CLASSIFICAÇÃO DE TÉCNICAS ESTEGANOGRÁFICAS

Nichols Aron Jasper[1], Silvio do Lago Pereira[2]
[1]Aluno do Curso de Processamento de Dados – FATEC-SP
[2]Prof. Dr. do Departamento de Tecnologia da Informação – FATEC-SP
nicholsaron@hotmail.com, slago@ime.usp.br

Resumo

Atualmente, a segurança da informação é um tema de grande relevância para a tecnologia da informação. Basicamente, há duas formas de proteger informação: usar criptografia para ocultar seu significado ou usar esteganografia para ocultar sua presença. Claramente, combinando estas duas formas de proteção, conferimos um nível adicional de segurança à informação. Apesar disto, a maioria dos sistemas informatizados usa apenas criptografia, de modo que a esteganografia ainda é pouco conhecida. Assim, neste artigo, apresentamos uma visão geral das técnicas esteganográficas e propomos uma forma de classificá-las em função de suas similaridades. A partir desta classificação, usamos conceitos da segurança de informação para evidenciar seus pontos fortes e fracos. Ademais, usando o conceito de esteganografia em camadas, discutimos como o uso simultâneo de diversas técnicas de esteganografia pode fortalecer a segurança da informação.

1. Introdução

Nos dias atuais, a segurança da informação [1] é um tema amplamente discutido e de grande relevância para a tecnologia da informação. Garantir confidencialidade, integridade e autenticidade de informações é uma questão que traz grande preocupação para os usuários de sistemas informatizados, especialmente para aqueles que fazem uso da internet e que trocam mensagens cuja interceptação e divulgação indevida poderiam comprometer seriamente pessoas e organizações.

Basicamente há duas formas de proteger informação: a primeira delas, conhecida como *criptografia* [2], oferece meios de *ocultar o significado* de uma mensagem, de modo que este se torne inacessível a pessoas externas à comunicação; a segunda, conhecida como *esteganografia* [3], oferece meios de *ocultar a presença* de uma mensagem, de modo que esta passe despercebida por pessoas externas à comunicação.

Embora estas formas de proteção possam parecer alternativas mutuamente exclusivas, na verdade, é perfeitamente possível combiná-las. Neste caso, além de ocultarmos o significado da informação, ocultamos também a sua própria existência, o que, sem dúvida, confere um nível adicional de proteção à informação.

Apesar de sua grande importância, até recentemente, muito pouca ênfase tem sido dada às técnicas de esteganografia na área de tecnologia da informação. De fato, o uso de técnicas de criptografia tem sido predominante em sistemas informatizados e, por este motivo, é muito difícil encontrar na literatura especializada referências sobre o uso efetivo de esteganografia.

Visando divulgar os conceitos da esteganografia, neste artigo, apresentamos uma visão geral das técnicas esteganográficas e propomos uma forma de classificá-los, em função de suas características específicas e similaridades. A partir desta classificação, usamos conceitos fundamentais de segurança da informação para evidenciar os pontos fortes e fracos de cada uma das classes. Além disto, usando o conceito de esteganografia em camadas, discutimos como o uso simultâneo de diversas técnicas de esteganografia pode fortalecer a segurança da informação.

O restante deste artigo está organizado do seguinte modo: na Seção 2, introduzimos os fundamentos da criptologia; na Seção 3, descrevemos as principais técnicas esteganográficas; na Seção 4, apresentamos a classificação proposta neste trabalho; e, finalmente, na Seção 5, apresentamos nossas conclusões.

2. Fundamentos da Criptologia

A *criptologia* é uma área de conhecimento que estuda formas de proteger informação contida em mensagens que são transmitidas num processo de comunicação. A criptologia engloba tanto a criptografia quanto a esteganografia, como vemos na estrutura apresentada na Figura 1.

