PONTIFÍCIA UNIVERSIDADE CATÓLICA DO RIO GRANDE DO SUL
FACULDADE DE INFORMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

UTILIZAÇÃO DE ESTEGANOGRAFIA PARA AMPLIAR CONFIDENCIALIDADE EM SISTEMAS RFID

RAFAEL MEZZARI

Dissertação apresentada como requisito parcial à obtenção do grau de Mestre em Ciência da Computação na Pontifícia Universidade Católica do Rio Grande do Sul.

Orientador: Fabiano Passuelo Hessel

Porto Alegre
2012

M617u Mezzari, Rafael
Utilização de esteganografia para ampliar a confiabilidade em sistemas RFID / Rafael Mezzari. – Porto Alegre, 2012.
93 f.

Diss. (Mestrado) – Fac. de Informática, PUCRS.
Orientador: Prof. Dr. Fabiano Passuelo Hessel.

1. Informática. 2. RFID. 3. Sistemas Automáticos de Identificação. 4. Segurança – Computação. I. Hessel, Fabiano Passuelo. II. Título.

CDD 006.31

Ficha Catalográfica elaborada pelo
Setor de Tratamento da Informação da BC-PUCRS

Pontifícia Universidade Católica do Rio Grande do Sul
FACULDADE DE INFORMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

TERMO DE APRESENTAÇÃO DE DISSERTAÇÃO DE MESTRADO

Dissertação intitulada "***intitulada "Utilização de Esteganografia para Ampliar Confidencialidade em Sistemas RFID"***, apresentada por Rafael Mezzari, como parte dos requisitos para obtenção do grau de Mestre em Ciência da Computação, Sistemas Embarcados e Sistemas Digitais, aprovada em 23/01/2012 pela Comissão Examinadora:

Prof. Dr. Fabiano Passuelo Hessel– Orientador — PPGCC/PUCRS

Prof. Dr. César Augusto Missio Marcon - — PPGCC/PUCRS

Prof. Dr. Rubem Dutra Ribeiro Fagundes - — PPGEE/PUCRS

Homologada em..11.../09.../2012., conforme Ata No. ...20..... pela Comissão Coordenadora.

Prof. Dr. Paulo Henrique Lemelle Fernandes
Coordenador.

PUCRS
Campus Central
Av. Ipiranga, 6681 – P32– sala 507 – CEP: 90619-900
Fone: (51) 3320-3611 – Fax (51) 3320-3621
E-mail: ppgcc@pucrs.br
www.pucrs.br/facin/pos

"A mente que se abre a uma nova idéia jamais voltará ao seu tamanho original." - Albert Einstein

AGRADECIMENTOS

Primeiramente agradeço ao meu orientador, Professor Fabiano Passuelo Hessel, pela confiança, ensinamentos, incentivo e paciência.

Agradeço à Carmela, minha filha nascida durante o mestrado, e à meu filho Martin, concebido durante o mesmo, por toda alegria que trouxeram em minha vida.

À Mariana, minha amada esposa, por todo o suporte e apoio que recebi.

À meu Pai, meu Irmão, minha Mãe e demais familiares por tudo o que já fizeram por mim.

Aos demais Professores e colegas por tudo o que me ensinaram.

UTILIZAÇÃO DE ESTEGANOGRAFIA PARA AMPLIAR CONFIDENCIALIDADE EM SISTEMAS RFID

RESUMO

Esteganografia pode ser descrita como a ciência que estuda as formas de ocultar uma mensagem dentro de uma comunicação, escondendo sua existência. Atualmente, a segurança da informação e de dados é um tema amplamente discutido e de grande relevância para a tecnologia da informação. Questões como a confidencialidade e autenticidade de uma mensagem, assim como a privacidade de uma comunicação, são fatores que trazem preocupação para o cada vez crescente número de usuários de sistemas que trocam muitas mensagens, sejam pessoais ou comerciais. Ao mesmo tempo, sistemas RFID estão se tornando cada vez mais comuns, e isso gera o desafio de implementar segurança em tais sistemas RFID. Uma forma comum de tornar seguras as informações contidas nas etiquetas (tags) RFID é o uso de métodos de criptografia. Porém, informações visivelmente criptografadas atraem suspeitas e curiosidade. Desta forma, torna-se pertinente aumentar a confidencialidade das informações contidas em sistemas RFID sem atrair atenção indesejada, utilizando-se de técnicas de esteganografia para tal fim. Da mesma forma, faz-se necessário avançar a pesquisa em métodos que ampliem a segurança de sistemas sem haver alteração da máquina de estados padrão de sistemas RFID, visando evitar gastos e incompatibilidades em relação aos padrões usados no mercado. Assim, este trabalho tem como objetivo efetuar um estudo da utilização de técnicas de esteganografia para ampliar a confiabilidade de informações contidas em sistemas RFID sem atrair atenção indesejada e sem alterar a máquina de estados padrão.

Palavras-Chave: Esteganografia; Segurança da Informação; RFID.

USING STEGANOGRAPHY TO IMPROVE CONFIDENTIALITY IN RFID SYSTEMS

ABSTRACT

Steganography can be defined as the science that studies ways to hide a message within a communication, hiding its existence. Currently, information security and data security are topics widely discussed and highly relevant to information technology. Issues such as confidentiality and authenticity of a message, as well as privacy of communication are factors that bring concern for the increasingly growing number of users of systems who exchange many messages, whether for personal or commercial purposes.

At the same time, RFID systems are becoming more and more widespread, and that raises the challenge to implement security in RFID systems. One common way to secure the information available on the RFID tags is to use cryptography methods. But visibly encrypted information arouses suspicions and curiosity.

Due to this fact, it is desired to increase the confidentiality of the information that belong to a RFID system without attracting unwanted attention, using steganography techniques to this end. At the same time, it is necessary to advance the research in methods that increase security while at the same time avoiding incompatibilities related to the industry standards.

In order to achieve this, the present work describes a study regarding the use of steganography techniques in order to increase the confidentiality of the information stored in a RFID system without attracting unwanted attention and without changing the standard machine state

Keywords: RFID, Steganography, security, confidentiality.

Lista de Figuras

Figura. 1: Relação entre Comunicação encoberta, Esteganografia, Marca d'água e Ocultação de informações.....18
Figura 2: Classificação da técnica.....25
Figura 3: Esteganografia Digital com inserção de material secreto.....29
Figura 4: Ilustração de Esteganografia em vídeo.....31
Figura 5: Processo comum de compressão de dados no padrão MPEG....32
Figura 6. Uma arquitetura RFID típica.....43
Figura 7. Software de leitura/Escrita de tags utilizado.....70
Figura 8. Informação Oculta com o Método 3.....71
Figura 9. Informação Oculta com o Método 5.....72
Figura 10 - Geração do Padrão Secreto.....78
Figura 11 - Algoritmo de Embutimento do Padrão Secreto.....81
Figura 12 - Algoritmo de Extração do Padrão Secreto.....82

Lista de Tabelas

Tabela 1: Comparação entre criptografia e esteganografia.....38
Tabela 2: Comparação de métodos referentes a sua aderência ao padrão EPC Class I Gen 2.....57
Tabela 3: Comparação de características que afetam a robusteza de diferentes métodos.....58
Tabela 4: abordagens ao anonimato.....59
Tabela 5: abordagens à Autenticidade.....59
Tabela 6. Campos de uma etiqueta RFID Class 1 Gen 2.....62
Tabela 7. Números de série alterados para conter uma informação oculta..64
Tabela 8. Diferentes Códigos de Produtos.....67
Tabela 9. Métodos de Codificação.....69
Tabela 10 – Amostra de Números de Série de RFID.....76

SUMÁRIO

1. INTRODUÇÃO À ESTEGANOGRAFIA E RFID 12
1.1 Objetivos e Originalidade. 13
1.2 Organização do texto. 13
2 – ESTEGANOGRAFIA E HISTÓRIA DA TÉCNICA 15
2.1 Introdução à esteganálise 23
2.2 Técnicas de Esteganografia 25
2.3 – Aplicações de Esteganografia 29
2.4 – Marca d'água 33
2.5 – Método de Análise Esteganográfica – Esteganálise 36
2.6 – Criptografia X Esteganografia 37
3 – RFID - RADIO FREQUENCY IDENTIFICATION 40
3.1 – História e descrição do sistema 40
3.1.1 A Antena de RFID 40
3.1.2 O Transceiver e Leitor 41
3.1.3 O Transponder, etiqueta ou RF Tag 41
3.2 - A Técnica 44
3.3 – Aplicações RFID 46
3.3.1 Aplicações Médicas 47
3.3.2 - Linha de Montagem Industrial 47
3.3.3 - Transportes Aéreos, Terrestres e Marítimos 47
3.3.4 – Logística 48
3.3.5 - Aplicações Financeiras 49
3.3.6 - Aplicações para Bibliotecas 49
3.4 – Privacidade em aplicações RFID 49
3.4.1 - Ameaças à Privacidade 50
3.4.1.1 - Microchip no Dinheiro 51
3.4.1.2 - Microchip em Documentos 52
3.5 – Vantagens 52
3.6 – Desafios e desvantagens de sistemas RFID 53

4 – TRABALHOS CORRELATOS E DESCRIÇÃO FORMAL DO PROBLEMA. 56

4.1 - Descrição Formal do Problema e idéia básica da solução..... 60

5 – ESQUEMAS PROPOSTOS PARA A OCULTAÇÃO ESTEGANOGRÁFICA DE DADOS. 66

5.1 – Método 1 – Ocultação de informações em uma única etiqueta RFID 66

5.1.1. - Requisitos para a Solução OcEDados..... 67

5.1.2 - Lógica de Projeto para a Solução OcEDados..... 68

5.1.3 – Fundamento teórico do esquema OcEDados 68

5.2 - Método 2 - Recuperação e Restauração de Dados RFID Indevidamente Manipulados usando Princípios Esteganográficos... 72

5.2.1 – Esquema proposto para a recuperação de Dados - RecDados 74

5.2.2 - Visão Geral da Solução RecDados..... 74

5.2.3 - Requisitos para a Solução RecDados..... 76

5.2.4. - Lógica de Projeto para a Solução RecDados 77

5.2.5 – Fundamento Teórico do sistema RecDados..... 78

5.2.5.1 - Geração do Padrão Secreto..... 78

5.2.5.2. Seleção da Localização do Embutimento 79

5.2.5.3. Embutimento do Padrão Secreto..... 80

5.2.5.4 - Extração do Padrão Secreto para a Recuperação de Dados 82

5.3 Discussão e validação 83

6. CONCLUSÃO E TRABALHOS FUTUROS..... 85

REFERÊNCIAS 87

1. INTRODUÇÃO À ESTEGANOGRAFIA E RFID

A esteganografia é um método antigo, utilizado para inserir informações escondidas em meios não convencionais, de maneira que tais informações passem despercebidas para terceiros. Vários foram os episódios em que pessoas realizaram tentativas de ocultar informações em outros meios.

Durante milhares de anos, comandantes dependeram de comunicações eficientes para governar seus países e nações. Ao mesmo tempo, todos eram conhecedores das consequências de suas mensagens caírem nas mãos de terceiros, expondo segredos preciosos a nações rivais ou divulgando informações vitais para as forças inimigas [1]. Diversas vezes no decorrer da história, mensagens ocultas foram interceptadas, mas não foram descobertas graças à técnica de esteganografia, que tem auxiliado na ocultação de uma mensagem há vários séculos [2].

Seu principio é que esses dados não sejam percebidos por outras pessoas; ou seja, a presença de conteúdo escondido dentro de arquivos é simplesmente desconhecida [3]. Somente o receptor da mensagem tem conhecimento de sua existência, assim como da maneira como expô-las.

Essa técnica possui inúmeras aplicações, porém possui algumas limitações. Por exemplo, o tamanho das informações a serem escondidas é limitado pelo tamanho do próprio meio que será utilizado. Quanto menos essas informações degradarem a estética dos arquivos, maior é o potencial das técnicas esteganográficas. Em linhas gerais, as mensagens muito grandes acabam ferindo a aparência do meio, o que colabora para uma fácil detecção de que uma possível mensagem foi escondida no arquivo.

A difusão da tecnologia RFID surgiu em função da necessidade de captura mais eficiente das informações de produtos que estivessem em movimento, melhorando os processos produtivos. Juntou-se a isso a necessidade do uso em ambientes insalubres e em processos que

impediam o uso de código de barras, e temos como resultado a criação e o uso de sistemas RFID. A tecnologia facilita o controle do fluxo de produtos por toda a cadeia de suprimentos de uma empresa, permitindo o seu rastreamento desde a sua fabricação até o ponto final da distribuição [4]. A tecnologia RFID foi inicialmente desenvolvida para gerenciar e localizar itens em sistemas de logística, mas atualmente é utilizada nas mais diversas áreas, como manufatura, varejo, criação de animais, medicina, transporte e segurança [69].

1.1 Objetivos e Originalidade.

O Objetivo do presente trabalho é realizar um estudo da aplicação de esteganografia em etiquetas RFID, unindo as duas tecnologias e utilizando a esteganografia como método para melhorar a segurança do sistema RFID, impedindo ou dificultando o acesso de terceiros as informações dentro do sistema e possibilitando a recuperação de dados manipulados em alguns casos. O objetivo específico é desenvolver um método esteganográfico para codificação de dados em etiquetas RFID e um método para recuperação destas informações. A originalidade deste trabalho é usar a esteganografia como técnica para aumentar a confidencialidade e confiabilidade de sistemas RFID.

1.2 Organização do texto.

Esta Dissertac□ão é composta de 8 capítulos, sendo o primeiro esta introduc□ão. O restante está está estruturado da seguinte forma: No Capítulo 2 é abordada a técnica de esteganografia, seu uso histórico e diferentes modalidades de aplicação da técnica. No Capítulo 3 há uma explanac□ão sobre RFID e seus componentes, sendo também abordadas as diferentes características de ambientes RFID. No Capítulo 4 são listados

os trabalhos correlatos e é iniciada a descrição do problema proposto. No capítulo 5 são descritos os dois métodos propostos de uso da esteganografia e da tecnologia RFID abordado neste trabalho, incluindo o projeto e execuc□ão dos experimentos realizados em tal cenário. Finalmente, no Capítulo 6 é apresentada a conclusão e os trabalhos futuros que podem vir a ser realizados.

2 – ESTEGANOGRAFIA E HISTÓRIA DA TÉCNICA

O termo esteganografia se refere à arte das comunicações encobertas[1]. Esteganografia também é definida como sendo a arte e ciência de ocultação de dados [29] ou também é conhecida como o termo que refere-se aos métodos de escrever e enviar informações ocultas em outras informações, de forma que ninguém, exceto o remetente e o destinatário, suspeitem da existência da mensagem. O termo foi cunhado por Johannes Trithemius, autor que escreveu o primeiro tratado conhecido sobre o assunto, Steganographia, que foi publicado em 1606. A idade Antiga abrange o período entre a invenção da escrita, atribuída aos sumérios, por volta de 3500 a.C. e o ano de 476 d.C.. Durante essa época, as principais civilizações que se desenvolveram foram as localizadas na Mesopotâmia, região Egípcia, Persa e Romana. Porém o primeiro registro do uso da Esteganografia se dá a mais de 3000 anos do início da idade antiga [3].

Aos gregos são creditados os primeiros registros históricos do uso da esteganografia, documentados durante a época de conflito entre a Grécia e a Pérsia, durante o século V a.C. por Heródoto.

Um dos mais antigos exemplos de esteganografia data de em torno de 440 AC na História Grega. Heródoto, um historiador grego do século V AC, revelou alguns exemplos de seu uso em sua obra intitulada "As Histórias de Heródoto". Um exemplo sugere que Histeu, governador de Mileto, tatuou uma mensagem secreta na cabeça raspada de um de seus escravos de máxima confiança. Após crescido o cabelo, o escravo foi mandado a Aristágoras onde lhe rasparam a cabeça de novo e a mensagem de comando de revolta contra os persas foi revelada[6]. Neste exemplo o escravo foi usado como portador da mensagem secreta, e ninguém que o visse teria notado que ele portava uma mensagem. Em

virtude disso, a mensagem chegou ao receptor sem jamais levantar suspeitas.

Na China antiga, mensagens eram escritas sobre seda fina e o pequeno retalho era recoberto por cera. Para transportar a mensagem oculta, um mensageiro era obrigado a engolir a bolinha, ir até o destinatário e entregá-la após expeli-la. [7].

A técnica também foi bastante utilizada nas Guerras mundiais, principalmente na comunicação, espiões alemães na Primeira Grande Guerra colocavam pequenos pontos de tinta invisível sobre letras de revistas e jornais de grande circulação [8,9]. As folhas de revistas quando eram aquecidas, revelavam a seqüência das letras [10].

Já na Segunda Grande Guerra, outra maneira que começou a ser empregada na esteganografia foram os micropontos, devido ao fato do aumento da qualidade das câmeras, lentes e filmes. Utilizando deste método, uma mensagem poderia ser fotografada e reduzida ao tamanho de um ponto, podendo este ser um ponto final de sentença ou o ponto de uma letra de outra mensagem qualquer [6]. Após o conflito em Pearl Harbor, diversos meios suspeitos de conterem mensagens esteganografadas foram criteriosamente analisados nos Estados Unidos. Jogos de xadrez enviados por cartas, palavras cruzadas eram examinados ou removidos das correspondências, assim como papéis em branco enviados pelo correio eram testados com a suspeita de tintas invisíveis e fotos eram também examinadas minuciosamente.

Todas as mensagens em outras línguas foram proibidas, bem como textos que não fossem claros. Qualquer menção a espécies de flores ou listas de natal das crianças também foram analisadas com o objetivo de impedir que qualquer informação que comprometesse a segurança nacional fosse passada de forma esteganográfica com o auxílio do correio nacional [2].

Outro exemplo simples, básico e real do uso de esteganografia de texto nos é dado pelo caso do espião nazista que enviava por correio

mensagens aparentemente inócuas, tais como "Apparently neutral's protest is thoroughly discounted and ignored. Isman hard hit. Blockade issue affects pretext for embargo on by-products, ejecting suets and vegetable oils". Ao utilizar apenas a segunda letra de cada palavra, a mensagem oculta aparece: "Pershing sails from NY June 1". [30]

A implementação da esteganografia possibilita que uma pessoa envie uma mensagem secreta para outra de modo tal que ninguém mais saberá que esta mensagem existe. Tipicamente, a mensagem está embutida dentro de outro objeto conhecido como "cover Work", pelo entrelaçamento de suas propriedades. O resultado, conhecido como estegograma, tem uma engenharia tal que se torna um modelo perceptual quase idêntico ao cover Work (cobertura), mas que também contém a mensagem escondida. É o estegograma que a fonte da informação envia para o destino. Se alguém interceptar a comunicação irá obter o estegograma, mas como este é absolutamente semelhante à cobertura fica difícil determinar o risco que ele apresenta. Portanto, o papel da esteganografia é assegurar que o adversário enxergue o estegograma – e assim, a comunicação – como sendo inócua.

Em termos modernos, a esteganografia costuma ser implementada de modo computacional, onde os "cover Works", tais como os arquivos de texto, imagem, áudio e vídeo são entremeados permitindo que sejam utilizados para codificar mensagens secretas.

As técnicas são muito semelhantes ao das marcas d'água digitais, contudo uma grande diferença deve ser salientada entre elas. Nas marcas d'água digitais o foco está em garantir que ninguém possa remover ou alterar o conteúdo dos dados marcados, ainda que sua existência seja flagrante. A esteganografia, por outro lado, procura tornar extremamente difícil afirmar que sequer existe uma mensagem secreta. Quando terceiros não autorizados conseguem determinar, com segurança, que um arquivo contém uma mensagem secreta, é porque a esteganografia fracassou.

Neste trabalho, será utilizado "Cover Work" ou "Cover Imagem", ou simplesmente "cover" (cobertura) para indicar as imagens que ainda não contêm uma mensagem secreta, e "stego Work", ou "stego imagens", ou "stego object" para indicar uma imagem que contém uma mensagem secreta embutida. Além disso, para a mensagem secreta será utilizado o termo "stego-mensagem" ou mensagem escondida.

Dependendo do significado e o objetivo dos metadados embutidos é possível definir vários campos de informações escondidas, ainda que na literatura o termo 'informações hiding' seja frequentemente usado como sinônimo de esteganografia. Nas marcas d'água digitais, por exemplo, as informações são usadas para a prevenção de cópias, controle de cópias, e proteção de direitos autorais. Neste caso, os dados embutidos devem ser robustos contra ataques maliciosos para preservar seu objetivo.

