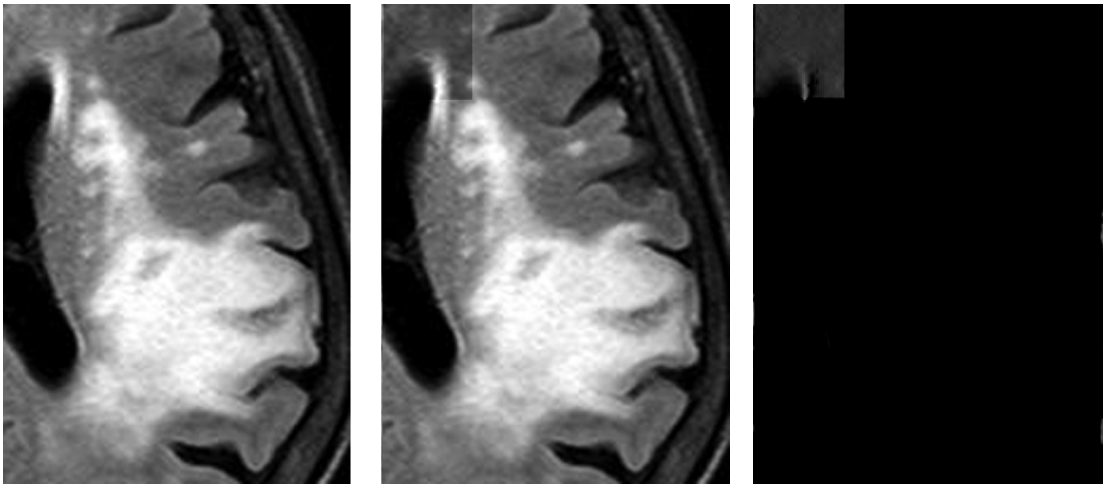

Figura 4. (a) Imagem original. (b) Imagem depois do método de divisão em blocos. (c) Imagem diferença.

Tal efeito indesejável também é observado na aplicação do método a uma imagem de mamografia, como visto na Figura 5.

O método modificado de alteração da média é o que produz o melhor resultado visual em relação à degradação da imagem médica. Veja a Figura 6 de uma ressonância magnética de um cérebro humano.

O resultado também é favorável aplicando-se o MMAM a uma imagem de mamografia (Figura 7).

4.2. Análise quantitativa

Três critérios critérios foram considerados para comparar as imagens médicas antes e depois da esteganografia [Ulysses and Conci 2010]. Sejam A a matriz que corresponde à imagem original e B a matriz da imagem obtida após a aplicação do método esteganográfico.

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 comparação foi feita com cada um dos métodos de esteganografia, utilizando-se as métricas anteriores e a partir do mesmo conjunto de imagens médicas[3] (veja Tabela 4).

[3]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]