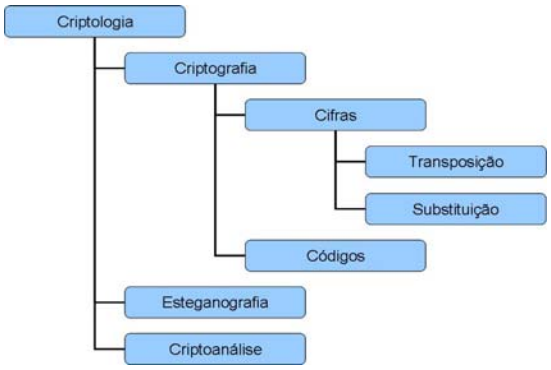

Figura 1 – Estrutura da Criptologia

A *criptografia* tenta proteger a informação contida numa mensagem ocultando seu significado. Para tanto ela utiliza códigos e cifras. Basicamente, um código consiste na substituição de uma palavra por uma outra palavra, enquanto a cifra age num nível mais baixo, substituindo símbolos por outros símbolos. As cifras podem ser de dois tipos: substituição ou transposição. Na cifra de transposição, os símbolos na mensagem são simplesmente rearranjados, gerando, efetivamente um anagrama. Na Figura 2, temos um exemplo que ilustra o

funcionamento básico da criptografia. Neste exemplo, cada bit da mensagem original é substituído pelo seu complemento. Note que a existência da mensagem não é ocultada, mas apenas o seu significado.

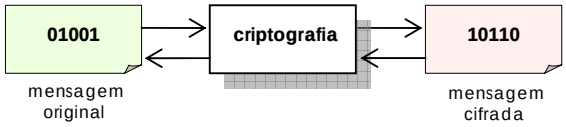

Figura 2 – Processo de criptografia.

Diferentemente da criptografia, a *esteganografia* não se preocupa em ocultar o significado de uma mensagem, mas sim em ocultar a sua existência. Para isto ela utiliza uma mensagem portadora, dentro da qual ela esconde a mensagem confidencial. O objetivo é alterar a mensagem portadora de tal forma que o resultado seja imperceptível. Na Figura 3, temos um exemplo que ilustra o funcionamento da esteganografia. Neste exemplo, os bits da mensagem original são escondidos entre as palavras da mensagem portadora. Cada bit 0 é codificado como um espaço e cada bit 1 é codificado como dois espaços. Na Figura 3, para maior clareza, estes espaços são representados na mensagem esteganografada como pontos. Observe como a presença da mensagem original fica, de fato, praticamente imperceptível na mensagem esteganografada.

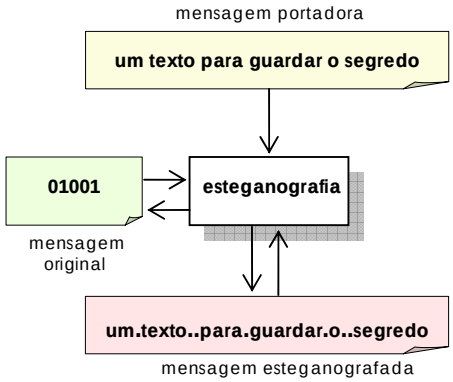

Figura 3 – Processo de esteganografia.

Evidentemente, poderíamos ainda combinar os dois processos e tirar proveito das duas formas de proteção de informação. Para isto, bastaria criptografar a mensagem original e, em seguida, esteganografar a mensagem cifrada obtida.

3. Técnicas Esteganográficas

Atualmente, a maioria dos algoritmos esteganográficos [4] funciona conforme esquematizado na Figura 4. Estes algoritmos recebem como entrada uma *chave*, um *recipiente* e uma *mensagem* confidencial e, como saída, devolvem um *objeto esteganográfico*, também denominado *stego-objeto*. A chave, também denominada *stego-key*, é uma senha usada para garantir uma maior proteção da informação, permitindo que esta só seja recuperada após o fornecimento da mesma senha. O recipiente, ou *objeto portador*, é o meio em que a mensagem confidencial é escondida. Após a esteganografia, a informação escondida no objeto portador é denominada *dado embutido*.

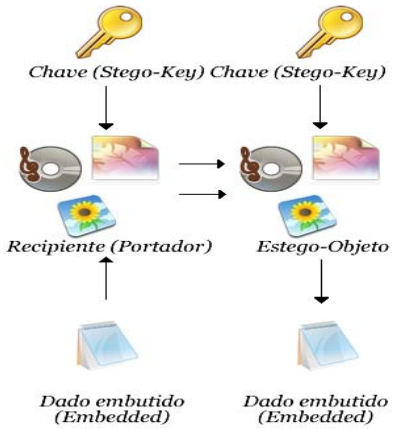

Figura 4 – Processo de esteganografia digital.

A seguir descrevemos as principais idéias da história [5] que deram origem a técnicas e algoritmos esteganográficos conhecidos atualmente.