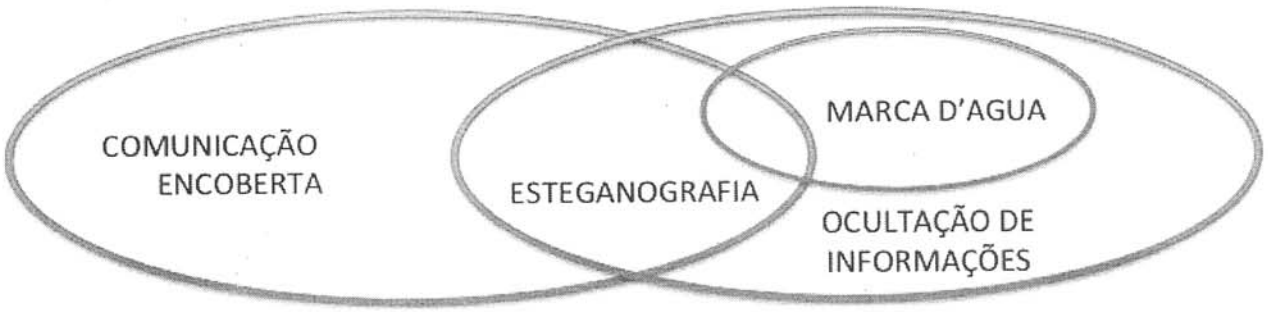

Figura. 1: Relação entre Comunicação encoberta, Esteganografia, Marca d'água e Ocultação de informações. [1]

A diferença chave entre a esteganografia e a marca d'água é a ausência (na esteganografia) de um adversário ativo porque geralmente não há valor associado ao ato de remover informações escondidas no conteúdo do hospedeiro. Entretanto, a esteganografia pode precisar ser robusta contra distorções comuns ou acidentais como as compressões ou o ajuste de cores (neste caso denominada de esteganografia ativa).

Por outro lado, a esteganografia visa se comunicar de uma forma completamente indetectável que não necesite ser solicitada em marca d'água. Por este motivo considera-se a esteganografia também como parte da ciência da comunicação de cobertura. A figura 1 mostra de forma gráfica as conexões entre a esteganografia e os campos relacionados. A intersecção entre a esteganografia e as marcas d'água compreendem a esteganografia ativa e alguns tipos de marca d'água para aplicações de autenticação.

Da perspectiva da Teoria da Informação podemos introduzir a esteganografia através da adoção de um ponto de vista levemente diferente [57]. Shannon [58] foi o primeiro a considerar os sistemas secretos do ponto de vista da teoria da informação. Shannon identificou tipos de comunicações secretas as quais descreveu como: sistemas de esconderijo, incluindo métodos como o link invisível, o esconderijo de uma mensagem em um texto inocente, ou num criptograma de cobertura falso, ou outros métodos nos quais a existência da mensagem é escondida do inimigo.

Depois disso, o conceito de esteganografia foi recuperado por Simmons [59] em sua famosa explicação da esteganografia descrita por meio do problema dos prisioneiros. Hoje em dia a esteganografia também é vista como um modo de assegurar liberdade de expressão em países sob ditadura militar ou ligada a segurança nacional. A esteganografia também é supostamente usada pelos terroristas para planejar ataques. Um exemplo é o manual técnico do jihad [60].

A partir de outro ponto de vista se sabe que há algumas transmissões proibidas [62] e se deseja saber quem está enviando as informações secretas, por exemplo, para a imprensa. Aparentemente, durante os anos 80, a Primeira Ministra Britânica Margaret Thatcher ficou tão irritada com os vazamentos para a imprensa de documentos do gabinete que solicitou que seus processadores de texto fossem programados para codificar a identidade das secretárias nos espaços entre

palavras dos documentos de forma que se pudesse rastrear os ministros desleais. Mais tarde, a esteganografia passou a ser usada por algumas da impressoras HP e Xerox, as quais embutiam pequenos pontos amarelos durante a impressão, escrevendo uma mensagem codificada na qual constava o número da impressora e o horário da impressão. Esta segurança foi inicialmente forçada pelo Governo Federal Americano junto aos fabricantes de impressoras porque as notas de dólar eram forjadas com facilidade por estas impressoras (uma das cotações mais baixas naquela época).

Durante os últimos anos a pesquisa em esteganografia de imagens ganhou um crescente interesse. Uma variedade de técnicas foram propostas especificamente a formatos de arquivos de imagem como gif, jpeg ou imagens representadas no domínio pixel. De fato, a idéia principal por trás da indetectabilidade da esteganografia era: menos mudanças a serem embutidas no "cover Work" significa um "stego object" menos detectável. Outras técnicas [46,44], especialmente no domínio JPEG usam um subconjunto de suporte para tentar ajustar as estatísticas de imagens modificadas pela incorporação da mensagem.

O objetivo duplo da esteganografia é pertinente à steganálise cujo objetivo é descobrir a presença de canais secretos de comunicação (mensagems secretas) estabelecidas pela esteganografia. Para cada método esteganográfico foram propostas várias técnicas [42, 26, 24, 19, 18].

Diferentes métodos de esteganografia possuem diferentes pontos fortes e fracos. As características que tornam um método mais ou menos atraente são[29]:

1. Capacidade de carga: Refere-se à quantidade de informação que pode ser ocultada em um determinada *cover,* comparado ao tamanho do próprio *cover*. Uma grande capacidade permite o transporte de mais dados, mas torna mais fácil a detecção. Por

outro lado, uma pequena capacidade de carga normalmente se traduz em uma maior facilidade para ocultar a informação de forma a dificultar a detecção da mesma. Esta capacidade é medida em *bit-per-bit (bpb)*, e a reduzida capacidade de carga de uma tag RFID comum torna bastante desafiadora a tarefa de ocultar informações em uma etiqueta.

2. Invisibilidade: Para ocultar dados em um cover é necessário alterá-lo. Invisibilidade refere-se à medida de alteração que é feita no cover. Uma grande capacidade de carga é inútil se causa muita alteração, tornando-se facilmente detectável. Invisibilidade é uma característica subjetiva, e a melhor forma de medi-la é apresentar a diversos observadores o cover antes e depois de receber a informação oculta. Se ninguém perceber a diferença, o algoritmo é considerado de grande invisibilidade.

Ao desenvolver um sistema esteganográfico é importante considerar qual seria o "cover Work" mais apropriado, e também determinar como o estegograma vai alcançar seu receptor. Com a funcionalidade oferecida pela internet há muitos diferentes modos de mandar mensagens a pessoas sem que ninguém saiba que elas existem. Por exemplo, é possível que um estegograma de imagem seja mandado ao receptor por email.

Alternativamente pode ser postado em um fórum da web para que todos vejam, o receptor se logando no fórum e recuperando a imagem para ler a mensagem. Aparentemente, mesmo que qualquer um possa ver o estegograma, não há motivos para crer que se trate de mais do que uma simples mensagem.

Em termos de desenvolvimento a esteganografia compreende dois algoritmos, um para incorporação e um para extração. O processo de incorporação se ocupa de esconder uma mensagem secreta no interior de um "cover Work", sendo o processo mais cuidadosamente construído dos dois.

Presta-se grande atenção para garantir que uma mensagem secreta passe despercebida caso terceiros interceptem o "cover Work". O processo de extração é tradicionalmente um processo muito mais simples, já que trata simplesmente do processo inverso da incorporação, no qual a mensagem secreta é revelada no final.

A próxima etapa é passar os dados de entrada através do codificador do estegosistema cuja meticulosa engenharia embute a mensagem numa cópia exata do cover Work para evitar distorções mínimas; quanto menor a distorção, tanto melhores a chances de indetectabilidade. O codificador do estegosistema geralmente exige uma chave para operar, a qual também será utilizada na fase de extração. Esta é uma medida de segurança destinada a proteger a mensagem secreta. Sem uma chave seria possível a alguém extrair corretamente a mensagem, basta obter os algoritmos de incorporação e extração. Entretanto, usando uma chave, é possível randomisar a operação do codificador do estegosistema, e a mesma chave precisará ser usada para extrair a mensagem de modo que o decodificador do estegosistema saiba qual processo utilizar. Isso significa que se o algorítmo cair nas mãos do inimigo é extremamente improvável que ele consiga extrair a mensagem com sucesso.

Os dados de saída do codificador do estegosistema é o estegograma que deve ser o mais parecido possível ao cover Work, exceto pelo fato de conter a mensagem secreta. Este estegograma é, então, enviado aos canais de comunicação juntamente com a chave utilizada para embutir a mensagem. Ambos o estegograma e a chave são então alimentados para o decodificador do estegosistema onde uma estimativa da mensagem secreta é extraída. Note que o resultado do processo de extração é somente uma estimativa já que estegograma está sujeito a ruídos que alteram alguns dos valores quando enviado ao canal de comunicações. Portanto, nunca teremos certeza de que a mensagem extraída é uma representação exata do original. Da mesma forma, o receptor nunca saberá qual era a mensagem original, não tendo nada ao que comparar com o que extraiu.

Este é provavelmente o sistema mais comum de esteganografia atualmente, com especial foco no cuidadoso desenvolvimento do codificador do estegosistema. Para obter sucesso, é da máxima importância que na esteganografia o estegograma não contenha pistas de incorporação de uma mensagem secreta.

2.1 Introdução à esteganálise

A esteganálise é a arte de identificar estegogramas que contêm uma mensagem secreta. Porém, a esteganálise não considera a extração bem sucedida da mensagem, isso é normalmente uma exigência da criptanálise.

Nos anos recentes, muitos algorítmos esteganográficos foram disponibilizados ao público sendo, portanto, muito fácil para qualquer um com ainda que um conhecimento limitado de esteganografia conseguir se comunicar de forma encoberta. A maioria dos sistemas utiliza imagens do dia-a-dia como base para seus modelos e, logicamente, as informações escondidas dentro das imagens podem variar de coisas inofensivas para mensagens que representam uma ameaça à segurança nacional. Além disso, há uma crescente preocupação com a forma pela qual podemos identificar esteganografia contida numa mensagem, de modo a assegurar que a tecnologia não está sendo utilizada para os propósitos errados. Esta contra- atividade é denominada de esteganálise, e muitas pesquisas e recursos têm sido empregados na determinação de mensagens inocentes ou não.

Tipicamente, a esteganálise começa identificando a presença de artefatos existentes num arquivo suspeito devido à incorporação de uma mensagem. Nenhum dos sistemas esteganográficos conhecidos hoje em dia obtêm a segurança perfeita[8], e isto significa que todas deixam pistas da incorporação no estegograma. Isso fornece ao esteganalista uma forma útil de identificar se uma mensagem secreta existe ou não.

A esteganálise é uma ciência extremamente difícil, pois se baseia numa esteganografia insegura. Conforme foi discutido na seção 2, esteganografia bem sucedida não deixa indícios da existência de uma mensagem secreta. Portanto, se o modelo tiver sido criado com sucesso, ele deve tornar difícil a tarefa a qualquer Terceira parte de identificar que ocorreu uma intromissão.

Jessica Fridrich [61] sugere que "a capacidade de detectar uma mensagem secreta em imagens se relaciona ao comprimento da mensagem". Esta afirmação se baseia na lógica de que uma pequena mensagem embutida num portador grande resulta numa baixa porcentagem de manipulações sendo, portanto, muito mais difícil localizar artefatos no interior do estegograma.

É claro, o sucesso da esteganálise também depende das informações que o esteganalista utiliza para começar seu trabalho. Há duas principais classificações de esteganografia – objetiva e cega. A esteganálise objetiva funciona quando um método destinado a identificar se um algoritmo esteganográfico específico foi desenvolvido [56]. Por exemplo, embutir em valores de pixel deixa padrões que podem ser revistados na busca de arquivos suspeitos. Se o esteganalista tiver certeza de que estão ocorrendo comunicações encobertas e se conhecer um possível método de embutir uma mensagem secreta, então deve ser uma tarefa trivial sumarizar para ver se o arquivo contém ou não este tipo de esteganografia. A esteganálise Cega, por outro lado, é uma tarefa bem mais difícil, pois significa que o esteganalista não tem motivos para acreditar que estejam ocorrendo comunicações encobertas. Este conjunto de algoritmos é tipicamente desenvolvido para procurar sinais de intromissão. Caso sinais de intromissão forem detectados pelos algoritmos, então provavelmente o arquivo suspeito contém esteganografia.

2.2 Técnicas de Esteganografia

Há basicamente dois tipos de esteganografia, a lingüística e técnica, [13, 14] que foram alinhadas em uma classificação hierárquica visualizada na Figura 2.

Esteganografia Técnica: envolve o uso de metodos técnicos para esconder a existência de uma mensagem. Ela pode ser por meios químicos ou físicos. Algumas técnicas de esteganografia lingüística também estão nessa categorização [15]. A Esteganografia Técnica (Technical steganography) utiliza métodos científicos para ocultar uma mensagem, como o uso de tinta "invisível", micro pontos ou outras formas de redução de tamanho.

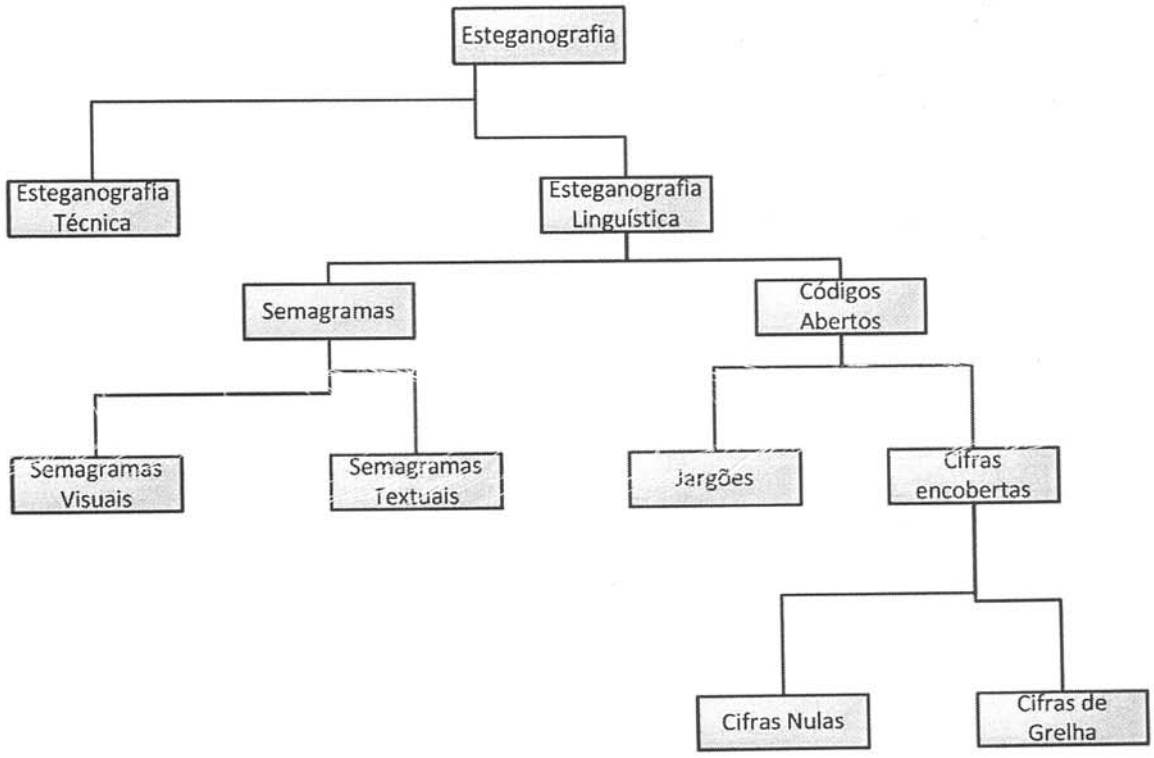

Figura 2: Classificação da técnica.

Esteganografia Linguística *(Linguistic steganography)* oculta uma mensagem em outra através do uso de formas não-óbvias e é posteriormente categorizada entre Códigos Abertos ou Semagramas. Semagramas ocultam informação através do uso de símbolos ou sinais. Semagrama vem do Grego, onde sema significa sinal e grama significa escrito ou desenhado. O semagrama é um tipo especial de esteganografia que faz uso de objetos pouco usuais para transmitir informações. Como exemplo de semagrama visual, em um carregamento de relógios é possível que a posição dos relógios e seus ponteiros possam representar algum tipo de informação. Um semagrama de texto oculta a informação modificando a própria aparência do texto, como mudanças sutis no tamanho ou tipo da fonte, adição de espaços extras ou sinais particulares em determinados caracteres.

Códigos abertos (*Open codes*) ocultam a mensagem em formas que não são visíveis a um observador desinformado. Esta categoria é dividida em Códigos de Jargão (*jargon codes*) e Cifragem Oculta (*covered cipher*).

Códigos de Jargão, como o nome indica, usa linguagem que é compreendida apenas por um grupo de pessoas e é desprovida de sentido para as outras. Exemplos de Códigos de Jargão são o uso de palavras com significado especial para quem recebe a mensagem e o uso de certas frases pré-arranjadas para distribuir uma mensagem.

Cifragem Oculta é usada para ocultar uma mensagem de forma aberta, visando a fácil recuperação por quem conheça a forma secreta de ocultação. Como exemplos de cifragem oculta temos o uso de regras como "leia a cada cinco palavras" ou "observe a terceira letra de cada palavra".

Também é possível classificar técnicas de esteganografia de acordo com suas características de indetectabilidade e robustez, a saber:

1. Indetectabilidade: Um observador pode detectar a presença de informação oculta computando certas propriedades estatísticas do

arquivo e comparando o resultado com o que é normalmente esperado para aquele tipo de arquivo. Portanto, um bom algoritmo esteganográfico não deve alterar as propriedades estatísticas do *cover*. Indetectabilidade diferencia-se de Invisibilidade por não depender da percepção do observador. O algoritmo usado para obter a imagem da Figura 3 é de grande invisibilidade, mas também é de baixa Indetectabilidade.

2. Robustez: Refere-se à capacidade do algoritmo de reter a informação oculta mesmo após mudanças no *cover* tais como compressão e descompressão ou certos tipos de processamento tais como conversão analógica/digital e vice versa.

Esteganografia Digital: para que a mensagem seja protegida, é necessária uma chave esteganográfica que é secreta e protege os dados de invasores ou de qualquer pessoa que não está autorizada a acessar o conteúdo original da mensagem, podendo ser um número qualquer dedicado a inserir e extrair a mensagem do objeto portador, sendo basicamente uma chave simétrica.

Há três maneiras de esconder uma mensagem digital em uma mensagem:

1) Geração: O objeto portador é gerado somente para esconder a mensagem secreta, podendo ser um arquivo qualquer, sem nenhuma informação relevante.

2) Injeção: Os dados a serem escondidos são diretamente injetados no objeto portadora mensagem oculta, o que normalmente aumenta o tamanho da mensagem.

3) Substituição: Os dados a serem escondidos substituem parte dos dados existentes no objeto portador. Isto impede que o tamanho do objeto portador aumente significativamente, mas pode acarretar em perda da qualidade do mesmo.

Na esteganografia existe um esquema básico de montagem do objeto estegano-gráfico (*stego-object*), que é composto por um objeto portador (*cover-object*) e uma chave esteganográfica (*stego-key*) [7]. O objeto portador da mensagem pode ser qualquer tipo de dado que possa ser manipulado pelo computador, como uma imagem ou um arquivo de som.

As técnicas de esteganografia podem ser classificadas de acordo com seu tipo e quanto à necessidade da marca [17]:

- Robustos: aqueles em que mesmo após o experimento da remoção a marca permanece ilesa.
- Frágeis: são os sistemas em que qualquer tentativa de modificação na mídia resulta na perda da marcação.

Aplicações que precisam da permanência da marca para fins de verificação de autenticidade, como watermarks e fingerprints, são consideradas robustas. Como exemplo de técnicas frágeis, cita-se a verificação de copias ilegítimas, em que se um usuário pode editar o conteúdo original.

Já quanto à percepção da marca, as técnicas podem ser classificadas da seguinte forma, conforme o autor:

- Marcação Imperceptível: sistema onde a marca encontra-se no objeto ou material, porem não é aparente.
- Marcação Visível: nesse sistema a marca do autor deve ficar visível, comprovando a autoria visualmente.

A esteganografia provê meios de inserir informações ocultas dentro de mídias, sejam elas discretas ou continuas [2]. Essa inserção de informações ocultas esta relacionada ao conceito de chaves que visam dificultar o alcance de seu conteúdo por pessoas não autorizadas.