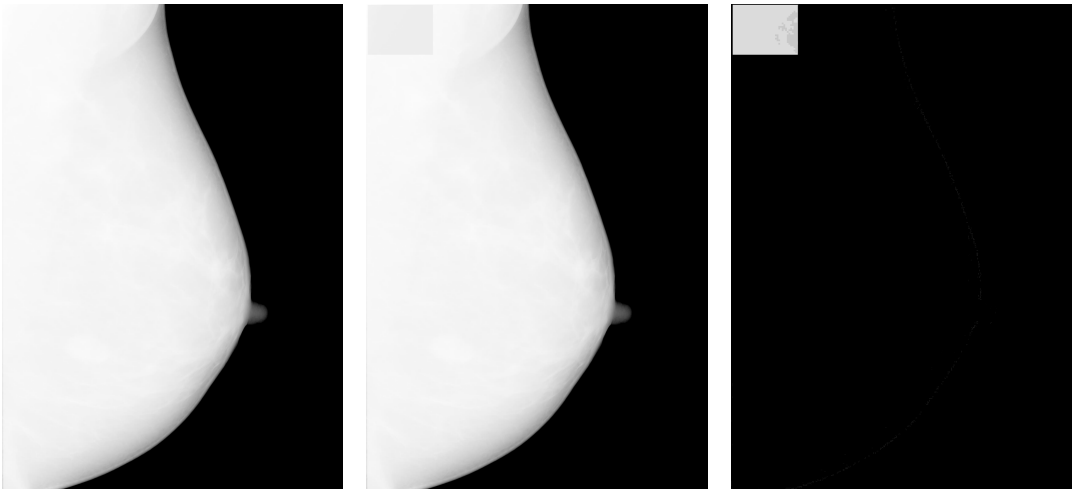

Figura 5. (a) Imagem original. (b) Imagem depois do método de divisão em blocos. (c) Imagem diferença.

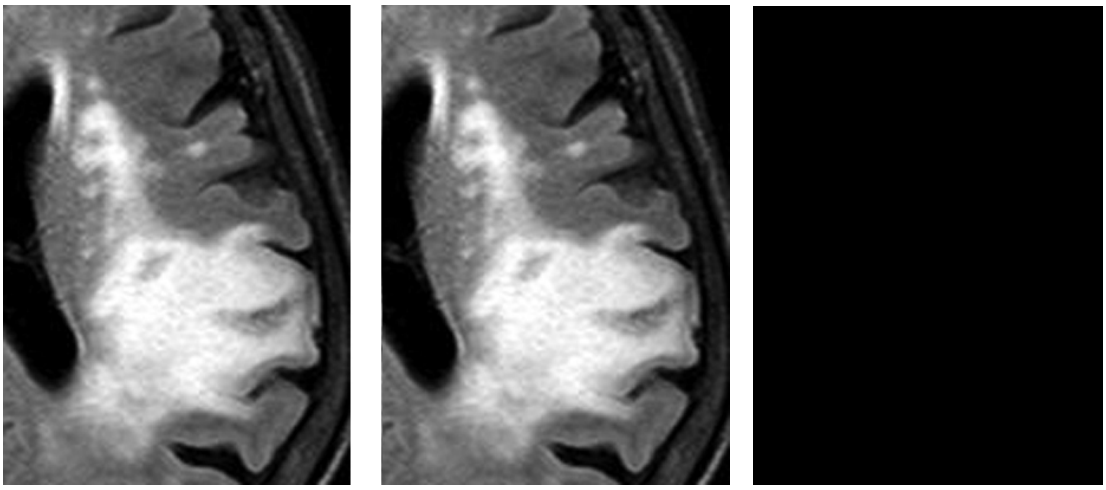

Figura 6. (a) Imagem original. (b) Imagem depois do MMAM. (c) Imagem diferença.

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

Tabela 4. Valores médios para um conjunto de imagens médicas[3]