3.1 Tintas invisíveis

Em 1641 o bispo John Wilkins publicou anonimamente o livro *The Secret and Swift Messenger*[1], em que ele sugeria a utilização de suco de cebola, alúmem, sal de amônia e um suco destilado de "bioluminescência", extraído de alguns tipos de insetos, para criar uma tinta que brilhasse apenas no escuro [3].

Atualmente, há diversas técnicas inspiradas nesta idéia, como as tintas invisíveis que se tornam visíveis apenas quando submetidas a calor ou luz ultravioleta.

3.2 Lugares escondidos

Durante a guerra franco-prussiana, ocorrida durante os anos de 1870 e 1871, Paris esteve completamente cercada e todas as suas comunicações regulares com o resto da França estavam cortadas. Toda essa eficiência do cerco prussiano era devida à movimentação de suas tropas, que se moveram para Paris seis semanas antes do início do confronto. Desesperados com o cerco, os parisienses tentaram uma opção inusitada para a época: transmitir mensagens escondidas em pombos. Em 27 de setembro de 1870, o primeiro pombo conseguiu sair de Paris com uma mensagem e, em 1º de Outubro do mesmo ano, ele retornou. Apesar de diversos pombos nunca terem voltado, o método funcionou muito bem durante o conflito, em que mais de 95.000 mensagens foram entregues através de suas viagens [3].

[1] O Mensageiro Secreto e Rápido.

3.3 Técnicas digitais

Marca d'água é um sinal inserido dentro de um arquivo digital (que pode conter áudio, imagens, vídeo ou texto) que pode ter sua presença detectada posteriormente para garantir a origem (ou autenticidade) de um arquivo ou documento [6].

A noção de robustez contra ataques é aplicada tanto na esteganografia quanto nas marcas d'água. Mesmo se a presença da mensagem secreta for conhecida, deverá ser muito difícil para alguém mal intencionado destruir a marca d'água sem conhecer a chave que deve usada para sua remoção [7].

Uma marca d'água robusta será, portanto, difícil de ser retirada ou removida sem comprometer drasticamente o conteúdo que pretende se preservar [3]. A Figura 5 mostra um exemplo de marca d'água.

Figura 5 – Exemplo de marca d'água.

3.4 Códigos abertos

A *Grelha de Cardano*, inventada por Girolamo Cardano (1501-1576), consiste numa folha de material rígido na qual existem aberturas retangulares da altura de uma linha de texto e de comprimento variável, colocadas em intervalos irregulares [8]. Esta grelha é projetada levando-se em conta uma outra folha, de iguais dimensões, que contém um texto portador. Quando a grelha é posicionada da maneira correta sobre a folha com o texto portador, a mensagem original é revelada. A Figura 6 exemplifica o uso da grelha.

T	C	O	A	E
C	R	D	R	J
E	E	G	N	S
H	T	B	B	E
G	O	A	U	N
Y	Z	A	O	G
I	R	F	A	F
L	P	I	X	A

T	C			
C		D		
E	E			S
	T			E
G		A		N
			O	G
	R		A	F
		I		A

Figura 6 – Exemplo de esteganografia com grelha.

3.5 Semagramas

A palavra *semagrama* vem do grego, onde *sema* significa sinal e *grama* significa escrito ou desenhado. Em outras palavras, semagramas são signos ou símbolos usados para esconder informação [9].

Os semagramas podem ser visuais ou textuais. Um exemplo de semagrama visual é o uso das posições dos ponteiros de um relógio para codificar informações. Um exemplo de semagrama textual é o uso de espaçamento extra entre as palavras de uma mensagem para codificar informações (Figura 3) [10].

4. Classificação da Esteganografia

Nesta seção, primeiramente apresentamos uma classificação de técnicas esteganográficas existente na literatura da área. Em seguida, propomos uma nova classificação destas técnicas e, com base nesta nova classificação, usamos os conceitos fundamentais de segurança de dados para evidenciar os pontos fracos e fortes de cada uma delas, em função da proteção que elas oferecem à informação. Com isto esperamos fornecer subsídios para a escolha de técnicas, ou combinações de técnicas, que ofereçam maiores garantias de proteção à informação.

4.1 A Classificação existente

Uma classificação existente na literatura, proposta por Bauer [11] e revisada por Arnold et al. [12], divide esteganografia em duas classes: *técnica* e *lingüística*.