O objeto de mídia utilizado para inserção de material oculto recebe o nome de Objeto de Cobertura. O objeto contendo a mensagem confidencial recebe o nome de Estego Objeto. Por exemplo, se for inserida uma mensagem texto em um documento texto, este recebera o nome de Estego Texto. Se for inserido um texto no interior de uma imagem, esta recebera a alcunha de Estego Imagem. No exemplo da figura 3 temos uma ilustração de uma Estego Imagem. No arquivo JPG desta image, está embutida de forma oculta o título da presente dissertação com a senha "rfid".

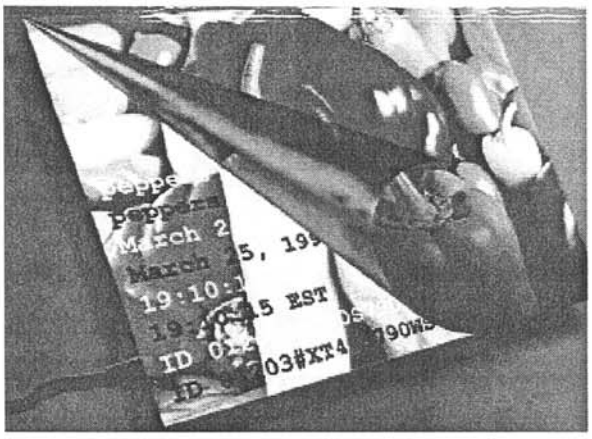

Figura 3: Esteganografia Digital com inserção de material secreto.

2.3 – Aplicações de Esteganografia

Um autor de um documento, por exemplo, pode incluir mensagens escondidas de direitos autorais de modo que quando forem expostas, demonstrem que a propriedade intelectual do documento lhe pertence. Se outra pessoa possuir acesso ao documento e requisitar, o autor pode provar o contrário, já que só ele tem conhecimento de como readquirir a mensagem escondida. Este tipo de aplicação é conhecido como watermarking [30] ou marca d'água digital e será discutido em profundidade na Seção 2.5.

Ainda segundo o autor [30], as agências militares e de

inteligência precisam de meios discretos para trocar informações, principalmente em áreas de conflito. A transmissão de conteúdo criptografado não é eficaz neste quesito. Por este motivo, técnicas de esteganografia são muito usadas em comunicações militares, como a modulação por espalhamento de espectro, dificultando a detecção da transmissão pelo inimigo.

Para movimentações financeiras via Internet, devido à necessidade de um rigoroso nível de segurança, também é comum o uso da esteganografia como uma tecnologia de suporte no processo de comunicação. O mesmo é válido para esquemas de eleições, em que o uso de técnicas para comunicação é um fator importante para garantir a integridade da votação [31].

É possível citar também aplicações ilegais para a esteganografia, como registros ocultos de atividades fraudulentas ou de dados que tenham a ver com espionagem industrial. Além de esconder dados sigilosos, criminosos também podem se comunicar usando métodos esteganográficos, para que suas mensagens dificilmente sejam detectadas ou interceptadas [32].

Para a utilização da técnica em vídeos digitais, é necessário o manuseio dessas imagens que estão no vídeo, conforme é descrito na Figura 4. Para essa tarefa, utiliza-se o fato da visão humana não ter a competência de perceber pequenas mudanças nas imagens causadas pela introdução de bits relativos à mensagem que se pretende ocultar. Basicamente, para inserir essa técnica em vídeos digitais, se necessita seguir 3 passos principais:

1. Transformação do vídeo em imagens, quadro a quadro.
2. Escolha da informação a ser ocultada e determinação dos quadros que receberão os dados a serem escondidos.
3. Ocultação da informação via LSU e empacotamento das imagens em formato de vídeo.

Para empacotar as imagens em formato de vídeo, a compressão do vídeo pode ser dividida em três estágios (Figura 5): Estimativa de Movimento, Codificação por DCT e Quantização. A Estimativa de Movimento é responsável por reduzir as redundâncias temporais dos quadros do vídeo. Já a Codificação por DCT e Quantização é responsável por eliminar as redundâncias espaciais.

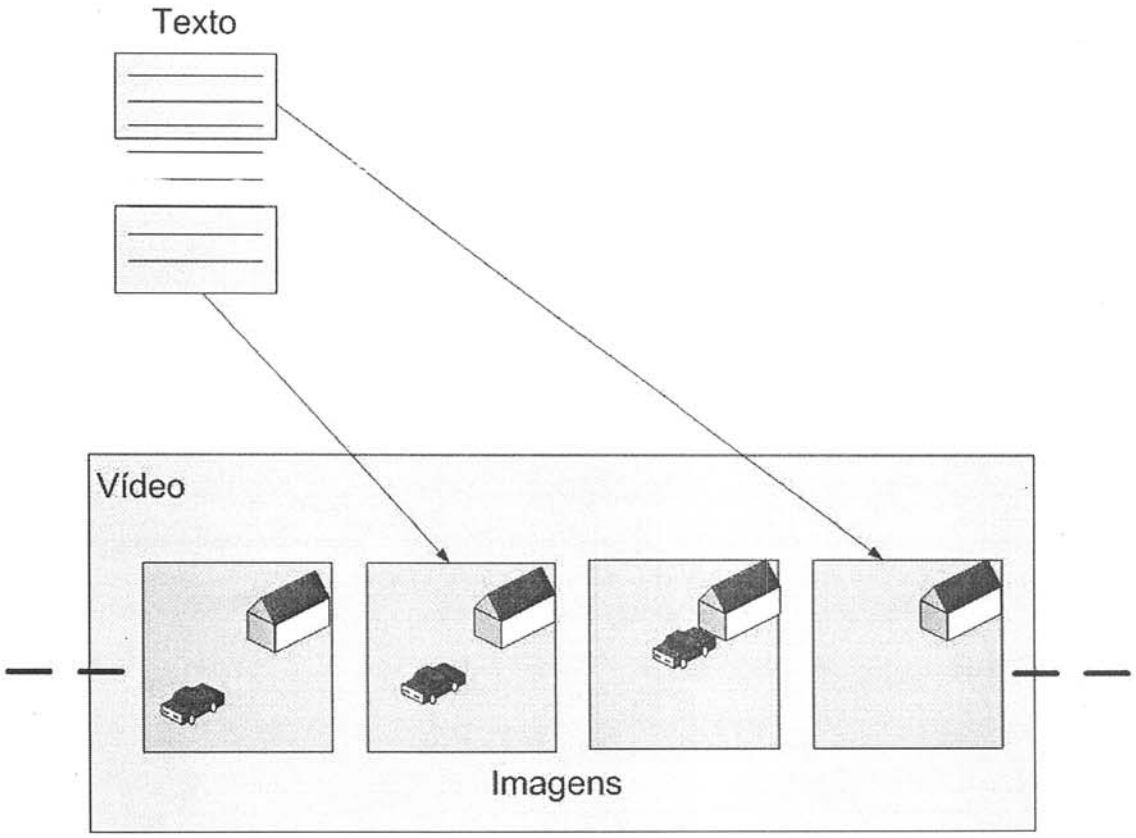

Figura 4: Ilustração de Esteganografia em vídeo.

Na codificação de diversas imagens de um vídeo percebe-se um alto nível de informação visual redundante entre quadros consecutivos de uma cena. Os modelos de redundância temporal exploram as similaridades entre os quadros vizinhos, sejam eles anteriores ou posteriores, visando a eliminação destas informações redundantes. Basicamente procura-se as informações repetidas presentes em quadros próximos para codificar apenas um desses quadros e eliminar a codificação da informação nos

demais diminuindo a quantidade de informação a ser codificada no bitstream final [35].

Independentemente da abordagem escolhida, deve se considerar requisitos para o vídeo final: tem que ser passível de recuperação de informações inseridas quando utilizado um player especifico, ou seja, deve haver uma aplicação cliente capaz de retirar as informações inseridas via esteganografia do interior do vídeo. Também deve poder ser reproduzido em player comum sem alteração visual perceptível ao usuário, garantindo o sigilo da técnica.

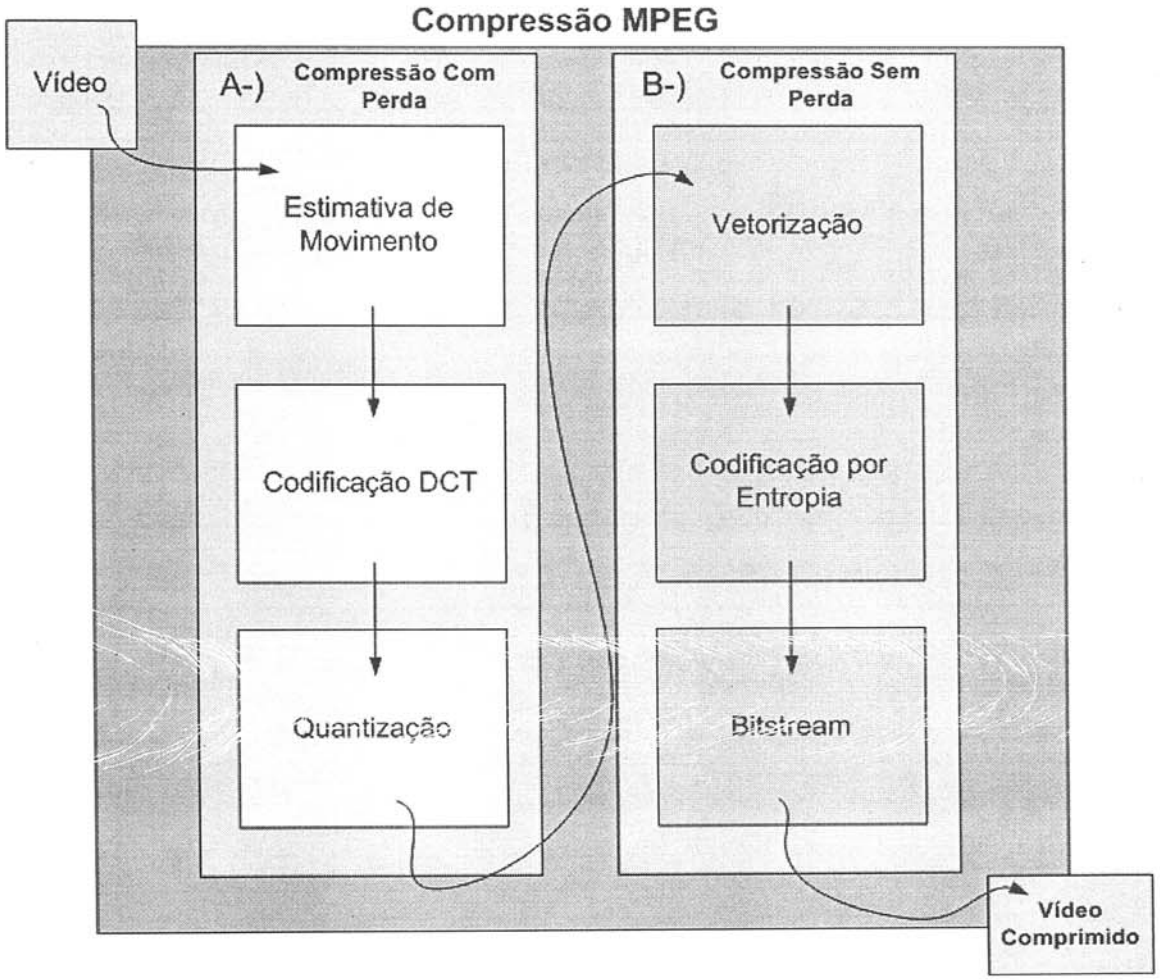

Figura 5: Processo comum de compressão de dados no padrão MPEG.

2.4 – Marca d'água

Uma marca d'água é um sinal carregador de informação, embutido no dado digital que pode ser extraído mais tarde para fazer alguma asserção sobre o dado hospedeiro. Um dos usos mais comuns de esteganografia é a criação de marcas d'água (watermarks), visando proteger direitos autorais ou servindo como uma "assinatura" do criador em sua obra [35]. As marcas d'água digitais são normalmente rotuladas em robustas e frágeis. As robustas são projetadas para resistirem à maioria dos procedimentos de manipulação de imagens, e geraimente, são usadas para atestar a propriedade da figura. As marcas frágeis são corrompidas com facilidade por qualquer processamento na imagem.

O grande crescimento dos sistemas de multimídia interligados pela rede de computadores nos últimos anos apresenta um enorme desafio nos aspectos propriedade, integridade e autenticação dos dados digitais. Para enfrentar tal desafio, o conceito de marca d'água digital foi definido. Uma marca d'água é um sinal portador de informação, visualmente imperceptível, embutido em uma imagem digital. A imagem que contém uma marca é dita imagem marcada ou hospedeira. Apesar de muitas técnicas de marca d'água poderem ser aplicadas diretamente para diferentes tipos de dados digitais, as mídias mais utilizadas são as imagens estáticas.

Existe alguma certa confusão entre as marcas d'água imperceptíveis e as visíveis utilizadas em cédulas de dinheiro, por exemplo. As visíveis são usadas em imagens e aparecem sobrepostas, sem prejudicar muito a sua percepção.

São usadas geralmente para expor imagens em locais públicos, como páginas na internet, sem o risco de alguém copiá-las e usá-las comercialmente, pois é difícil remover a modificação sem destruir a obra original. É possível também inserir digitalmente marcas visíveis em vídeo e até audíveis em música. As marcas d'água digitais são classificadas,

de acordo com a dificuldade em removê-las, em robustas, frágeis e semi-frágeis. Normalmente, esta classificação também determina a finalidade para a qual a marca será utilizada.

A informação embutida em uma imagem, por meio de uma marca robusta, poderia ser extraída mesmo que a imagem hospedeira sofresse rotação, mudança de escala, mudança de brilho/contraste, compactação com perdas com diferentes níveis de compressão, corte das bordas, etc. Uma boa marca d'água robusta deveria ser impossível de ser removida, a não ser que a qualidade da imagem resultante deteriore a ponto de destruir seu conteúdo visual. Por causa deste motivo, as marcas d'água robustas são normalmente utilizadas para a verificação da propriedade das imagens.

As marcas frágeis são facilmente adulteradas por qualquer processamento na imagem. Este tipo de marca d'água é útil para checar a integridade e a autenticidade da imagem, pois possibilita detectar alterações nesta. Em alguns casos, esta característica é indesejável. Por exemplo, ajustar brilho ou contraste para melhorar a qualidade da imagem pode ser um processamento válido, que não deveria ser detectado como uma tentativa de alteração de ma fé. Compactar uma imagem com perdas em diferentes níveis de compressão deveria ser uma operação permitida. Ainda, imprimir e escanear uma imagem não deveria levar à perda da autenticação.

Assim, foram criadas as marcas d'água semi-frágeis. Uma marca semi-frágil também serve para autenticar imagens. Diferentemente, estas procuram distinguir as alterações que modificam uma imagem substancialmente daquelas que não modificam o conteúdo visual da imagem. Uma marca semi-frágil extrai algumas características da imagem que continuam invariantes por meio das operações toleradas e as inclui de volta na imagem de forma que a alteração de uma dessas características possa ser detectada. Podem-se subdividir as marcas de autenticação em três subcategorias [41]: com chave secreta, com chave pública ou privada e sem chave. Com relação à extração da

marca d'água, têm-se três modos de sistemas. Cada um deles diferencia-se pela sua natureza ou combinação de entradas e saídas:

Marcas d'água privadas (também apontadas como não-cegas): esse sistema demanda a marca d'água original. Dentro desse esquema, existem dois tipos. No primeiro, é necessário o arquivo original para achar rastros de onde se encontra a marca dentro do arquivo marcado. O sistema do segundo tipo necessita das mesmas informações do anterior, mas somente tenta responder se o arquivo contém a marca d'água. Espera-se que este sistema seja mais robusto, já que transporta pouca informação e requer acesso a dados secretos;

Marcas d'água semi-cegas ou semi-privadas: não utiliza o arquivo original na extração. Exemplificando, poderia ser utilizado para provar a propriedade em corte ou em mecanismos de controle de cópia como em aparelhos de DVDs.

Marcas d'água cegas ou públicas: não requer nem o arquivo original nem a marca. A intenção do método é remover a marca do dado sem rastros de onde este está.

Entre os três tipos de marca de autenticação, a chave pública é a que proporciona mais recursos. Os possíveis usos de uma marca de autenticação de chave pública são enormes. Abaixo, cita-se três exemplos:

Câmera digital segura: Na câmera digital sugerida, a câmera fabrica dois arquivos de saída para cada imagem capturada. Na primeira, a própria imagem digital capturada pela câmera em algum formato. A segunda é uma assinatura digital produzida aplicando a chave privada da câmera. O usuário deve tomar cuidado para guardar os dois arquivos, para que se possa autenticar a imagem mais tarde. Uma vez que a imagem digital e a assinatura digital são originadas pela câmera e arquivadas no computador, a integridade e a autenticidade da imagem podem ser verificadas usando um programa para decodificar a assinatura digital, que pode ser distribuído livremente aos usuários. Esse

esquema [44] poderia ser melhorado de duas formas. A primeira seria embutir a assinatura digital no arquivo da imagem, acabando com a necessidade de armazenar dois arquivos para cada imagem. Alguns formatos de imagem permitem armazenar alguns dados adicionais no cabeçalho ou rodapé do arquivo.

A segunda seria permitir a localização da área distorcida. Isto poderia ser interessante, por exemplo, para descobrir a intenção do falsificador ao adulterar a imagem. A marca d'água de autenticação de chave pública pode ser usada para incorporar essas melhorias à câmera.

Marcas d'água também podem auxiliar a autenticação de imagens distribuídas pela rede: supõe-se que uma agência de notícias chamada Alice deseja distribuir pela internet um retrato jornalístico, com alguma amostra de autenticidade de que a foto foi distribuída pela Alice e que ninguém incluiu alterações maliciosas na imagem. Alice utiliza a sua chave privada para inserir marca d'água de autenticação na imagem e distribui a foto marcada. Supõe-se que Bob recebe a foto demarcada. Bob usaria a chave pública da Alice para verificar que a foto está assinada pela Alice e que ninguém inseriu qualquer alteração depois de Alice assiná-la. Se Mallory, um hacker malicioso, mudar a foto, ele não será capaz de inserir a marca correta na imagem falsificada porque ele não conhece a chave privada da Alice. Além disso, Mallory não poderá distribuir uma foto sua como sendo da Alice porque ele não obterá a assinatura, por não saber a chave privada da Alice.

2.5 – Método de Análise Esteganográfica – Esteganálise

A esteganalise é a arte de detectar mensagens ocultadas via esteganografia, pode ser comparada ao método de analise da criptografia. O objetivo da esteganálise é determinar a existência de uma mensagem, e após esta determinação, decifrar mensagens a partir de cifras e chaves empregadas no processo de criptografia. Ela atua de duas

formas, a primeira tem como objetivo identificar o aspecto de mensagens ocultas na mídia e a segunda tem o objetivo de extrair do material a mensagem esteganografada.

Atualmente, as pesquisas [28] estão mais reunidas em identificar a presença de mensagens escondidas ao invés de extraí-las. Recuperar os dados escondidos, está além da competência da maioria das técnicas de esteganalise.

2.6 – Criptografia X Esteganografia

A criptografia é uma ciência que, ao contrário da esteganografia, não se dedica a esconder a presença da mensagem secreta, mas tornar as mensagens ininteligíveis para pessoas externas à comunicação através de diversas transformações do texto original [45]. Diferentemente da Criptografia, que protege a informação transformando-a em um formato ininteligível, a esteganografia torna a informação invisível ao ocultá-la em outro conjunto de dados, sem despertar suspeitas sobre o conteúdo oculto.

Outra vantagem da Esteganografia sobre a Criptografia é que as informações a serem enviadas do remetente ao destinatário não atraem atenção indesejada, porque aparentemente toda a informação constante na mensagem está disponível a qualquer um que a observe. Já o uso de técnicas criptográficas acaba atraindo atenção indesejada porque é trivial perceber que a informação que está sendo enviada na mensagem está protegida por algum método de criptografia. O indivíduo que interceptou a mensagem percebe que a mesma está criptografada e tende a suspeitar que ali possam estar ocultas informações referentes a atos maliciosos e/ou ilegais. Na mesma situação, um arquivo com informações ocultas de forma esteganográfica tende a parecer inócuo e a não despertar suspeitas.