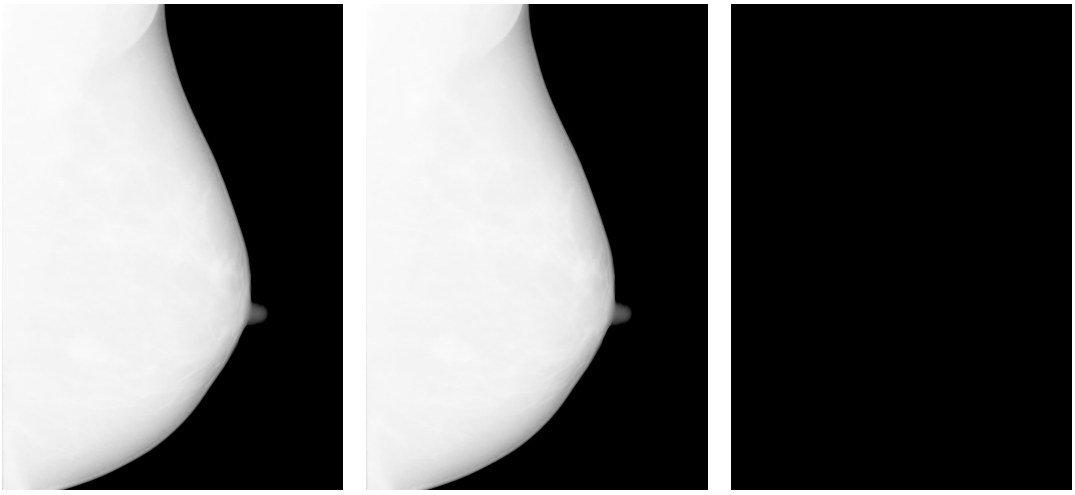

Figura 7. (a) Imagem original. (b) Imagem depois do MMAM. (c) Imagem diferença.

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

5. Conclusões

O DICOM é um padrão 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.

Este trabalho mostra que o Método Modificado de Alteração da Média fornece uma técnica para ocultar a informação, guardando-a nos pixels da imagem. O MMAM não provoca degradação aparente, preservando a informação clínica. Dessa forma, a partir de uma chave compartilhada entre o remetente e o destinatário da imagem, é possível que se esteganografe as *tags* confidenciais e se faça a extração delas posteriormente. Qualquer alteração intencional ou acidental nas *tags* não irá interferir na informação esteganografada, o que garante a autenticidade. Além disso, MMAM preserva a informação clínica melhor que os métodos LSB e a Divisão em Blocos, dada a tabela de comparação 4. Apesar disso, pesquisas adicionais ainda devem ser realizadas.

A integração do MMAM ao padrão DICOM propiciaria um grande avanço para a segurança da informação em imagens médicas, coibindo fraudes e invasão de privacidade, enquanto preserva a informação para o uso clínico.

Referências

Cao, F. (2003). Medical image security in a HIPAA mandated PACS environment. *Computerized Medical Imaging and Graphics*, 27(2-3):185–196.

Fridrich, J. (2009). *Steganography in Digital Media*. Cambridge University Press.

Kannammal, A. and Rani, S. S. (2011). Authentication of DICOM Medical Images using Multiple fragile watermarking Techniques in Wavelet Transform Domain. *IJCSI International Journal of Computer Science Issues*, 8(1):181–189.

Kim Hyoungseop, Onishi Ramu, I. S. K. S. N. M. and Akiyoshi, Y. (2005). Embedding of DICOM image based on steganography techniques. *IEICE Technical Report*, 105(303):31–34.

Lawrence Berkeley National Laboratory Visualization Group (2005). Medical Imaging in IDL - DICOM Attributes. `http://vis.lbl.gov/NERSC/Software/idl/help6.2/medical.pdf`. (acessado em 14/11/2013).

MicroDicom. Sample DICOM images. `http://www.microdicom.com/downloads.html`. (acessado em 14/11/2013).

National Electrical Manufacturers Association (2011a). Digital imaging and communications in medicine - part 1: Introduction and overview. `http://medical.nema.org/Dicom/2011/11_01pu.pdf`. (acessado em 14/11/2013).

National Electrical Manufacturers Association (2011b). Digital imaging and communications in medicine - part 6: Data dictionary. `http://medical.nema.org/Dicom/2011/11_06pu.pdf`. (acessado em 14/11/2013).

Pianykh, O. S. (2008). *Digital Imaging and Communications in Medicine: A Practical Introduction and Survival Guide*. Springer.

Pouria Mortazavian, M. J. and Fatemizadeh, E. (2004). A low-degradation steganography model for data hiding in medical images. *4th IASTED International Conference*, pages 914–920.

Schneier, B. (1996). *Applied Cryptography, Second Edition: Protocols, Algorthms, and Source Code in C*. John Wiley & Sons, Inc.

Ulysses, J. N. and Conci, A. (2010). Measuring similarity in medical registration. *IWSSIP 2010 - 17th International Conference on Systems, Signals and Image Processing*.

Zain, J. M. and Clarke, M. (2007). Reversible Region of Non-Interest (RONI) Watermarking for Authentication of DICOM Images. *International Journal of Computer Science and Network Security*, 7(9):19–27.