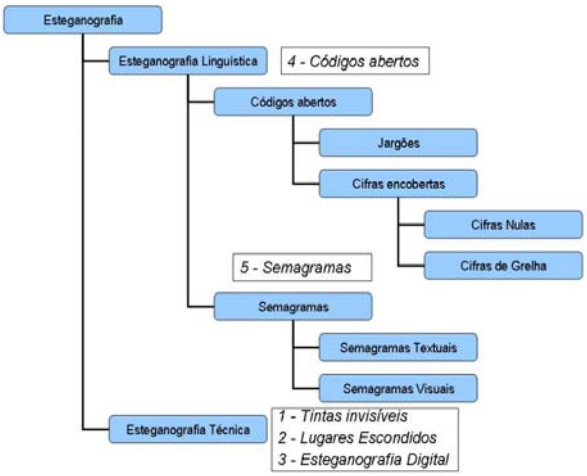

Figura 7 – Classificação de esteganografia existente.

A esteganografia técnica envolve o uso de meios técnicos para ocultar a existência da informação. O foco das técnicas nesta classe é manipular diretamente o objeto portador da mensagem e não a mensagem em si.

A esteganografia lingüística, por outro lado, envolve de uma linguagem como ferramenta para esconder o segredo [3]. O foco das técnicas nesta classe é manipular diretamente a mensagem que será encoberta antes de ser enviada.

Na Figura 7, podemos ver a classificação proposta por Bauer [11] e revisada por Arnold et al. [12]. Nesta classificação, adicionamos as caixas brancas a fim de indicar onde as ideias e técnicas apresentadas na Seção 3 podem ser inseridas.

Uma crítica feita a esta classificação é que seu foco não está no nível de proteção oferecido pelas técnicas esteganográficas, mas somente o fato de elas manipularem o objeto portador ou a mensagem confidencial.

4.2 Critérios de segurança da informação

Segurança da informação é área que tem como objetivo proteger informações contra as várias ameaças às quais elas estão expostas, a fim de garantir a continuidade do negócio, minimizar seu risco e maximizar seu retorno e oportunidades de negócio [13].

A segurança da informação possui vários critérios necessários para que uma informação possa ser considerada segura. Entre estes, destacaremos os três indicados a seguir:

- *Confidencialidade*: é a garantia de que uma informação só será acessível às pessoas autorizadas. Tanto a criptografia quanto a esteganografia oferecem meios de aumentar a confidencialidade de uma informação.
- *Integridade*: é a garantia de que uma informação não sofreu nenhum tipo de manipulação ou alteração que possa ter comprometido sua veracidade.
- *Autenticidade*: é a garantia de que uma informação é, de fato, originária da procedência alegada. Tanto a criptografia quanto a esteganografia podem ser usadas para garantir a autenticidade de uma informação.

Além destes critérios de segurança da informação, adotamos outros quatro critérios para a classificação de esteganografia proposta neste artigo:

- *Capacidade*: indica a quantidade de informação que pode ser escondida no objeto portador.
- *Perceptividade*: indica a capacidade de ocultação de informação da técnica esteganográfica, ou seja, quão imperceptível é a alteração feita no objeto portador para que a informação confidencial seja nele embutida.
- *Complexidade*: indica o grau de dificuldade de uso da técnica esteganográfica.
- *Informatizável*: indica se a técnica pode ser empregada em ambiente computacional.

4.3 A classificação proposta

Nesta seção, propomos uma classificação diferente daquela proposta por Bauer & Arnold et al. Usando esta nova classificação, juntamente com os critérios de segurança da informação descritos na seção anterior, podemos apontar mais facilmente os pontos fortes e fracos de cada técnica esteganográfica. Com isto esperamos oferecer subsídio para a escolha da técnica, ou combinação de técnicas, mais apropriada em cada situação, a fim de aumentar a segurança da informação.

A classificação proposta é resumidamente apresentada na Tabelas I. Embora esta classificação pareça, à primeira vista, similar àquela proposta por Bauer & Arnold, ressaltamos que nesta nova classificação as técnicas são agrupadas em função de suas similaridades e não em função do fato de elas modificarem ou não a mensagem confidencial ou o objeto portador.

Tabela I – Classes de técnicas esteganográficas.