Pode-se diferenciar a esteganografia da criptografia nos aspectos relacionados na Tabela 1, que faz uma comparação entre diferentes características da Criptografia e da Esteganografia:

A esteganografia também difere da criptografia porque esta não tenta esconder o fato de que existe uma mensagem. Em vez disso, a criptografia meramente obscurece a integridade das informações de modo que somente façam sentido ao receptor. O adversário conseguirá ver que a mensagem existe, e o processo inverso de criptanálise devolve as informações sem sentido à sua forma original.

Neste sentido, é bem provável que um sistema esteganográfico completo possa empregar medidas criptográficas como uma rede de segurança para proteger o conteúdo da mensagem no caso de violação da esteganografia.

Tabela 1: Comparação entre criptografia e esteganografia

Esteganografia	**Criptografia**
Oculta outra mensagem em arquivos aparentemente inocentes, como imagens, sons, vídeos e outros arquivos	A mensagem é visível, mas por estar cifrada é ininteligível para o observador casual.
Resulta em arquivos, vídeos, imagens ou sons que não despertam suspeitas.	Resultam em arquivos evidentemente criptografados, o que gera curiosidade e atrai atenção indesejada.
Requer cuidado ao reutilizar o mesmo arquivo.	Requer cuidado ao reutilizar a mesma chave.
Não existem leis proibindo ou regulando esteganografia.	Em alguns países, existem leis regulando e até mesmo proibindo criptografia.

Embora a esteganografia também seja chamada de "a arte da comunicação invisível" [3], o termo invisível não está ligado ao sentido da comunicação, como na criptografia na qual o objetivo é proteger as comunicações de um bisbilhoteiro, mas refere-se a esconder a existência do próprio canal de comunicação. A idéia geral de se esconder mensagens em conteúdos digitais comuns interessa a uma classe mais ampla de aplicações que vão além da esteganografia.

3 – RFID - RADIO FREQUENCY IDENTIFICATION

3.1 – História e descrição do sistema

No fim da década de sessenta apareceram os primeiros sistemas que se aparentam com os sistemas de RFID atuais, como o *Electronic Article Surveillance* (EAS) [74], que continham um bit que indicava a presença ou ausência de um artigo. Porém, a afirmação do RFID como tecnologia madura veio nos anos oitenta, com uma difusão de aplicações aparecendo nos EUA, em áreas como controle de mercadorias, controle de acesso de pessoas, transporte e identificação animal [5].

Também nos anos oitenta, a aplicação RFID em UHF (Ultra High Frequency) veio junto com baterias, e podia-se decifrar entre dois e oito Kbytes. O custo de um transponder era alto, e eram utilizados em aplicações complexas ou com alto valor. Desse estudo, nasceu o Código Eletrônico de Produtos - EPC (*Electronic Product Code*). O EPC definiu uma arquitetura de identificação de produtos que utilizava os recursos vindos de radiofreqüência, chamada posteriormente de RFID.

A tecnologia RFID que conhecemos hoje veio nos anos 90 com a miniaturização dos componentes, reduzindo a energia que eles consomem, e com o desenvolvimento de padrões internacionais. Sistemas RFID basicamente consistem em três componentes [75]: Antena, Transceiver e um Transponder (normalmente chamado de RF Tag), conforme podemos ver na Figura 6.

3.1.1 A Antena de RFID

A antena emite um sinal de rádio ativando o RF Tag, atingindo a leitura ou escrevendo algo. Na verdade a antena servirá como o meio

capaz de fazer o RF Tag trocar ou enviar as informações ao leitor. As antenas são fabricadas em varias formas e tamanhos, possuindo configurações e características diferentes, cada uma para um tipo de aplicação. Quando a antena, o transceiver e o decodificador estão juntos, recebem o nome de "leitor" [70].

3.1.2 O Transceiver e Leitor

O leitor emite freqüências de rádio [75] que são disparadas em diversas direções no espaço, dependendo da saída e da freqüência de rádio utilizada. O leitor trabalha pela emissão de um campo eletromagnético utilizando a fonte que alimenta o Transponder, Por apresentar essa característica, o equipamento pode entender através de diversos materiais como papel, cimento, plástico, madeira, vidro, etc. Quando o Tag passa pela área de cobertura da antena, o campo magnético é detectado pelo leitor, que decodifica os dados codificados no Tag, passando-os para um computador realizar o processamento.

3.1.3 O Transponder, etiqueta ou RF Tag

O transponder [47] é um receptor-transmissor que envia um sinal de radio como resposta a um comando recebido de uma estação. Para alguns transponders ativos (capazes de iniciar uma comunicação) ou semi-ativos (incapazes de inicar transmissão, mas tem fonte de energia par aaumentar o alcance), é necessário determinar a transmissão do sinal de resposta, que contém ao menos o código único de identificação, enquanto que os transponders, o sinal de retorno pode ser transmitido continuamente devido à presença de uma bateria.

Tipicamente, etiquetas RFID são anexadas a um determinado item que desejamos identificar de forma automática. Um sistema RFID é composto de três componentes principais, conforme visto na Figura 6: [2,

3, 4] A etiqueta RFID (que contém as informações a serem utilizadas), o Leitor RFID (que se comunica de forma sem fio com as etiquetas para efetuar a leitura das mesmas) e o Middleware RFID (que leva a informações coletadas pelos leitores até os sistemas que as processarão). Cada tipo de aplicação requer um tipo específico de etiqueta.

O tipo mais simples de etiqueta RFID é o modelo Passivo, que não possui fonte de alimentação própria e que para funcionar necessita coletar através de sua antena energia que é transmitida na forma de radiofrequência por um leitor RFID. Tipicamente, o alcance de uma etiqueta passiva é de até quatro metros [22], embora existem padrões como o ISO 14443 que prevê o uso de PDAs com leitores cujo alcance de leitura não supere 10 centímetros. Normalmente, recursos computacionais são muito limitados em uma etiqueta passiva. Além do modelo Passivo, existe também o modelo Ativo, que é capaz de iniciar uma comunicação e é equipado com fonte de alimentação própria, normalmente uma bateria. Etiquetas RFID ativas possuem vantagens (maior alcance para leitura, maior capacidade de armazenamento, maior velocidade de leitura) mas também possuem desavantagens (preço mais alto, menor vida útil, a etiqueta é fisicamente maior, o funcionamento cessa quando acaba a bateria). Um terceiro tipo de etiqueta é a chamada semi-passiva, este tipo de tags têm um funcionamento muito semelhante ao das tags passivas, ainda não são capazes de iniciar comunicação e estão dependentes do sinal do leitor para comunicar, no entanto são fabricadas com uma bateria interna, esta tem como objetivo fornecer energia à tag para que ela possa se comunicar em uma distância mais expressiva. Etiquetas passivas são de utilização muito mais comum do que as etiquetas passivas devido ao custo inferior, e por sua abundância as etiquetas passivas serão o foco do presente estudo.

Devido à existência de fonte de alimentação, etiquetas ativas podem possuir módulos de hardware extras que permitam o uso de métodos de segurança mais refinados do que os disponíveis para etiquetas passivas. Porém, técnicas de segurança desenvolvidas para etiquetas passivas podem também ser utilizadas em etiquetas ativas [25]. Devido a isso e ao fato de que as etiquetas em uso no mercado são majoritariamente passivas, o presente estudo será focado em etiquetas passivas e no presente trabalho, o uso da palavra "etiqueta" refere-se à etiquetas passivas EPC Class 1 Gen 2, exceto onde especificamente indicado.

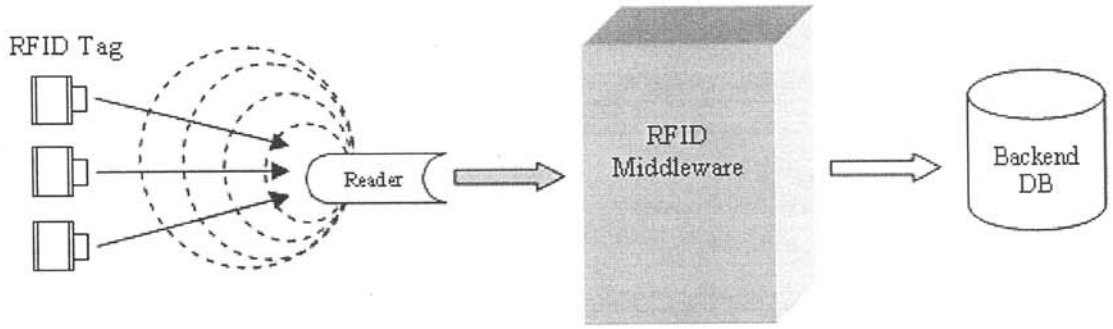

Figura 6. Uma arquitetura RFID típica.

O leitor RFID ocupa-se principalmente de acessar a memória da etiqueta e ler seu conteúdo, que pode ser constituído de vários kilobytes. Entretanto, uma memória maior significa também um custo maior. As etiquetas podem ser de somente leitura ou permitir operações de leitura e escrita. As tags que possibilitam escrita abrem muitas oportunidades de aplicações, mas também estão expostas à operações de escrita não-autorizadas, que permitem a um terceiro alterar as informações contidas na etiqueta. As etiquetas do tipo EPC Class I Gen 2 [9] são largamente utilizadas no mercado e a implementação de uma etiqueta deste tipo requer entre 1000 e 4000 gates, enquanto que uma implementação comercial do protocolo Advanced Encryption Standard (AES) requer entre 20000 e 30000 gates [25]. Devido a esta necessidade de um número grande de gates para a

implementação de sistemas de criptografia, o uso de sistemas de esteganografia se torna mais atraente já que a etiqueta costuma implementar apenas os tipos mais básicos de segurança e possuir recursos computacionais muito limitados. Entretanto, existem no mercado alternativas como a etiqueta DEFfire da Philips, que possui um coprocessador dedicado para operações AES. Porém, o custo de tais etiquetas não a torna indicada para um número grande de aplicações.

As organizações mais importantes para a padronização de sistemas RFID são a International Organization for Standardization (ISO) e a EPCGlobal. Ambas definem os padrões físicos e lógicos de etiquetas e leitores, enquanto a EPC também define o formato e a estrutura dos dados contidos na etiqueta [25] [71].

3.2 - A Técnica

Implementar segurança em sistemas RFID é um grande desafio, devido a fatores como baixa capacidade computacional, memória limitada e exposição a leitores não-autorizados. Uma forma comum de tornar seguras as informações contidas nas etiquetas (tags) RFID é o uso de métodos de criptografia. Porém, informações visivelmente criptografadas atraem suspeitas e curiosidade, mesmo quando o esquema de criptografia usado é muito eficiente. Uma alternativa ao uso de criptografia é a proteção aos dados contidos em uma etiqueta através da utilização de técnicas de Esteganografia. O uso de esteganografia possui a vantagem de levar o processamento necessário à obtenção da informação desejada para os leitores e/ou para o middleware, itens não afetados pelas limitações das etiquetas e que podem utilizar a capacidade computacional necessária.

O RFID pode armazenar dados, além de não necessitar da leitura visual como o código de barras. Junto com isso, o transponder tem um código único (Unique Identification code – UIC)

vindo de fábrica, que não pode ser modificado, além dos dados poderem conter criptografia, leitura simultânea de vários transponders e alta resistência às condições ambientais.

As maiores vantagens [49] do RFID são o aumento da visibilidade na cadeia de valor, prevenção mais eficaz da falta de estoque, ganhos de eficiência, melhor controle no levantamento de inventário e menor trabalho em operações de varejo. Um dos exemplos citados pelo autor é o benefício de que o cliente possa adquirir uma calça jeans de um dado tamanho em uma loja bastando escolher a calça e inserir em um painel o tamanho desejado e em seguida, por meio do sistema RFID, localizar onde está a calça dentro do estabelecimento.

Outra afirmação [50] é que é possível resolver os problemas de excesso de estoque e de produtos com prazo de validade vencido, o que beneficiaria, o mercado farmacêutico, o qual absorve mais de US$ 2 bilhões de produtos devolvidos por ano.

Também cita-se [51] que o RFID oferece liberdade, pois elimina uma barreira e cria um novo valor. A autora identifica esta liberdade no fato de que a empresa prescindirá de um considerável volume de mão-de-obra humana em determinados fluxos de trabalho e poderá aumentar a visibilidade das informações para todos os participantes na cadeia de valor.

Muitos descrevem [75] a tecnologia RFID como uma substituta do código de barras, porém com mais benefícios, como a possibilidade de leitura de itens múltiplos, extensão da capacidade de captação de dados e maior durabilidade.

Alguns exemplos são o planejamento e gerenciamento de estoques, a automação da expedição e a rastreabilidade para as indústrias. Já na distribuição, a tecnologia traz o gerenciamento de estoque, a automação do recebimento, a rastreabilidade, movimento e expedição, o aumento da produtividade, a redução de obsolescência e nível de estoque. Proporciona o gerenciamento de estoque e gôndolas, a rastreabilidade e a redução de perdas, a automação do recebimento e de vendas.

As organizações perceberam a necessidade de uma nova tecnologia para ajudar no seu crescimento e desenvolvimento no mercado, evitando assim erros e aumentando o controle dos seus produtos.

As empresas que utilizam a tecnologia RFID se destacam com o aumento de suas chances de competição no mercado, pois podem vir a obter dados mais rápidos dos produtos, passando assim informações mais rápidas e precisa para seus clientes. Outra questão de importância é que essas empresas terão um controle maior dos seus produtos permitindo uma negociação mais eficiente de preços e quantidades [52]. Ainda segundo o autor, o RFID não vem a ser apenas um substituto do código de barras, pois além de ser seu substituto natural, é também uma tecnologia de transformação que pode ajudar a reduzir desperdício, gerir inventários, limitar roubos, simplificar a logística e até aumentar a produtividade.

3.3 – Aplicações RFID

A tecnologia RFID é usada [75] em todas as áreas que se necessita uma captura automática de dados, colaborando com a identificação de objetos sem contato físico, via radiofreqüência, com aplicações que variam de sistemas de pagamento via Internet, seguros, a automatização industrial e o controle de acesso [53].

As etiquetas com microchip colocadas nos produtos funcionam como uma espécie de documento de identificação com informações de preço, número do lote e prazo de validade, além de permitir uma relação mais afinada entre linhas de produção, os consumidores e os sistemas de informação de uma organização. Algumas outras aplicações para o sistema são:

3.3.1 Aplicações Médicas

Usados embaixo da pele, os dispositivos guardam registros que incluem desde a identidade, o tipo sangüíneo e outros dados da condição do paciente, agilizando o seu tratamento.

No caso de uma emergência, o chip pode salvar vidas, reduzindo necessidade de testes de grupo sangüíneo, alergias ou doenças crônicas, além de fornecer uma lista do passado de medicamentos em uso pelo paciente. Por isso, obtém-se maior agilidade na busca de informações e tratamento sem a necessidade de prontuários médicos.

3.3.2 - Linha de Montagem Industrial

Uma aplicação bastante usada para a tecnologia RFID está nas linhas de montagens de veículos. Com o sistema, todo o processo de montagem pode ser monitorado desde o início até a entrega final do produto ao consumidor, facilitando o acompanhamento do processo.

No caso dos veículos, a tecnologia pode ser utilizada ainda como integrante de sistemas de proteção contra roubos, agindo no sistema de ignição até o travamento de portas e bloqueio de combustível do veículo.

O uniforme dos funcionários da fábrica, remédios e equipamentos e crachás de visitantes também podem ser etiquetados, criando um ambiente de administração estruturado, aumentando a segurança das pessoas e reduzindo erros.

3.3.3 - Transportes Aéreos, Terrestres e Marítimos

Algumas empresas aéreas estão utilizando a tecnologia nas bagagens dos passageiros, evitando reduzir perdas e facilitar o itinerário das malas nos casos de mudanças nos planos de vôo das

companhias. Dessa maneira, o setor portuário também utiliza-se a tecnologia RFID para rastrear bagagens de passageiros e contêineres.

Outra aplicação é o uso de Transponders em cargas terrestres para circulação em rodovias, tendo em vista um melhor controle dos produtos e fiscalização na emissão de notas fiscais com o intuito de reduzir contrabando e até mesmo o tráfico de drogas.

3.3.4 – Logística

Dentro da logística estão envolvidos vários processos, como estoque, transporte, manuseio de materiais, armazenagem, entre outros. Nesses, a utilização da tecnologia RFID se faz presente visando redução de custos, menor desperdício, maior agilidade nos processos e maior satisfação dos clientes. Para efetuar rastreamento de objetos em contêiner, ada etiqueta é associada a um contêiner e a dados sobre os produtos contidos, informações essas que são atualizadas a cada vez que o contêiner é reutilizado. Para este tipo de aplicação, é obrigatório o uso de etiquetas com capacidade de leitura e escrita. [72]

Dentre a utilização do RFID neste setor, destaca-se:

- Controle de qualidade, possibilitando o controle de produtos de forma integrada e automática ao sistema de manufatura. [73]

- Inventário de produtos em tempo real, garantindo um correto levantamento dos estoques existentes.

- Auxílio nas operações de recebimento, separação, transporte, armazenamento de materiais em depósitos e armazéns.

3.3.5 - Aplicações Financeiras

Pode-se encontrar aplicações da tecnologia RFID especialmente relacionadas à segurança nas transações bancárias. Pode-se se dar o exemplo de cartões bancários do tipo *Smart-Card*. Por exemplo, quando um cliente portando um exemplar do mesmo, associado com o Transponder RFID, chega a um caixa eletrônico bastará digitar a senha de acesso e o equipamento varrerá o corpo buscando captar as informações contidas no chip que irá transmitir outros dados pessoais e autorizará a transação.

Outra aplicação seria colocar Transponders em cédulas de dinheiro, procurando com isso reduzir a falsificação. Com o chip no papel moeda, a contagem de grandes quantias também seria feita muito mais rapidamente.

3.3.6 - Aplicações para Bibliotecas

Cada etiqueta é associada a um livro. As etiquetas podem ser do tipo somente leitura, ou do tipo capaz de leitura e escrita para quando se faz necessário atualizar as informações contidas nos livros. Neste tipo de aplicação, normalmente não se requer capacidade de leitura a longa distância porque as etiquetas são comumente lidas por dispositivos portáteis como PDAs.

3.4 – Privacidade em aplicações RFID

Visando o respeito à privacidade dos consumidores, os estabelecimentos comerciais, financeiros ou de qualquer outro ramo de atividade que envolva o uso de etiquetas RFID, deveriam seguir regras básicas [5]:

- Etiquetas RFID devem estar bem visíveis, devem ser facilmente identificáveis e removíveis pelo cliente.

- Os consumidores devem ser notificados quanto à presença de etiquetas RFID nos produtos e onde isso ocorre.

- Etiquetas com o sistema devem ser desativadas após a compra do produto, independente de uma solicitação prévia do consumidor.

- Etiquetas com o sistema também devem ser posicionadas na embalagem do produto, para facilitar sua retirada.

- Uso de códigos, para que o teor da etiqueta só possa ser usado perante a informação de um código adicional. Por exemplo: em um supermercado, o usuário digita um código pessoal no caixa para liberar a compra usando um Smart-Card, onde esse possui a tecnologia.

- Criptografia baseada em chaves, para que somente emissor e receptor tem ingresso ao material da informação atrelada aquela etiqueta. Qualquer pessoa que tente obter esses dados ilicitamente terá que decodificar um padrão criptográfico. Isso faz com que seu uso em larga escala seja viável e que o cotidiano das pessoas seja facilitado sem maiores transtornos. Esses recursos não garantem segurança total no uso das etiquetas RFID, porém já fazem com que esta tecnologia se torne menos vulnerável e mais confiável.

3.4.1 - Ameaças à Privacidade

A tecnologia RFID pode ser aplicada [75] conforme a necessidade, podendo ser utilizada em varias funções, desde o controle de estoques e identificação de propriedade até a prevenção contra furto. Todas as possibilidades de uso levantadas até aqui demonstram porque é mais ágil um processo pode tornar-se com sua utilização.

Quando utilizadas em um ambiente controlado, as etiquetas com a tecnologia e os dispositivos leitores funcionam perfeitamente bem. Nesse contexto, a grande maioria das aplicações vindas pela tecnologia é positiva. Contudo, nem todas trazem apenas benefícios, algumas retornam coisas negativas.

Por exemplo, uma diferença marcante entre as etiquetas e os tradicionais códigos de barras é que estes são utilizados nos produtos para identificação nas lojas, porém, depois da compra, perdem a sua função. No entanto, as etiquetas RFID são, em muitos casos, permanentes nos produtos, respondendo sempre que recebem o sinal de um leitor.