Classe	Técnicas e Algoritmos
Tintas invisíveis	- Bioliminescência de Wilkins - Ovo de Givani Porta
Lugares escondidos	- Tabuletas de Demarato - Mensageiro de Histaeu - Bolo de lua chinês - Maria, Rainha da Escócia - Micropontos
Técnicas digitais	- Bit menos significativo - marcas d'água
Códigos abertos	- Cifra de Ave Maria - Cifra de Bacon - Código de jargões - Acrósticos - Grelhas de Cardano - Disco de Enéas
Semagramas	- Tapetes da Guerra Civil - Código náutico - Anamorfose

Uma síntese das propriedades de cada uma destas classes, ressaltando seus pontos fortes e fracos à luz dos critérios estabelecidos na Seção 4.2, é apresentada nas Tabelas II a VI. Esperamos que esta síntese possibilite o uso mais consciente das técnicas e algoritmos esteganográficos disponíveis. Por exemplo, podemos usar os dados nestas tabelas para escolher duas ou mais técnicas a serem combinadas, de modo que a capacidade do objeto portador seja aumentada e a integridade da informação escondida seja fortalecida.

Tabela II – Propriedades da classe tintas invisíveis.

Tintas Invisíveis			
Critérios/Nível	Baixa	Média	Alta
Confidencialidade		✓	
Integridade		✓	
Autenticidade	✓		
Capacidade	✓		
Perceptividade		✓	
Complexidade	✓		
Informatizável	não		

As propriedades da classe *tintas invisíveis* são apresentadas na Tabela II. As técnicas desta classe garantem confidencialidade e integridade médias; pois, apesar de ocultarem a informação, podem despertar suspeitas. A autenticidade é baixa, já que assinaturas podem ser adulteradas. Apresentam baixa capacidade, pois a ocultação de mensagens longas requer muito espaço físico. A perceptividade é média, pois os componentes da tinta

podem ter odores que revelem a existência da mensagem oculta. Também apresentam baixa complexidade, uma vez que atualmente existem disponíveis diversos mecanismos para escrita invisível. E, finalmente, não são informatizáveis, já que necessitam de meios físicos.

Tabela III – Propriedades da classe lugares escondidos.

Lugares Escondidos			
Critérios/Nível	**Baixa**	**Média**	**Alta**
Confidencialidade		✓	
Integridade			✓
Autenticidade	✓		
Capacidade			✓
Perceptividade		✓	
Complexidade		✓	
Informatizável	não		

As propriedades da classe *lugares escondidos* são apresentadas na Tabela III. As técnicas desta classe garantem uma confidencialidade média; pois, apesar de ocultarem a informação, caso o objeto portador seja interceptado, seu conteúdo pode ser revelado. A integridade, em geral, é alta, mas depende da durabilidade do objeto portador. A autenticidade, no entanto, é baixa, já que a informação oculta, se detectada, pode ser substituída por outra. Apresentam alta capacidade, pois grande quantidade de informação pode ser transmitida de forma escondida. A perceptividade e a complexidade são médias e dependem também do objeto portador escolhido. A informatização não é possível.

Tabela IV – Propriedades de classe técnicas digitais.

Esteganografia Digital			
Critérios/Nível	**Baixa**	**Média**	**Alta**
Confidencialidade			✓
Integridade			✓
Autenticidade			✓
Capacidade			✓
Perceptividade	✓		
Complexidade			✓
Informatizável	sim		

As propriedades da classe *técnicas digitais* são apresentadas na Tabela IV. As técnicas desta classe usam recentes tecnologias digitais e, desta forma, conseguem garantir confidencialidade, integridade e capacidade bastante altas. A complexidade também é alta, pois sua utilização exige grande conhecimento de métodos computacionais. A perceptividade, porém, é muito baixa.

Tabela V – Propriedades da classe códigos abertos.

Códigos Abertos			
Critérios/Nível	**Baixa**	**Média**	**Alta**
Confidencialidade			✓
Integridade		✓	
Autenticidade	✓		
Capacidade	✓		
Perceptividade		✓	
Complexidade		✓	
Informatizável	sim		

As propriedades da classe *códigos abertos* são apresentadas na Tabela V. As técnicas desta classe garantem alta confidencialidade, embora integridade seja média; pois ocultam a informação confidencial na mesma camada de visão da mensagem portadora. A autenticidade e a capacidade são, em geral, baixas. A perceptividade e a complexidade são médias; pois embora sejam relativamente fáceis de serem usados, há códigos abertos que apresentam padrões visíveis na mensagem portadora como, por exemplo, acrósticos. A informatização destas técnicas também é, em geral, muito simples.

Tabela VI – Propriedades da classe semagramas.