A ameaça à privacidade surge quando a etiqueta eletrônica permanece ativa mesmo quando deixa o estabelecimento comercial. Um exemplo é uma residência e tudo o que existe no seu interior identificado e rastreado com etiquetas eletrônicas. Uma pessoa mal intencionada que caso tenha um leitor, poderia levantar todos os bens existentes na casa.

3.4.1.1 - Microchip no Dinheiro

No caso dos microchips colocados em dinheiro, não há duvida de que essa tecnologia traria maior segurança quanto à possibilidade de falsificação, mas também conceberia uma mudança radical na forma como nos portamos com nossas finanças.

Considerando que a tecnologia usada dessa forma habilitaria o rastreamento das transações individuais, o dinheiro deixaria de ser uma forma de anonimato nas compras e vendas. Além disso, governo e bancos não seriam os únicos a saberem quanto uma pessoa possui ou gasta já que os criminosos também poderiam obter leitores e ter acesso a tais informações de alguma forma.

3.4.1.2 - Microchip em Documentos

Outra questão, relacionada com a segurança e privacidade das pessoas, é dos dispositivos RFID na autenticação e uso em documentos importantes como carteiras de motorista, diplomas universitários, certidões de nascimento e passaportes, devido ao risco de roubo de identidade. As etiquetas RFID para esse tipo de aplicação ainda apresentam um fator negativo: não contém nenhuma rotina ou dispositivo extra para proteger seus dados além da criptografia, sendo perfeitamente possível a um terceiro quebrar o código e roubar a identidade da outra pessoa.

3.5 – Vantagens

A tecnologia RFID oferece [75] algumas possibilidades de aplicação, apresentando soluções para os sistemas de rastreamento e identificação com diversas vantagens:

- Eliminação de erros humanos e maior confiabilidade
- Aumento da segurança em operações repetitivas;
- Redução de custos operacionais;
- Operação sem a necessidade de contato com as pessoas.
- Aumento na velocidade dos processos, devido à automação dos mesmos;
- Melhor controle de qualidade com conseqüente redução de perdas

Como se percebe, a confiabilidade é uma das maiores vantagens da tecnologia RFID. Ao contrário da maioria dos sistemas existentes no mercado, não existe possibilidade da operação de leitura dos Transponders depender de contato físico ou elétrico. Algumas outras vantagens do sistema são:

- Rastreabilidade de produtos e de seres vivos.
- Capacidade de armazenamento dos dados coletados.
- Leitura simultânea de milhares de itens diferentes por segundo
- Possibilidade de reutilização e alta durabilidade das etiquetas.
- A otimização do processo de gestão portuária, permitindo às organizações operarem muito próximo da capacidade nominal dos portos.Ficam assim eliminados os problemas decorrentes de oxidação, sujeira e desgaste de superfícies. A operação é simples, bastando apenas juntar o leitor do Transponder, não sendo necessária uma posição predefinida para a leitura.

3.6 – Desafios e desvantagens de sistemas RFID

Alguns dos problemas que pode surgir [75] às pessoas e organizações caso a tecnologia RFID seja disseminada em larga escala e sem existir o devido cuidado com a segurança são os seguintes:

Violação de integridade - Uma etiqueta possui dados específicos do material ou pessoa em que está acoplada. Caso for retirada e colocada em outro local poderá causar sérios prejuízos ao seu proprietário.

Cópia de etiquetas - Uma pessoa mal intencionada e com conhecimento técnico poderia reproduzir os dados de uma etiqueta e criar uma nova etiqueta com os mesmos dados. Exemplo: automóveis com a tecnologia que não necessitam da chave podem ter seu código copiado, facilitando seu roubo.

Monitoramento da etiqueta - Obtenção de dados para uso indevido sem envolver a etiqueta. Exemplo: as informações bancárias de um indivíduo podem ser rastreadas e usadas indevidamente por terceiros.

Transporte de Bens – Vários portos e aeroportos pelo mundo utilizam-se

dessa tecnologia para controlar a movimentação de bagagens dos seus usuários. Porém, esse tipo de tecnologia pode representar um grande problema se a etiqueta, integrada ao objeto transportado, armazenar uma quantidade elevada de informações. Por exemplo, uma etiqueta falsificada, tem seu conteúdo modificado e passa a transportar, juntamente com os dados válidos, um vírus. Na hora que for exposta poderá causar um estouro de memória, infectando o sistema leitor e o servidor com esse vírus. Uma vez alojado no servidor, o agente poderia infectar todo o banco de dados e prejudicar outras etiquetas cadastradas ou ainda, instalar "backdoors", desviando informações confidenciais para uso indevido por outras pessoas. Devido ao custo ainda elevado da tecnologia, seria praticamente impossível se proteger contra tais ataques, sendo necessário protocolos mais complexos que os atuais para controlar o acesso dos leitores aos dados contidos no microchip. Mesmo as etiquetas passivas, que tem um raio de alcance de alguns metros, podem sofrer interceptação e extravio de suas informações.

Segurança Pessoal e Material – No caso da segurança pessoal, deve-se considerar que RFID e GPS são tecnologias diferentes. Uma pessoa usando um microchip RFID, tem que portar um dispositivo transmissor de GPS, que ainda é grande e precisa de uma bateria de longa duração para funcionar, associado ao microchip, que contém suas informações pessoais. Apenas assim sistemas RFID com chips implantados em pessoas permitem o rastreamento a longas distâncias para prover segurança pessoal.

Nesse caso, argumenta-se que distância de leitura de uma etiqueta pode apresentar variações quando há obstáculos entre o leitor e o emissor. Exemplificando, os móveis com etiquetas RFID contidos no interior de uma residência.

Assim, para que pessoas possam utilizar essa tecnologia para praticar ações ilícitas, teriam que possuir um receptor com mais capacidade de recepção do que o normal. Mas isso não é um grande

problema atualmente. O valor desse aparelho é muito grande, mas é perfeitamente possível construir um de forma artesanal.

Tais sistemas se baseiam em transmissores passivos que emitem sinais de radiofrequência e que funcionam com um código criptografado, permitindo a liberação do sistema que deixa o automóvel imóvel e da parte elétrica do veículo, inclusive o sistema de ignição do motor.

Algumas outras desvantagens: [54,55]

- O custo elevado da RFID em relação aos sistemas de código de barras é um dos principais obstáculos para o aumento de sua aplicação comercial.
- O uso em materiais condutivos e metálicos relativos ao alcance de transmissão das antenas. Como a operação é fundamentada em campos magnéticos, o metal pode interferir negativamente no desempenho. Outrora, alguns encapsulamentos especiais podem resolver esse problema fazendo com que automóveis, vagões de trens e contêineres possam ser identificados, guardadas as limitações com relação às distâncias de leitura.
- O preço final dos produtos, pois a tecnologia não se limita ao microchip anexado ao produto. Por trás disso estão antenas, leitoras, ferramentas de filtragem das informações e sistemas de comunicação.
- A invasão da privacidade dos consumidores por causa da monitoração das etiquetas coladas nos produtos. Perante a isso, existem técnicas de alto custo que quando o consumidor sai fisicamente de uma loja, a funcionalidade do RFID é automaticamente bloqueada.

4 – TRABALHOS CORRELATOS E DESCRIÇÃO FORMAL DO PROBLEMA.

A tecnologia RFID vem apresentando um grande potencial de utilização em setores da automação industrial, residencial e hospitalar. No entanto, estas aplicações podem resultar em riscos a segurança e privacidade dos usuários.

As etiquetas RFID possuem um grande problema: não contém nenhuma rotina ou dispositivo para proteger seus dados. Mesmo as etiquetas passivas, que possuem pouco raio, podem sofrer interceptação de suas informações.

Neste capítulo analisamos alguns trabalhos que possuem relação com o estudo proposto. Para isto, efetuou-se uma revisão literária responsável por detalhar outras pesquisas cujos objetivos focam a área de segurança em sistemas RFID e também apresenta os trabalhos relacionados com Esteganografia.

A literatura é abundante no que se refere a segurança para sistemas RFID, mas a maioria dos artigos publicados refere-se ao uso de outros métodos que não esteganografia, como criptografia, assinaturas digitais e autenticação. Nas situações em que Esteganografia é aplicada a RFIDs, o foco tende a ser não em Confiabilidade mas em um dos outros três pilares da segurança de informação, como Disponibilidade e Integralidade [32]

Inicialmente, o desenvolvimento de sistemas de RFID focou-se em questões de usabilidade e performance, com menos atenção dedicada à parte de segurança. Com o crescimento do uso de sistemas RFID e sua aplicação em ambientes de alta segurança, surgiu a necessidade de disponibilizar amplos recursos de segurança, e muitos trabalhos foram desenvolvidos visando aumentar a segurança na identificação e autenticação desses sistemas. [6, 7].

Vários estudos apontam formas de resolver alguns desses

problemas de segurança, seja por alteração dos protocolos utilizados [16, 17], através do uso de dispositivos auxiliares [15, 18, 20], ou por força de legislação. [14]. Também foram feitos estudos propondo um sistema que se utiliza de Esteganografia em sistemas RFID [32], mas o trabalho citado é focado no aumento de Integralidade, enquanto que o presente trabalho é focado em Confidencialidade, um outro pilar da Segurança de Informações [34].

Há trabalhos que comparam o uso de Esteganografia com outros métodos de ampliação de segurança em sistemas RFID. Gandino [76] resumiu em tabelas as diferenças entre os diferentes métodos. Conforme podemos ver na Tabela 2, Esteganografia é o único método que possibilita o uso de etiquetas padrão EPC96, com middleware e canal de comunicação padrão. A grande adaptabilidade da Esteganografia a sistemas de RFID simples e já existentes a torna uma opção vantajosa em relação a métodos que exigem alterações e/ou sistemas proprietários.

Tabela 2: Comparação de métodos referentes
a sua aderência ao padrão EPC Class I Gen 2 [76]

Técnica	Requerimentos		
	Etiquetas	Leitores	Comunicação
Marca d'água	Standart (EPC96)	Capazes de gerar Marca d'água	Padrão
Atividade de Leitura	Área especial de memória e protocolo de leitura customizado	Padrão	Padrão
Autenticação	Padrão de grande área de memória	Padrão com criptografia	Padrão
Proteção de Privacidade	Padrão de grande área de memória	Padrão com criptografia	Padrão
Esteganografia	Padrão EPC96	Padrão	Padrão
Senha	Padrão com senha	Padrão	Padrão
Autenticação	Criptografia	Padrão com criptografia	Autenticação

Também é possível comparar os diferentes métodos de acordo com os elementos que influenciam a robusteza do método escolhido. No caso do RFID, Gandino [76] também comparou os diferentes métodos e podemos ver que sistemas que utilizam esteganografia tem a sua robustez ampliada de acordo com fatores como tamanho da mensagem a ser oculta (quanto menor, melhor), divulgação do lugar onde as informações serão armazenadas (quanto menos divulgado, melhor) e confiança nos participantes do sistema (quanto mais confiáveis, melhor). Portanto, na tabela 3 pode-se ver que o maior problema do uso de esteganografia em etiquetas RFID é o pouco espaço disponível para armazenamento de informações.

Tabela 3: Comparação de características que afetam a robusteza de diferentes métodos

Técnica	Fator de Robustez	Obstáculos no RFID
Marca d'água	Tamanho da Marca d'água, sigilo da função e confiabilidade dos participantes	Área no padrão EPC, atualização difícil
Atividade de Leitura	Apenas leitura e tamanho da memória especial	Alterações não são perceptíveis, necessidade de memória extra e de comunicação, vulnerável a participantes
Proteção de Privacidade	Tamanho das chaves, sigilo das chaves	Área de memória e tempo de transmissão
Esteganografia	Tamanho do código, FCC, sigilo da área utilizada, confiabilidade dos participantes	Área no padrão EPC, pode necessitar várias tags
Senha	Tamanho, sigilo e número de senhas	Memória extra, vulnerável a espionagem
Autenticação	Tamanho das chaves, sigilo das chaves	Computação extra nas tags

Existem muitos estudos já desenvolvidos que tratam de detecção de alterações (*tampering*) em etiquetas RFID. Tais estudos são muito eficientes quando se trata de evitar e detectar alterações em dados contidos em etiquetas RFID, mas isso é conseguido à custo de etiquetas e/ou leitores customizados. Além disso, estes estudos não oferecem

formas de evitar a leitura dos dados por pessoas não-autorizadas. Normalmente, para evitar a leitura de dados por pessoas não-autorizadas são utilizados métodos de autenticação [2], [7], [21], watermarking [20], [22] ou de criptografia [3], [1], [7]. Na tabela 4 [77] temos um resumo das técnicas no que tange ao Anonimato.

Tabela 4: abordagens ao anonimato [77]

Proposta	Abordagem
Inoue e Yasuura 2003	Utilizando duas etiquetas – uma para identificação exclusiva e outra para detalhes do produto. Não resolve inventários ou rastreamentos clandestinos.
Juels e Pappu 2003	Recriptografia do conteúdo da etiqueta utilizando o criptossistema El Gamal. A solução é apresentada no contexto de garantia de cédulas habilitadas por RFID.
Juels, Rivest e Szydlo 2003	Etiquetas de Bloqueio: Uma etiqueta que especifica se pode ser lida ou não. Um bit de privacidade (0 ou 1) é designado na etiqueta, o que determina se a etiqueta pode ser escaneada publicamente (bit 0) ou pode ser usada de forma privada (bit 1).
Ateniese, Camenisch e de Medeiros 2005	Propuseram a utilização do pareamento bilinear em criptografia de curva elíptica. A autenticidade no identificador da etiqueta é mantida assinando-se digitalmente o texto cifrado com um CA confiável. Esta abordagem não pode resolver a questão da troca do texto cifrado, i.e., quando o bisbilhotador troca o conteúdo de duas etiquetas, traocando simultaneamente o seu conteúdo.
Rakesh Kumar	Uma gaiola de Faraday é um recinto projetado para excluir campos eletromagnéticos. Como resultado, determinadas frequências de rádio não podem penetrar através desta. Ela pode resolver preocupações com a privacidade, por exemplo, se cédulas de moeda de valor elevado começarem a embutir uma etiqueta RFID, e então o uso de carteiras forradas com lâmina pode garantir a privacidade

Tais métodos, porém, não atendem à necessidade de manter uma etiqueta legível a todos os participantes legítimos da cadeia de Produção-Transporte-Consumo e tampouco atendem à necessidade de utilizar etiquetas de custo bastante reduzido. Na Tabela 5 [77] temos um resumo das técnicas no que tange à Autenticidade.

Tabela 5: abordagens à Autenticidade [77]

Proposta	Abordagem
Juels 2005	PIN: Autenticar a etiqueta para o leitor
Juels 2004	Provas de Yoking – proporcionam provas criptográficas de que duas etiquetas foram simultaneamente escaneadas e em proximidade física. Podem ser usadas em uma farmácia para provar a uma agência do governo de que a farmácia escaneou um frasco de medicamento etiquetado e entregou o medicamento exato, como prescrito na receita etiquetada com RFID
Engberg et al. (2004)	Protocolos baseados em conhecimento zero para comunicação entre o leitor e a etiqueta de forma que possam autenticar um ao outro sem revelar qualquer secreto que possa permitir que sejam rastreados.
Molnar e Wagner, 2004	Esquemas de autenticação mútua usando desafio-resposta baseada no uso de função pseudo-randômica na computação de respostas a desafios.
Feldhofer et al., 2004	Propõe o protocolo Simple Authentication and Security Layer (SASL) com criptografia AES e analisa os requisitos de hardware
Dimitriou, 2005	Proporciona segredo futuro usando nonces (números aleatórios que nunca são reutilizados) tanto pelo leitor quanto pela etiqueta, nos seus desafios um para o outro.

Neste aspecto, o presente trabalho visa aprofundar os estudos no uso de Esteganografia em sistemas simples e padronizados, mesmo tendo em vista as poucas possibilidades de ocultação de informações em uma quantidade de memória tão restrita. Para tanto, vamos demonstrar dois métodos, um que oculta informações apenas em uma etiqueta e outro que oculta e recupera informações alteradas em um grupo de etiquetas.

4.1 - Descrição Formal do Problema e idéia básica da solução.

As mesmas características que tornam o RFID tão versátil acabam tendo como consequência inesperada alguns problemas que são intrínsecos à tecnologia RFID. Um desses problemas é a leitura das informações das etiquetas RFID por pessoas não-autorizadas. Se um carregamento de um determinado produto é identificado por uma etiqueta RFID, então podemos ler as informações contidas na etiqueta quando o produto está na fábrica, quando está sendo transportado ou quando o mesmo encontra-se armazenado, e utilizar essas informações para tomar decisões referentes a este carregamento.

Um problema existente é que essas mesmas informações podem ser lidas, analisadas e utilizadas para tomar decisões por pessoas externas ao andamento normal do processo de produção e transporte de um carregamento. Por exemplo, pessoas mal-intencionadas podem posicionar um leitor de RFID ao lado de uma rodovia movimentada e ler as informações das etiquetas referentes às cargas que estão passando por esta rodovia. Ao saber qual o produto que está sendo transportado, tais pessoas podem selecionar os carregamentos de produtos de valor mais elevado para eventuais roubos. Também é possível que um concorrente de uma determinada empresa posicione leitores de RFID próximos a via de acesso principal de uma determinada fábrica e seja capaz de determinar o que está sendo produzido nesta fábrica e em que quantidade, obtendo de forma não- autorizada informações estratégicas e

mercadológicas valiosas sobre seu concorrente.

Outro exemplo de uso é o de uma operação de transporte de material militar. Munição e outros equipamentos sensíveis que possuam etiquetas RFID podem ter suas informações sobre tipo, quantidade e destino lidas por uma entidade não-autorizada, o que pode representar um problema de segurança significativo.

Uma forma comum de evitar tais problemas é criptografar as informações referentes a produtos de valor elevado. Embora pareça lógica, essa idéia traz consigo problemas próprios, como o fato de que ao se criptografar o conteúdo de um determinado carregamento, deixa-se claro que ali há uma informação valiosa e atrai-se a curiosidade e a atenção das mesmas pessoas que queremos evitar

Além disso, há a necessidade de ciclos extras para criptografar e descriptografar as informações contidas nas etiquetas RFID, o que ocasiona diminuição da velocidade de leitura, além de gerar um gasto maior de energia para efetuar este processo. É possível demonstrar e quantificar a diminuição da velocidade de leitura (expressa em ciclos) e o aumento do consumo de energia em sistemas RFID quando utilizamos um método de criptografia [1].

Também é tentador criar uma etiqueta ou um leitor com características diferentes daquelas encontradas em sistemas de mercado e que seguem as especificações internacionais. Embora eficaz para ocultar a informação, este tipo de abordagem apresenta como principal problema o aumento de custos, já que sistemas proprietários não se beneficiam das reduções de custo que a produção em larga escala (como a que é feita em sistemas aderentes aos padrões e normas da indústria) oferece. Alterar a máquina de estados de um sistema RFID torna o mesmo caro e de manutenção problemática, além de tornar necessário o uso de sistemas proprietários em toda a cadeia de produção e transporte, o que nem sempre é possível.

O método proposto trata-se de uma forma de ocultar informações em sistemas RFID sem utilizar criptografia nem alterar

a máquina de estados de um sistema RFID padrão, utilizando-se para isso de métodos de Esteganografia passíveis de serem implementados em um *cover* com baixa capacidade de armazenamento como uma etiqueta RFID. Para exemplificar o processo, vamos imaginar uma fábrica de onde saem dois tipos de produtos, um chamado "Caro" e um outro chamado de "Barato". Sabemos que as informações contidas nas etiquetas RFID possuem um formato padrão chamado EPC (*Electronic Product Code*), determinado por um consórcio chamado EPCglobal [10] mas também sabemos que se indicarmos na etiqueta que o produto que está na caixa é do tipo "Caro", atrairemos para ele atenção indesejada. O método proposto envolve colocar no campo padrão de todas as etiquetas a descrição do produto como sendo do tipo "barato" e ocultar de forma esteganográfica a verdadeira informação sobre o tipo do produto em outro lugar da etiqueta. A informação correta será posteriormente obtida pelo Middleware, que será programado para ser ciente do lugar onde verdadeiramente estão armazenadas as informações desejadas.

Como no presente exemplo estamos tratando de um problema que envolve apenas dois produtos, apenas um bit cuidadosamente manipulado é necessário para diferenciá-los, mas o presente sistema pode ser facilmente ampliado para usar um número maior de bits caso seja necessário. Como se depreende do formato padrão chamado EPC (Electronic Product Code) e conforme pode ser visto na Tabela 6, existem 4 campos principais em uma etiqueta passiva Classe 1 Gen 2

Tabela 6. Campos de uma etiqueta RFID Class 1 Gen 2. [10]

Header (Cabeçalho)	EPC Manager (Fabricante)	Object Class (dados do produto)	Serial Number (Número de série)
8 bits	28 bits	24 bits	36 bits

Desta tabela depreende-se que há um campo de 36 bits destinado ao número de série da etiqueta. Se reservarmos o bit menos

significativo desses 36 para indicar qual tipo de produto estamos transportando (zero=Caro, um=Barato) ainda assim temos 35 bits destinados ao número de série da etiqueta, o que é suficiente para a imensa maioria das aplicações.

Ao utilizar um bit do número de série para indicar o tipo de produto, evitamos que pessoas não-autorizadas e que desconheçam o método esteganográfico utilizado possam acessar a informação verdadeira sobre qual é o tipo do produto está sendo transportado.

Mesmo com a ocultação dessa informação, um eventual invasor acreditará ter obtido todas as informações sobre o produto (pois a etiqueta não está criptografada) e evitamos os custos extras decorrentes do uso de um sistema proprietário. Além disso, a etiqueta ainda pode ser usada normalmente por terceiros envolvidos de forma autorizada no processo de manufatura e transporte, pois as etiquetas usadas são padrão de mercado e o tipo de um produto não altera, por exemplo, o nome do fabricante que o originou ou o endereço onde deve ser entregue (informações úteis para cobrança e logística), pois essas informações estão disponíveis normalmente na etiqueta. Para se utilizar a informação oculta de forma correta, é necessário apenas fazer uma alteração no middleware do sistema que deve efetivamente e de forma autorizada utilizar a informação verdadeira sobre o tipo de produto ("Caro" ou "Barato").

Caso se faça necessário, o mesmo método pode ser utilizado para ocultar outros tipos de informação presentes na etiqueta RFID, como por exemplo o nome do fabricante ou o destino final da mercadoria. Caso seja necessário o uso de um número maior de bits (em comparação com apenas um bit utilizado no exemplo) basta aumentar o número de bits reservados para este uso entre os utilizados no número de série da etiqueta, ou mesmo usar grupos de tags (como por exemplo, as tags de todo um lote de produção) para ocultar uma parte da informação em cada etiqueta. Como exemplo, se tivermos quatro tipos de produtos fabricados (no caso de uma fábrica de bicicletas pode ser

"Feminina", "Masculina", "Infantil" e "Mountain Bike") bastaria utilizarmos dois bits reservados do campo do número de série, onde armazenaríamos bits de acordo com o tipo de bicicleta, conforme indicado na tabela 7.

Tabela 7. Números de série alterados para conter uma informação oculta.

Tipo de Bicicleta	Feminina	Masculina	Infantil	Mountain Bike
Bits a serem inseridos	00	01	10	11
Conteúdo do campo Número de Série	00000000000000000000000000011100	00000000000000000000000000010101	00000000000000000000000000011010	00000000000000000000000000001111
Significado Real (tipo e número de série em decimal)	Bicicleta Feminina, NS 7	Bicicleta Masculina, NS 5	Bicicleta Infantil, NS 6	Mountain Bike, NS 3

Novamente, o padrão de esteganografia utilizado deve ser informado ao middleware utilizado, mas mantemos o uso de leitores e etiquetas padrão. No campo onde teoricamente deveríamos colocar o tipo da bicicleta, podemos colocar qualquer informação errônea de forma a frustrar eventuais leituras não-autorizados destas etiquetas. Note que para todos os outros participantes da cadeia de Produção-Transporte-Consumo o uso da etiqueta permanece possível e funcional, afinal não estamos alterando campos que indicam o destino da mercadoria (para o uso da logística) nem informações sobre o tamanho da embalagem (para uso dos responsáveis pelo armazenamento) e tampouco informações referentes ao fabricante e a datas de fabricação. Caso seja necessária a ocultação de informações ainda maiores, é possível replicar todos os 24 bits do campo Product Code no campo do número de série e ainda ficariam disponíveis 12 bits para o número de série, o suficiente para dar um número distinto a 4.096 diferentes itens fabricados.

Visando formalizar o sistema e a ideia apresentada, serão

desenvolvidos dois sistemas capazes de receber uma informação, ocultá-la dentro do número de série de uma etiqueta RFID e recuperar a informação correta após leitura posterior da etiqueta. O algoritmo usará a área inicialmente dedicada ao número de série para inserir a informação a ser ocultada. A escolha de tal campo deve-se ao relativo pouco espaço disponível em uma etiqueta RFID, o que impede a utilização de certos métodos de esteganografia que são apropriados para uso em covers de capacidade bem mais elevada, como por exemplo a manipulação de bits menos significativos em imagens digitalizadas. Além disso, trabalhos correlatos indicam que o campo do número de série realmente é o mais apropriado para este tipo de manipulação [77].

5 – ESQUEMAS PROPOSTOS PARA A OCULTAÇÃO ESTEGANOGRÁFICA DE DADOS.

5.1 – Método 1 – Ocultação de informações em uma única etiqueta RFID

Nesta seção, uma visão geral da solução de Ocultação Esteganográfica de Dados (OcEDados) é fornecida, seguida da obtenção dos principais requisitos para o OcEDados. Com base nestes requisitos, a lógica de projeto para o OcEDados é esboçada.

O OcEDados oferece uma solução esteganográfica para ocultar dados em etiquetas RFID. Na solução OcEDados proposta, é presumido que somente vamos ocultar as informações do campo "item". Isto é devido ao fato de é presumido que o ataque intencional ou a tentativa de leitura indevida foi causada por motivações econômicas, como descobrir o conteúdo de um container ou o valor de uma carga de transporte.

A estrutura de dados de RFID é composta de quatro partições – Cabeçalho, EPC Manager (EM), Object Class (OC) e Número de Série (SN). O EM identifica globalmente um fabricante de forma única, a OC identifica um produto fabricado por um fabricante, i.e., o EM e o SN identificam um item único que pertence a um produto. Uma explicação detalhada pode ser encontrada em [79,80,81].

Para ocultar os dados, o OcEDados embute um padrão secreto dentro de campos de todas as etiquetas de RFID que se deseja proteger. Por exemplo, digamos que se tenha um conjunto de etiquetas que serão usados para identificar caixas com CPUs de diferentes fabricantes e de diferentes modelos. Serão utilizados os códigos para os diferentes modelos de CPUs constantes na Tabela 8: Estes códigos serão então usados para escrever informaçãos em etiquetas RFID no padrão descrito na Tabela 6.

Tabela 8. Diferentes Códigos de Produtos.

Código	CPU
123456	ARM9
234567	Intel I3
345678	Intel I5
456789	Intel I7
567890	AMD Phenom
080002	AMD Athlon
789012	TI DaVinci

5.1.1. - Requisitos para a Solução OcEDados

Para resolver as questões de ocultação de dados, os requisitos a seguir são estabelecidos para a solução proposta:

1. Comprimento do Padrão Secreto: O comprimento do padrão secreto deve ser menor do que ou igual ao número total de bits disponíveis no número de série de etiquetas de RFID que podem ser utilizadas para embutimento. Ele não deve ocupar muito espaço porque a quantidade de dados que podem ser armazenados em uma etiqueta é muito limitada.

2. Geração do Padrão Secreto: As entradas para a geração do padrão secreto devem estar disponíveis na própria etiqueta.

3. Locais de Embutimento: O padrão secreto deve ser embutido na partição do número de série.

4. Ocultação de Dados: O algoritmo deve ser capaz de ocultar dados.

5. Arquitetura Plug-n-Play: A solução proposta deve ser projetada de forma que possa ser facilmente conectada nas aplicações de middleware de RFID existentes.

5.1.2 - Lógica de Projeto para a Solução OcEDados

O fundamento teórico para o OcEDados é proposto para atender os requisitos esboçados anteriormente. As decisões de projeto a seguir são propostas nesta solução.

1. O tamanho do padrão secreto depende de quantos tipos de produtos diferentes vamos utilizar, mas no caso demonstrado, com 6 tipos de produtos, é menor do que o campo SN (Req. 1)

2. O padrão secreto é gerado a partir dos dados armazenados no EM e na OC. (Req. 2)

3. O padrão secreto é embutido na partição do número de série porque este oferece bits suficientes (36 bits), que podem ser utilizados para o embutimento. (Req. 3)

4. O padrão secreto seria extraído do jogo de etiquetas de RFID para recuperar os dados ocultos. (Req. 4)

5. O algoritmo é projetado como um componente; assim, ele pode ser facilmente conectado em uma aplicação de middleware existente. (Req. 5)

Agora será discutido o fundamento teórico do OcEDados.

5.1.3 – Fundamento teórico do esquema OcEDados

A estrutura proposta pode ser decomposta em quatro diferentes estágios:

Geração do Padrão Secreto. Para gerar o padrão secreto, primeiramente será definido quais métodos de ocultação de dados serão utilizados. Para o presente projeto, foram desenvolvidos 8 formas diferentes de armazenar a informação a ser ocultada em uma etiqueta RFID. Estes métodos estão descritos na Tabela 9:

Tabela 9. Métodos de Codificação.

Método (Filtro)	**Localização dos seis bytes do campo "Item"**
0	normal
1	2 bytes finais "" + 2 bytes finais campo "Item" + 2 bytes finais campo "série"
2	2 bytes iniciais "empresa" + 2 bytes iniciais campo "Item" + 2 bytes iniciais campo "série"
3	1o e último byte campo "empresa" + 1o e último byte campo "Item" + 1o e último byte campo "série"
4	Método 1, invertido
5	Método 2, invertido
6	Método 3, invertido
7	6 bytes finais do número de série

Para ler e gravar informações em etiquetas RFID, foi utilizado o leitor M5 da Mercury, equipamento pertencente ao Grupo de Sistemas Embarcados (GSE) da PUC-RS.

O programa utilizado para efetuar as gravações e testes do presente trabalho é o "Gravação de Tags padrões EPCGlobal" desenvolvido pelo GSE (Grupo de Sistemas Embarcados). Na Figura 7 temos uma captura de tela deste programa.

No caso ilustrado na Figura 7, o método selecionado no campo "filtro" é zero, o que significa não está sendo utilizado método de embutimento e que o conteúdo do campo Item estará de padronizado.

Tendo 456789 como conteúdo do campo Item, e de acordo com a Tabela 8 de produtos, é possível ver que se trata de um processador I7 da Intel. Para inserir a informação de forma oculta, é possível utilizar um dos métodos descritos. No exemplo da figura 8, será utilizado o método 3.

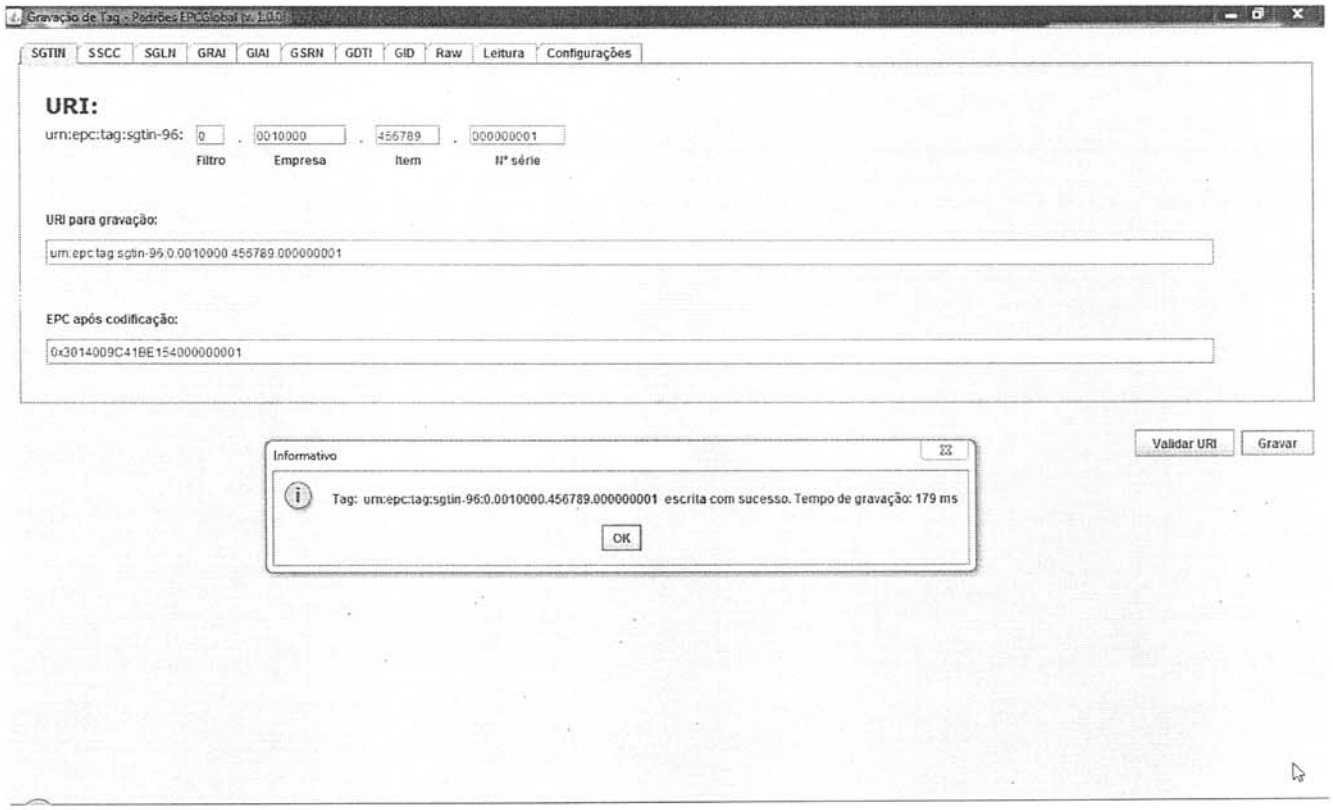

Figura 7. Software de leitura/Escrita de tags utilizado

Como é possível notar, o campo "Filtro" está indicando o uso do método 3 (1° e último byte campo "empresa" + 1° e último byte campo "Item" + 1° e último byte campo "série"). Então, para esta entrada os bytes são:

1° byte do campo empresa: 4
Último byte do campo Empresa: 5
1° byte do campo "Item": 6
Último byte do campo "Item" : 7
1° byte do campo "Série": 8
Último byte do campo "Série": 9

De onde é possível obter o código 456789 (referente a processador Intel I7) como sendo o verdadeiro conteúdo do campo "Item".

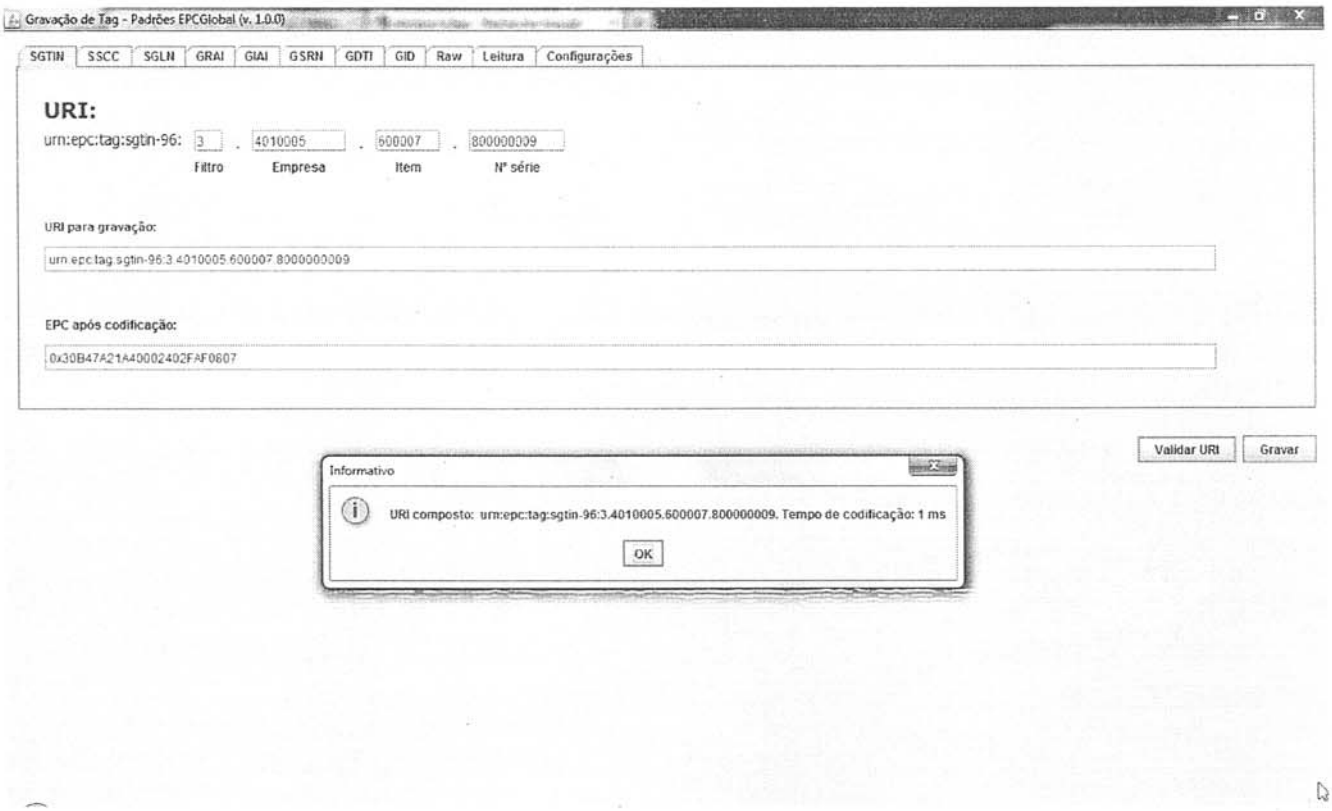

Figura 8. Informação Oculta com o Método 3

Na Figura 9 temos mais um exemplo, utilizando o Método 5:

2 bytes iniciais "empresa":	20
2 bytes iniciais campo "Item":	00
2 bytes iniciais campo "série")	80

Resultando em 200080, que deve ser invertido para mostrar a informação verdadeira 080002 do campo "Item", (referente a processador AMD Athlon) como sendo o verdadeiro conteúdo do campo.

Se for desejado utilizar o método 7 e apenas utilizar outro campo para ocultar a informação, a mesma deve ser embutida integralmente na partição do número de série da etiqueta de RFID

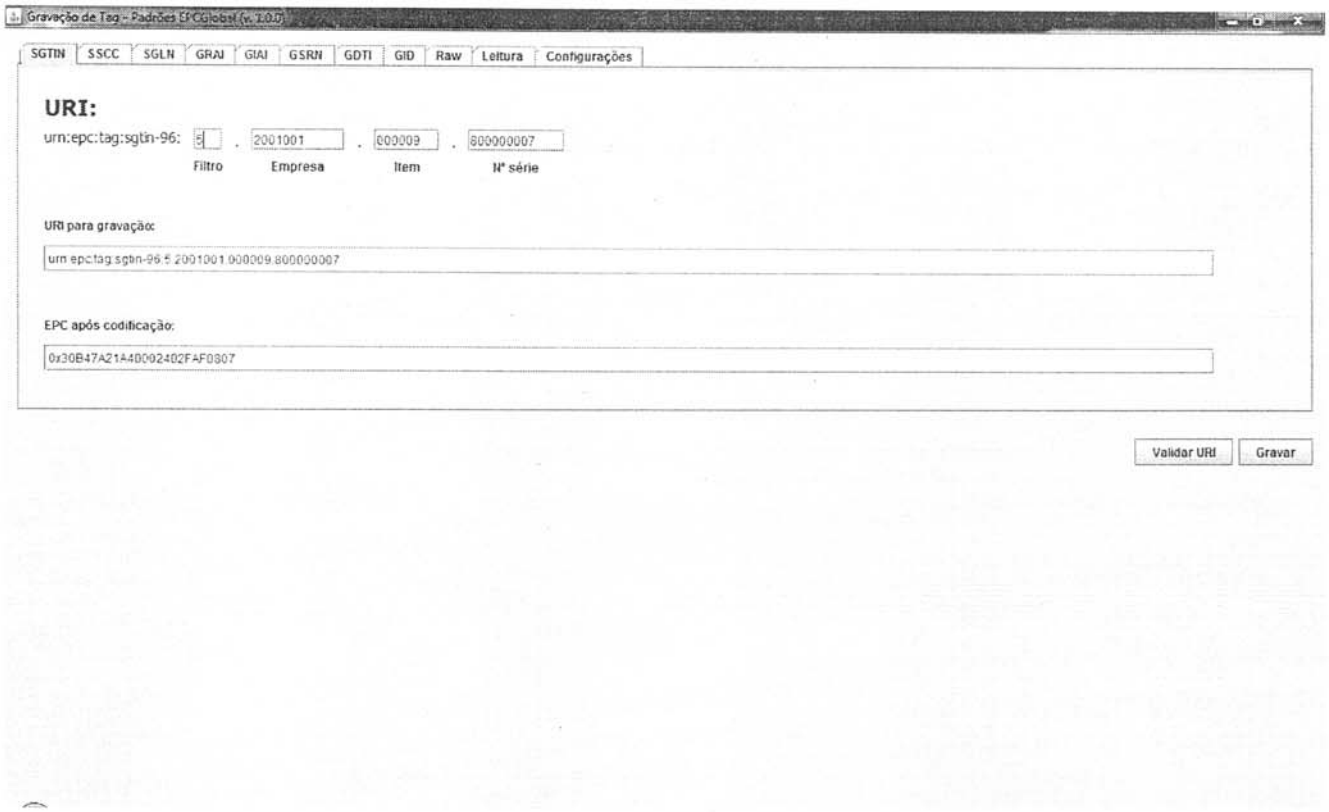

Figura 9. Informação Oculta com o Método 5

5.2 - Método 2 - Recuperação e Restauração de Dados RFID Indevidamente Manipulados usando Princípios Esteganográficos

Neste estudo, será apresentada uma solução para detectar dados indevidamente manipulados de uma coleção de etiquetas de RFID. A solução proposta está baseada nos conceitos derivados de ocultação de informações e esteganografia.