Semagramas			
Critérios/Nível	**Baixa**	**Média**	**Alta**
Confidencialidade			✓
Integridade		✓	
Autenticidade		✓	
Capacidade	✓		
Perceptividade			✓
Complexidade	✓		
Informatizável	sim		

As propriedades da classe *semagramas* são apresentadas na Tabela VI. As técnicas desta classe garantem alta confidencialidade, uma vez que empregam códigos para ocultar a informação. A integridade e a autenticidade são médias; pois, estes códigos podem ser substituídos indevidamente sem que isto seja detectado. A perceptividade é alta, pois os símbolos que carregam a informação oculta não são ocultos. A complexidade é baixa, pois requer apenas um código específico seja previamente combinado. A informatização é simples.

Tabela VII – Exemplo de combinação de técnicas.

Tintas Invisíveis / Códigos Abertos			
Critérios/Nível	**Baixa**	**Média**	**Alta**
Confidencialidade			✓
Integridade		✓	
Autenticidade	✓		
Capacidade	✓		
Perceptividade		✓	
Complexidade		✓	
Informatizável	não		

Na Tabela VII, apresentamos um exemplo de como a combinação de duas ou mais técnicas podem aumentar a segurança conferida à informação esteganografada. Neste exemplo, consideramos a combinação de *tintas invisíveis* e *códigos abertos*. Esta combinação permite a transmissão de uma mensagem confidencial com alguns de seus caracteres escondidos por tinta invisível e outros visíveis a olho nu, porém codificados. A confidencialidade garantida pelo método é alta e a integridade, apesar de média, é satisfatória; pois a existência de duas camadas de esteganografia dificulta a adulteração completa da mensagem. Quanto à capacidade e à perceptividade, esta fusão não fortalece o processo esteganográfico.

5. Conclusões

Neste artigo, apresentamos as principais ideias que surgiram ao longo da história e que deram origem a técnicas e algoritmos esteganográficos bem conhecidos na atualidade.

Em seguida, propusemos uma forma de classificar as técnicas esteganográficas, em função de suas similaridades. Então, partindo desta classificação, empregamos critérios atuais da segurança da informação para analisar as propriedades destas classes e evidenciar seus pontos fortes e fracos. Como resultado desta análise, sintetizamos tabelas de propriedades para cada classe.

Com isto esperamos oferecer subsídio para a escolha da técnica, ou combinação de técnicas, mais apropriada em cada situação, a fim de aumentar a segurança da informação.

Agradecimentos

Ao CNPq, pela bolsa de produtividade em pesquisa concedida a um dos autores deste artigo, conforme o processo de número 304322/2009-1.

Referências Bibliográficas

[1] M. C. P. Peixoto, **Engenharia Social e Segurança da Informação na Gestão Corporativa**, Brasport, 2006.

[2] B. Schneier, **Applied Cryptography**, Willey, 1996.

[3] G. Kipper, **Investigator's Guide to Steganography**, Auerbach Publications, 2004.

[4] J. G. R. Júnior e E. S. Amorim, **Esteganografia: integridade, confidencialidade e autenticidade**. São Bernardo do Campo, 2008.

[5] D. Kahn, **The Codebreakers – The Story of Secret Writing**. New York, New York, U.S.A. 1967.

[6] T. Mesquita Neto, T. **Uma aplicação de técnicas de ocultação de dados para armazenamento e recuperação de informações em arquivos multimídia**, Unioeste, Paraná, 2007.

[7] F. A. P. Petitcolas e S. Katzenbeisser, **Information Hiding Techniques for Steganography and Digital Watermarking**, Artech House, 2000.

[8] V. Tkotz. **A Grelha de Cardano (e de Richelieu).** http://www.numaboa.com/criptografia/esteganografia/163-grelha-de-cardano, acesso em 25 out. 2009.

[9] V. Tkotz. **Criptografia - Semagrama**. http://www.numaboa.com/glossarios/cripto, acesso em 25 out. 2009.

[10] G. C. Kessler. **An Overview of Steganography for the Computer Forensics Examiner**. http://www.fbi.gov/hq/lab/fsc/backissu/july2004/research/2004_03_research01.htm, acesso em 03 jun. 2009.

[11] F. L. Bauer, **Decrypted Secrets: Methods and Maxims of Cryptology**, 3rd edition, Springer-Verlag, New York, 2002.

[12] M. Arnold, M. Schmucker and S. D. Wolthusen, **Techniques and Applications of Digital Watermarking and Content Protection**. Artech House, Norwood, Massachusetts, 2003.

[13] **ABNT NBR ISO/IEC 27002:2005 - Código de Prática para a Gestão da Segurança da Informação**, 2005.