As manipulações citadas se referem a ataques contra a integridade das informações na etiqueta (ou sistema) de RFID, como manipulação indevida de dados. Os dados na etiqueta de RFID também podem ser indevidamente manipulados por leitores maliciosos. Considerando mais uma vez o cenário do armazém: se os dados na etiqueta foram manipulados indevidamente, isto pode resultar no despacho de itens errados do depósito. Por exemplo, se o leitor malicioso trocar as informações na etiqueta de RFID de Laranja para Maçã, então um pallet de

Maçãs pode ser despachado quando a intenção era despachar Laranjas. A manipulação indevida de dados (ou integridade) pode levantar questões como QoS (Quality of Service) (Qualidade do Serviço) e Confiança na logística e na cadeia de suprimentos e, portanto, precisa ser tratada.

A manipulação indevida de dados é uma das principais preocupações de segurança na aplicação de RFID. Qualquer solução que possa resolver esta questão, i.e., detectar se a manipulação indevida dos dados seria significativa, sempre que soluções grandes e complexas baseadas em RFID exigirem segurança e autenticidade.

Um bom exemplo seria a *e-logistics* e a *e-Warehouse*, em que *consórcios* de pequenas e médias empresas (PME) em todo o mundo trabalhem juntas para compartilhar negócios, clientes recursos e rastreamento de mercadorias para oferecer serviços just-in-time aos clientes. Um *ambiente colaborativo virtual,* assim, sobrevive com base na suposição de informações *confiáveis e autênticas*. A tecnologia de identificação automática fornecida pelo sistema RFID repousa fortemente na autenticidade das informações. Se esta informação for manipulada indevidamente, ela pode *destruir* a *reputação* da colaboração de *negócios* no ambiente virtual. Em redes de logística distribuídas e empresas estendidas, colegas colaboradores podem acusar uns aos outros de serem vulneráveis a ataques à segurança que podem *reduzir* a sua *fidedignidade*, e este ambiente colaborativo poderia, no fim, não se sustentar mais. Por exemplo, se os dados na etiqueta de RFID que representam a *'natureza da mercadoria'* fossem modificados de *'Mangas'* para *'Laranjas'*, as mercadorias erradas seriam enviadas aos clientes errados, o que, por sua vez, *afetaria* a *reputação* do prestador de serviços de logística. Estas ações poderiam ser organizadas por um concorrente em uma tentativa de frustrar a reputação de prestadores de logística.

Isto demonstra a necessidade de soluções que possam oferecer *detecção* de manipulação indevida. O trabalho inicial com respeito a manipulação indevida foi apresentado anteriormente pelos autores [65, 66, 67, 68]. No entanto, após realizar uma pesquisa detalhada da literatura

sobre soluções de segurança de RFID, não foi identificada uma solução para resolver a questão da recuperação de dados após sua manipulação indevida utilizando esteganografia. Isto oferece o argumento para apresentar a nossa solução proposta.

5.2.1 – Esquema proposto para a recuperação de Dados - RecDados

Nesta seção, será fornecida uma visão geral da solução RecDados, seguida da obtenção dos principais requisitos para o *RecDados*. Com base nestes requisitos, a lógica de projeto para o *RecDados* é esboçada onde será discutida as decisões básicas do projeto.

5.2.2 - Visão Geral da Solução RecDados

O RecDados oferece uma solução esteganográfica para detectar uma alteração e recuperar dados de RFID manipulados indevidamente. Na solução *RecDados* proposta, é utilizado um grupo de etiquetas para armazenar informação oculta de forma estaganográfica, ao contrário do sistema OcEDados, que trabalha com Tags RFID individuais. Também é presumido que somente os campos EPC Manager (EM) e a Object Class (OC) seriam manipuladas indevidamente. Isto é devido ao fato de ser presumido que o ataque intencional ou a tentativa de manipulação indevida foi causado por motivações econômicas, como custo de transporte reduzido ou admissão facilitada. E a única maneira de conseguir isto é modificar o componente do EM ou da OC da *estrutura de dados* de RFID. Por exemplo, a OC é usado para identificar de forma única um produto; se o produto A (Laranja) tem um custo de transporte mais barato em comparação com o produto B (Manga), o atacante pode tentar modificar a OC do produto B, para obter um benefício econômico. No entanto, se o atacante modificar o número de série (SN), que é utilizado para identificar um item de um produto específico, ele não pode obter um benefício econômico porque o

SN não representa um produto, mas apenas um identificador único de um item que pertence a um produto.

De acordo com os campos da Tabela 6, a estrutura de dados de RFID é composta de quatro partições – Cabeçalho, EPC Manager (EM), Object Class (OC) e Número de Série (SN). O EM identifica globalmente um fabricante de forma única, a OC identifica um produto fabricado por um fabricante, i.e., o EM e o SN identificam um item único que pertence a um produto. [65,66,67].

Para obter a recuperação de dados, o *RecDados* embute um padrão gerado pela combinação do EM e da OC, dentro da partição do SN de todas as etiquetas de RFID que pertencem a um determinado lote de produtos ou a uma consignação. Este padrão embutido é usado pelo módulo de recuperação de dados para gerar e recuperar os dados manipulados indevidamente. Isto é feito da seguinte maneira: é suposto que o padrão secreto tem um comprimento de n bits, embutimos m bits em cada etiqueta de RFID. Assim, um total de [*n/m*] de etiquetas RFID seria usado para ocultar o padrão secreto gerado usando-se o EM e a OC. Conforme mostrado na Tabela 10, a etiqueta de RFID com o número de série *'1111112345'* seria usada para ocultar o primeiro bit do padrão secreto. De forma semelhante, todos os outros bits no padrão secreto seriam adicionados às etiquetas de RFID restantes. Se o padrão secreto fosse representado por 7 bits, como '1010111', os bits correspondentes na etiqueta de RFID seriam modificações, conforme mostrado na Tabela 10. Utilizando o 3º bit mais significativo (MSB) do SN para ocultar o padrão secreto. Todos os números com um *negrito* e *sublinhado*, quando combinados, representariam o padrão secreto.

Quando o EM ou a OC forem manipulados indevidamente, podemos recuperar os valores originais recorrendo ao padrão embutido na partição do SN.

Presume-se que a funcionalidade para embutir o padrão secreto esteja presente no leitor de RFID que escreve a etiqueta, pois como não há

alteração de padrão a leitura é totalmente compatível com os sistemas atuais. Também se presume que o algoritmo de extração esteja disponível como um componente que pode ser conectado às aplicações de middleware de RFID. A solução *RecDados* seria uma parte do componente de detecção de manipulação indevida no middleware de RFID.

Tabela 10 – Amostra de Números de Série de RFID

Número de Série	SN Decimal
10101010101010111010101010101000	1111112345
10001010101010111010101010101001	1111112346
10101010101010111010101010101010	1111112347
10001010101010111010101010101011	1111112348
10101010101010111010101010101100	1111112349
10101010101010111010101010101101	1111112350
10101010101010111010101010101111	1111112351

Este componente toma dados de introdução da camada de gestão de dados, e então detecta se o EM ou a OC foram manipulados indevidamente. Se tiver sido manipulado indevidamente, então o padrão secreto é extraído usando-se todas as etiquetas de RFID usadas para embutir o segredo. Os dados manipulados indevidamente podem então ser restaurados e propagados para os níveis de integração da aplicação na arquitetura do middleware.

5.2.3 - Requisitos para a Solução RecDados

Para auxiliar nas questões de manipulação indevida e recuperação de dados, os requisitos a seguir são estabelecidos para a solução RecDados proposta.

1. *Comprimento do Padrão Secreto:* O comprimento do padrão secreto deve ser menor do que ou igual ao número total de bits disponíveis em

um jogo de etiquetas de RFID que podem ser utilizadas para embutimento. Ele não deve ocupar muito espaço porque a quantidade de dados que podem ser armazenados em uma etiqueta é muito limitada.

2. *Geração do Padrão Secreto:* As entradas para a geração da marca d'água devem estar disponíveis na própria etiqueta.
3. *Locais de Embutimento:* O padrão secreto deve ser embutido na partição do número de série.
4. *Recuperação de Dados:* A algoritmo deve ser capaz de recuperar dados manipulados indevidamente após a manipulação indevida de dados ter sido confirmada usando-se o RecDados.
5. *Arquitetura Plug-n-Play:* A solução proposta deve ser projetada de forma que possa ser facilmente conectada nas aplicações de middleware de RFID existentes.

5.2.4. - Lógica de Projeto para a Solução RecDados

O fundamento teórico para o *RecDados* é proposto para atender os requisitos esboçados anteriormente. As decisões de projeto a seguir são propostas nesta solução.

1. O tamanho do padrão secreto é de *cinquenta e dois bits*. Os 52 bits representam os 28 bits do EM e 24 bits da OC, concatenados. Presumindo-se que cada bit seja embutido em uma etiqueta RFID, o RecDados exigiria 52 etiquetas de RFID. O número mínimo de etiquetas necessárias é dado por 52/N, onde N é o numero de bits que serão armazenados em cada etiqueta. O numero mínimo e etiquetas é de 2, pois o campo de numero de série tem 36 bits e é preciso no mínimo 52. (Req. 1)
2. O padrão secreto é gerado a partir dos dados armazenados no EM e na OC. (Req. 2)

3. O padrão secreto é embutido na partição do *número de série* porque este oferece bits suficientes (36 bits), que podem ser utilizados para o embutimento. (Req. 3)
4. O padrão secreto seria extraído do jogo de etiquetas de RFID para recuperar os dados manipulados indevidamente. (Req. 4)
5. O algoritmo é projetado como um componente; assim, ele pode ser facilmente conectado em uma aplicação de middleware existente. (Req. 5)

5.2.5 – Fundamento Teórico do sistema RecDados

A estrutura proposta é mostrada nas Figuras 10, 11 e 12. Ela pode ser decomposta em quatro diferentes estágios:

5.2.5.1 - Geração do Padrão Secreto

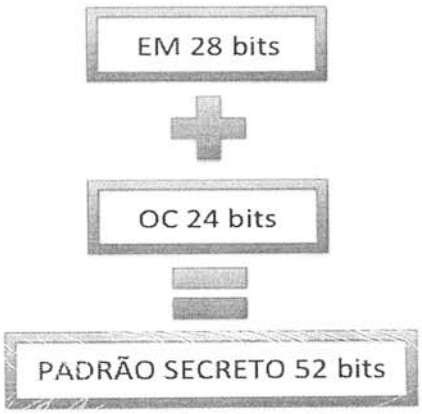

Figura 10 - Geração do Padrão Secreto

Entradas: EPC Manager (EM) e Object Class (OC)
Saída: Padrão Secreto

O padrão secreto é gerado conforme mostrado na Figura 11. Contatenamos um exemplo de EM e OC, que é uniforme em toda uma categoria dada de produtos, resultando em uma string de 52 bits. Quando

o padrão for gerado, é necessário identificar a localização para o embutimento. Agora será discutido como é selecionada a localização adequada para embutir o padrão secreto.

5.2.5.2. Seleção da Localização do Embutimento

Anteriormente, foi mencionado que o padrão secreto deveria ser embutido na partição do número de série da etiqueta de RFID. Nesta seção, será fornecida a razão para esta seleção.

O princípio básico da esteganografia (ou ocultação de informações) é que é necessário algum espaço redundante dentro do sinal do host que possa ser modificado para embutir o padrão secreto. Neste caso, a etiqueta de RFID é o sinal de host e é desejado identificar o espaço redundante. Para fazer isto, será investigada a estrutura de dados de RFID.

Com base nessa investigação, foi determinado que a partição do número de série dentro das etiquetas de RFID pode oferecer uma quantidade razoável de espaço redundante para o embutimento da frágil marca d'água. Esta seleção é atribuída aos fatos a seguir:

O *Cabeçalho* é completamente utilizado para identificar a chave EAN.UCC e o esquema de partição. Assim, não há espaço redundante, portanto, não há possibilidade de embutir a informação.

O *EPC Manager* é utilizado para identificar de forma exclusiva o fabricante. Assim, a partição também não oferece qualquer espaço redundante para o embutimento porque isto pode ser decidido pelo padrão da indústria e o fabricante tem o pouco controle sobre isto.

A *Object Class* é utilizada para identificar o produto fabricado pelo fabricante. Ela pode seguir alguma taxonomia de convenção de produto em que os *primeiros* dois dígitos podem representar a classificação daquele produto; os dois próximo podem ser a idade do produto, e assim por diante. Assim, modificar qualquer um destes dados pode interferir com o

padrão da indústria existente. Como resultado, esta partição também não oferece espaço suficiente para embutir a marca d'água.

O *Número de Série*, que é a última partição, é utilizado para identificar um item de forma exclusiva, que pertence a uma Object Class em particular. Sobre este, o fabricante pode decidir à vontade, sem violar qualquer padrão de indústria existente. Consequentemente, este oferece suficiente espaço redundante para embutir o padrão secreto. Enquanto isso, o comprimento desta partição é de 36 bits (em EPC96), que oferece espaço suficiente para acomodar o padrão secreto se for utilizado pelo menos 2 tags. Portanto, este se torna o candidato mais adequado para embutir padrão secreto e, assim, foi escolhida esta partição para o embutimento. Agora será discutido em detalhe o algoritmo de embutimento e extração.

5.2.5.3. Embutimento do Padrão Secreto

Entradas: Número de Série (SN)
Padrão Secreto (SP)
Número de Etiquetas de RFID (N)
Comprimento do Padrão Secreto (n)
Número de bits embutidos em uma etiqueta (M)
Locais de Embutimento (L)

Saídas: Etiqueta de RFID resistente à Manipulação Indevida (W)

Etapa 1: Carregar o Padrão Secreto. Na primeira etapa, o leitor de RFID carrega o padrão secreto na sua memória. O padrão secreto pode ser gerado pelo leitor de RFID ou pelo middleware de RFID. É presumido que o leitor tenha a funcionalidade de gerá-lo.

Etapa 2: Selecionar o local de embutimento dentro da partição do número de série. A partição do SN tem 36 bits; selecionamos m+1 bits

consecutivos da partição do SN, onde (0<m<36), para embutir os primeiros M bits do padrão secreto. Será denominado este local no SN como L.

Etapa 3: Embutimento do primeiro jogo do padrão secreto. Os m bits do padrão secreto são agora embutidos na partição do SN da etiqueta de RFID. O processo de embutimento do padrão secreto em 4 tags é mostrado na Figura 11.

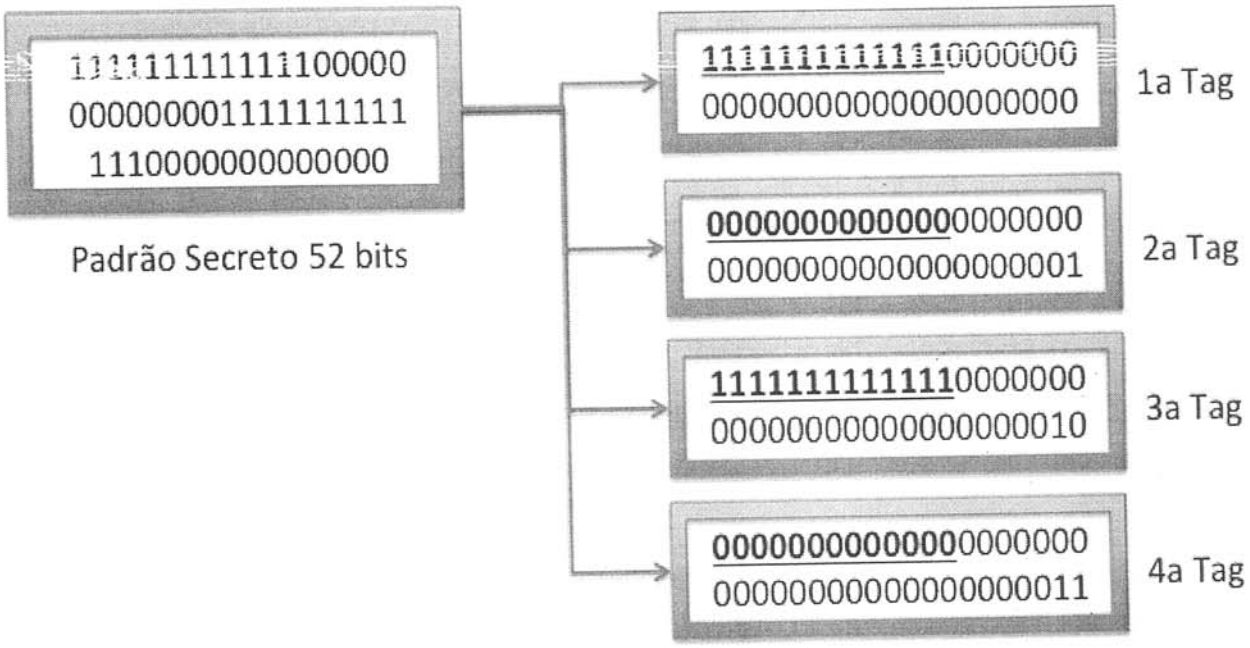

Figura 11 - Algoritmo de Embutimento do Padrão Secreto

A figura 11 mostra o processo de embutimento do padrão secreto em múltiplas etiquetas de RFID. Aqui, é presumido que o comprimento do padrão secreto é de 52 bits. Também é considerado o número total de etiquetas de RFID como sendo 4 neste caso, portanto, será embutido treze bits secretos em cada etiqueta de RFID. É assim que o padrão secreto é embutido na etiqueta. Agora será explicado o algoritmo de recuperação de dados.

5.2.5.4 - Extração do Padrão Secreto para a Recuperação de Dados

Entradas Número de Série (SN)
Local de Embutimento (L)
Local da Paridade (P)

Saída Dados Recuperados

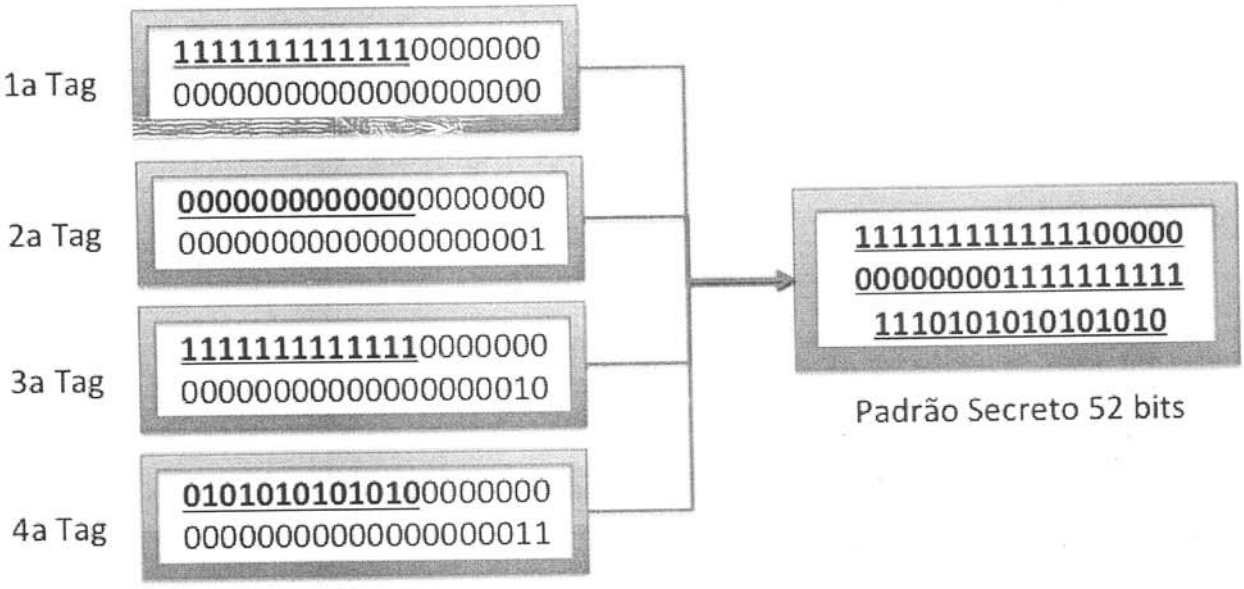

Figura 12 - Algoritmo de Extração do Padrão Secreto

A primeira tarefa é verificar se os dados contidos nos campos EM e OC das etiquetas que compõe o grupo foram indevidamente manipulados. Para verificar isto, é extraída a informação oculta no conjunto de etiquetas utilizando o método descrito na figura 12. Como se vê nesta figura, os 27 bits menos significativos formam não apenas o próprio número de série mas também são utilizados para indicar a ordem de reconstrução da informação original que foi oculta nas tags.

Esta informação oculta no grupo de etiquetas será separada em seus dois componentes, sendo os primeiros 28 bits referentes ao EM e os 24 bits restantes ferentes ao OC. Caso alguma das etiquetas do grupo apresente variação entre os valores de seus campos EM e OC e os valores de EM e OC retirados do padrão secreto, é indicativo de que ocorreu

alteração não-autorizada dos dados da etiqueta. Com a alteração detectada, podemos restaurar a informação correta na(s) etiqueta(s) atingida(s), bastando para isso reescrever as etiquetas de RFID com os dados recuperados.

5.3 Discussão e validação

Neste estudo, foi proposta uma solução para recuperar dados a partir de etiquetas de RFID indevidamente manipuladas. Isto foi obtido pelo embutimento de um padrão secreto em um grupo de etiquetas de RFID, que foram anexadas a um conjunto de etiquetas de um grupo de produtos.

Foi demonstrado como podemos gerar o padrão secreto usando o EM e a OC e embuti-lo no SN. A solução proposta tem limitações, como só funcionar em casos específicos e depender para sua segurança da obscuridade do algoritmo escolhido. Mas a técnica também possui muitas vantagens; além de ser usada para recuperação de dados, também pode ser usada para comunicação secreta. Por exemplo, esta abordagem pode ser usada para embutir algum outro tipo de informação como dados de fatura ou qualquer outra informação que tenha que ser compartilhada entre duas partes em comunicação que trocam mensagens.

O algoritmo também permite a utilização de etiquetas simples padrão EPCGlobal96, de custo reduzido, e demanda poucos recursos computacionais para ser executado.

Enquanto o número de série não tiver sido indevidamente manipulado, a técnica proposta pode recuperar exatamente os dados indevidamente manipulados que, neste caso, são o EM e a OC. Mas, se o SN for indevidamente manipulado, para corresponder ao SN de outro produto (com custo de transporte inferior), os dados ocultos serão perdidos.

Neste caso é recomendado que o fabricante deve seguir um padrão pelo qual os primeiros n bits do SN sejam uniformes em toda a linha de produtos. Estes n bits então seriam utilizados para a recuperação de dados com o uso de ocultação de informações ou esteganografia. Assim, é possível recuperar dados no caso de o SN também ter sido indevidamente manipulado.

6. CONCLUSÃO E TRABALHOS FUTUROS

Neste estudo, foi proposta uma solução para recuperar dados a partir de etiquetas de RFID indevidamente manipuladas. Foi concluído que a maior parte do trabalho de pesquisa recente sobre segurança de RFID foi efetuado nas áreas de anonimato, confidencialidade e autenticidade.

A integridade dos dados e a recuperação dos dados não foram abordadas em detalhe. Assim, foi proposta uma estrutura de recuperação de dados pela introdução de uma camada na arquitetura de middleware de RFID existente. Também foi proporcionada uma descrição detalhada do algoritmo de recuperação de dados, que pode recuperar os dados de etiquetas RFID indevidamente manipulados nos campos EM e a OC.

A esteganografia vem sendo cada vez mais procurada e utilizada nos dias de hoje. Ela possui numerosas aplicações, e talvez a mais importante delas seja a segurança da informação, já que, com a esteganografia, as mensagens ficam ocultas nos meios usados, e a informação passa desapercebida por terceiros.

As técnicas esteganográficas não são perfeitas; a esteganálise está sempre buscando seus erros a fim de descobrir os algoritmos usados. Porém, mesmo assim, a esteganografia mostrou-se ativa em esconder informações que não podem cair acidentalmente nas mãos de terceiros. Porém, devido ao pouco espaço disponível para armazenar dados em uma etiqueta RFID, não é possível utilizar todo o potencial da esteganografia em sistemas RFID.

Mas mesmo com um leque de opções limitados, o uso de esteganografia cria um obstáculo a mais contra indivíduos em busca de acesso indevido a informações, e com custos reduzidos em função da utilização de etiquetas e leitores padrão.

No futuro todas as organizações adotarão a tecnologia RFID, em busca da melhora na rapidez dos procedimentos e o incremento no

processamento dos dados. Dentro deste contexto, as técnicas esteganográficas podem ser usadas para aumentar a segurança e demonstram ser um campo profícuo de pesquisa e aplicações no futuro, especialmente se agregadas à técnicas de ECC.

REFERÊNCIAS

[1] Singh, S. "O livro dos códigos". Rio de Janeiro: Record, 2001.

[2] Kipper, G. "Investigator's guide to steganography". Boca Raton: Auerbach Publications, 2004.

[3] Artz, D. "Digital Steganography: hiding data within data". *IEEE Internet Computing*, vol. 5-3, Maio-Jun 2001, pp. 75-80.

[4] Czapski, C. "Prepare-se para enormes ganhos de eficiência". Capturado em: www.revistadistribuicao.com.br, Nov 2010.

[5] Bitko, G. "RFID in the retail sector: a methodology for analysis of policy proposals and their implications for privacy, economic efficiency and security". Santa Monica: RAND Corporation, 2007. Capturado em: http://www.rand.org/pubs/rgs_dissertations/RGSD209, Dez 2010.

[6] Provos, N.; Honeyman, P. "Hide and seek: an introduction to steganography". *IEEE: Security & Privacy*, vol. 1-3, Maio-Jun 2003, pp. 32-44.

[7] Ramalho Jr, J.G.; Amorim, E. S. "Esteganografia: integridade, confidencialidade e autenticidade". São Bernardo do Campo: FTT, 2008.

[8] Cox, I.; Miller, M.; Bloom, J.; Fridrich, J.; Kalker, T. "Digital watermarking and steganography". Morgan Kaufmann Publishers, 2007, 2nd ed.

[9] Fonseca, T. C. "Esteganografia". Capturado em: http://www.gta.ufrj.br/grad/07_2/thiago_castello/index.html, Dez 2010.

[10] EPC GLOBAL. "Ratified Specification EPCglobal Tag Data Standards Version 1.5". Capturado em: http://www.epcglobalus.org, Out 2010.

[11] Ker, A. D. "Steganalysis of LSB matching in grayscale images". *IEEE Signal Processing Letters*, vol. 12-6, Jun 2005, pp. 441–444.

[12] Fridrich, J.; Goljan, M.; Hogea, D.; Soukal, E. D. "Quantitative steganalysis of digitalimages: estimating the secret message length". *Multimedia Systems*, vol. 9-3, 2003, pp. 288-302.

[13] Bauer, F. L. "Decrypted secrets: methods and maxims of

cryptology". New York: Springer-Verlag, 2004, 3rd ed.

[14] Arnold, M.; Schmucker, M.; Wolthusen, S. D. "Techniques and applications of digital watermarking and content protection". Massachusetts: Artech House, 2009.

[15] Bohme, R.; Westfeld, A. "Exploiting preserved statistics for steganalysis". In: Sixth Workshop on Information Hiding, 2004, pp. 82-96.

[16] Lyu, S.; Farid, H. "Steganalysis using higher-order image statistics". *IEEE Transactions on Information Forensics and Security*, vol. 1-1, 2006, pp. 111–119.

[17] Julio, E. P.; Brazil, W. A.; Ibuquerque, C. N. "Esteganografia e suas aplicações". In: Anais do Simpósio Brasileiro de Segurança da Informação – SBSEG, 2007, pp. 55-75.

[18] Lu, P.; Luo, X.; Tang, Q.; Shen, E. L. "An improved sample pairs method for detection of LSB embedding". In: Proceedfings 6th Information Hiding Workshop, 2004, pp. 116–127.

[19] Ker, A. "Quantitative evaluation of pairs and RS steganalysis". In: Proceeedings of the VI Security, Steganography, and Watermarking of Multimedia Contents, 2006, pp. 83–97.

[20] Popa, R. "An analysis of steganography techniques". Dissertação de Mestrado, The Polytechnic University of Timisoara, 2002, pp. 56-59.

[21] Coutinho, P. S. "Técnicas modernas de esteganografia". Capturado em: http://www.gta.ufrj.br/grad/08_1/estegano/TcnicasModernas.html, Dez 2010.

[22] Marvel, L.; Boncelet, C.; Retter, J. "Spread spectrum image steganography". *IEEE Transactions on Image Processing*, vol. 8-8, Ago 1999, pp. 1075-1083.

[23] Wayner, P. "Disappearing cryptography: information hiding: steganography and watermarking". San Francisco: Morgan Kaufmann Publishers Inc., 2002, 2nd ed.

[24] Fridrich, J.; Long M. "Steganalysis of LSB encoding in color images". In: 2000 IEEE International Conference on Multimedia and Expo, 2000, pp. 1279-1282.

[25] Gonzalez, R. C.; Woods, R. E. "Digital image processing". Boston: Prentice-Hall, 2002, 2nd. ed.

[26] Dumitrescu, S.; Wu, X.; Wang, E. Z. "Detection of LSB steganography via samplepair analysis". *IEEE transactions on Signal Processing*, vol. 51-7, 2004, pp. 1995–2007.

[27] Salomon, D. "Data compression: the complete reference". Nova Iorque: Springer, 2000, 2nd ed.

[28] Julio, E. P.; Brazil, W. A.; Ibuquerque, C. N. "Esteganografia e suas aplicações". In: Anais do Simpósio Brasileiro de Segurança da Informação – SBSEG, 2007, pp. 199-202.

[29] Kessler, G. C. "An Overview of Steganography for the Computer Forensics Examiner". *Forensic Science Communications*, vol. 6, Jul 2004.

[30] Petitcolas, F. A. P.; Anderson, R. J.; Kuhn, M. G. Information hiding: a survey. In: Proceedings of the IEEE special issue on protection of multimedia content, 1999, pp. 1062-1078.

[31] Rocha, A. R.; Costa, H. A. X.; Chaves, L. M. "Camaleão: um software para segurança digital utilizando esteganografia", Monografia, Departamento de Ciências da Computação e Departamento de Ciências Extas, Universidade Federal de Lavras, 2003.

[32] Provos, N.; Honeyman, P. "Detecting Steganographic Content on the Internet", CITI Technical Report, 2001, pp. 1-11.

[33] Chang, C-C.; Chen, T-S.; Chung, L. Z. Z. "A steganographic method based upon jpeg and quantization table modification". *Information Sciences - Informatics and Computer Science: An International Journal - Special issue: Intelligent multimedia computing and networking*, vol. 141-1/2, Mar 2002, pp. 123-138.

[34] Pfitzman, P. A. B. "Information hiding terminology". *Information Hiding, Springer Lecture Notes in Computer Science*, vol. 4437, Jul 2006, pp. 1-4.

[35] Richardson, I. E. "264 and mpeg-4 video compression". New York: John Wiely & Sons Inc., 2003.

[36] Buccigrossi, R. W.; Simoncelli, E. P. "Image compression via joint statistical characterization in wavelet domain". *IEEE Transaction on Image Proceedings*, vol. 8-12, Dez 2000, pp. 18.

[37] Margi, C. B.; Bressan, G. "Um mecanismo para distribuição segura de vídeo mpeg". Capturado em: http://larc.usp.br/, Maio 2010.

[38] Rivest, R. "Rfc1321: the md5 message-digest algorithm". Capturado em: http://tools.ietf.org/html/rfc1321, Dez 2010.

[39] Burr, E. W. "Cryptographic hash standards: where do we go from here?" *IEEE Security and Privacy*, vol.4-2, Mar-Abr 2006, pp. 88-91.

[40] Rijmen, P. B. V. "The whirlpool hashing function". In: First open NESSIE Workshop, 2003, pp. 8.

[41] Julio, E. P.; Brazil, W.; Albuquerque, C. "Esteganografia e suas aplicações". In: VII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais, 2007, pp. 54-102.

[42] Roue, B.; Chassery, J. "Improving LSB steganalysis using marginal and joint probabilistic distributions". In: Proceedings of the 2004 Workshop on Multimedia and Security, 2004, pp. 75-80.

[43] Fridrich, J.; Pevn`Y, T.; Kodovsky, J. "Statistically undetectable jpeg steganography: dead ends challenges, and opportunities". In: Proceedings of the 9th Workshop on Multimedia & Security, 2007, pp. 3-14.

[44] Sallee, P. "Model-based methods for steganography and steganalysis". *International Journal of Image and Graphics*, vol. 5-1, Jan 2005, pp. 167–189.

[45] Kahn, D. "The Codebreakers: the story of secret writing". New York: Ed. New York, 1967, pp. 175-177.

[46] Fridrich, J.; Goljan, M.; Hogea D. "Attacking the outguess". In: Proceedings of the ACM Workshop on Multimedia and Security, 2002.

[47] Battezzati, L; Hygounet, J-L. "RFID: Identificazione automatica a radiofrequenza". Milan: Ulrico Hoepli Editore, 2006, 2nd ed.

[48] Pinheiro, J. M. S. "RFID: Identificação por Rádio Freqüência". Capturado em: http://www.projetoderedes.com.br/artigos/artigo_identificacao_por_radiof requencia.php, Fev 2011.

[49] Baker, S. "RFID technology review: Management briefing: The benefits of RFID". *ABI/INFORM Global*, Nov 2006, pp. 2.

[50] Hartman, L. R. "Comparing HF and UHF RFID technologies: the stakes couldn't be higher for consumers, pharmaceutical manufacturers, distributors and retailers, as up to seven percent of all drugs in the

international supply chain may be counterfeit. To combat the problem, the pharmaceutical industry is looking to radio frequency identification (RFID) as a primary solution. (smart packaging)". Capturado em: http://www.highbeam.com/doc/1G1-125335878.html, Set 2011.

[51] Angeles, R. "Rfid Technologies: supply-chain applications and implementation issues". *Information Systems Management*, vol. 22-1, Win 2005, pp. 51-56.

[52] Bernardo, C. G. "A Tecnologia RFID e os benefícios da etiqueta inteligente para os negócios". Capturado em: http://www.unibero.edu.br/download/revistaeletronica/Set04_Artigos/A%20Tecnologia%20RFID%20-%20BSI.pdf, Dez 2010.

[53] Finkenzeller, K. "RFID Handbook: fundamentals and applications in contactless smart cards and identification". New York: John Wiley & Sons, 2003, 2nd ed.

[54] AUTO-ID CENTER OF MIT. Massachusetts Institute of Technology. "860 MHz – 930 MHz Class I Radio Frequency Identification Tag Radio Frequency & Logical Communication Interface Specification Candidate Recommendation, Version 1.0.1", Technical Report, Massachusetts Institute of Technology, 2002.

[55] Viana, G. A. "RFID é nova onda em radiofrequência". Capturado em: http://www.sucesues.org.br/documentos/index.asp?cod_noticia=484, Maio 2010.

[56] Kharrazi, M.; Sencar, H.; Memon N. "Image steganography: concepts and practice". In: Kalker, T. (Editor). IWDW. Singapore: Institute for Mathematical Sciences, National University of, 2004, pp. 35-49.

[57] Cox, I. J.; Kalker, T.; Pakura, G.; Scheel, M. "Information transmission and steganography". In: 4th International Workshop on Digital Watermarking, 2005, pp. 15-29.

[58] Shannon, C. "Communication Theory of Secrecy Systems". *Bell System technical Journal*, vol. 28-4, 1954, pp. 656–715.

[59] Simmons, G. J. "The prisoners' problem and the subliminal channel". In: Advances in Cryptology: Proceedings of CRYPTO'83, 1984, pp. 51–67.

[60] Givner-Forbes, R. "Steganography: information technology in the service of Jihad". Capturado em: http://www.pvtr.org, Nov 2011.

[61] J. Fridrich, J.; Goljan, M.; Hogea D. "Attacking the outguess". In: Proceedings of the ACM Workshop on Multimedia and Security, 2002.

[62] *Anderson, R.* "Stretching the limits of steganography". *Computer Science*, vol. 1174, 1996, pp. 39-48.

[63] Cancelli G.; Barni, M. "MPSteg-color: a new steganographic technique for colorimages". In: 9th International Workshop, 2007, pp. 1-15.

[64] Fridrich, J.; Goljan, M.; Lisonek, P.; Soukal, D. "Writing on wet paper". *IEEE Transactions on Signal Processing*, vol. 53-10, Out 2005, pp. 3923-3935.

[65] Potdar, V.; Wu, C.; Chang, E. "Tamper detection for ubiquitous RFID enabled supply chain". In: Proceedings of the International Conference on Computational Intelligence and Security (CIS05), 2005, pp. 273-278.

[66] Potdar, V.; Wu, C.; Chang, E. "E-Supply Chain Technologies and Management", Hershey: IDEA Group Reference, 2007.

[67] Potdar, V.; Wu, C.; Chang, E. "Tamper Detection in RFID tags using Fragile Watermarking". In: Proceeding of the 10th IEEE International Conference on Industrial Technology (ICIT06), 2006, pp. 2846-2852.

[68] Potdar, M.; Chang, E; Potdar, V. "Applications of RFID in Pharmaceutical Industry". In: Proceeding of the 10th IEEE International Conference on Industrial Technology (ICIT06), 2006.

[69] Unander, T. "System Integration of Electronic Functionality in Packaging application", Doctoral Thesis, Mid Sweden University, Suécia, 2011, 97p.

[70] Nejad, M. B. "Ultra Wideband Impulse Radio for Wireless Sensing and Identification", Doctoral Thesis in Electronic and Computer Systems, Royal Institute of Technology, School of Information and Communication Technology, Suécia, 2009, 88p.

[71] Unander, T. "Characterization of low cost printed sensors for smart packaging", Thesis for the degree of Licentiate, Department of Information Technology and Media, Mid Sweden University, 2008, 74p.

[72] Urciuoli, L. "Security in physical distribution networks: A Survey study of Swedish transport operators", Thesis for Doctorate in Engineering degree, Department of Industrial Management and Logistics, Division of Engineering Logistics, Lund University, 2010, 236p.

[73] Ringsberg, H. "Traceability in food supply chains", Licentiate thesis, Department of Design Sciences, Division of Packaging Logistics, Lund University, 2011, 155p.

[74] Herzer, G. "Magnetic materials for electronic article surveillance". *Journal of Magnetism and Magnetic Materials*, 2003, pp. 254-255 e 598-602.

[75] Finkenzeller, K. "RFID-Handbook: fundamentals and applications in contactless smart cards, Radio Frequency Identification and near-field communication". Wiley & Sons LTD, 2010, 3rd ed.

[76] Gandino, F.; Montrucchio, B.; Rebaudengo, M. "Tampering in RFID : a survey on risks and defenses". *Journal Mobile Networks and Applications*, vol. 15-4, 2010, pp. 502-516.

[77] Mohan, M.; Potdar, V.; Chang, E. "Recovering and restoring tampered RFID data using steganographic principles". In: IEEE International Conference on Industrial Technology ICIT, 2006, pp. 2853-2859.