https://eventos.utfpr.edu.br//sicite/sicite2018

Esteganografia e esteganálise: fundamentos e o método LSB

Steganography and steganalysis: fundamentals and the LSB method

Cristiane Klein
criis.klein@gmail.com
Universidade Tecnológica Federal do Paraná, Curitiba, Paraná, Brasil

Fabio Antonio Dorini
fabio.dorini@gmail.com
Universidade Tecnológica Federal do Paraná, Curitiba, Paraná, Brasil
Departamento de Matemática.

RESUMO

A esteganografia tem o objetivo de transmitir uma mensagem sem que os outros percebam, e a esteganálise tem o objetivo de desmascará-la. O método mais trivial de esteganografia é o LSB, que consiste em trocar os bits menos significativos de um objeto de cobertura pelos da mensagem. Este método pode ser descoberto pelo Histogram Attack, um método de esteganálise que utiliza o comparação de histogramas. O objetivo deste estudo é a Iniciação nas áreas de estudo esteganografia e esteganálise, através da literatura e aplicação de métodos considerados básicos. Foram escolhidas 20 imagens da base BOSSbase e para cada uma destas foram geradas quatro mensagens semi-aleatórias, cada mensagem com um tamanho diferente. Foi determinado um caminho também semi-aleatório que deve-se percorrer dentro da imagem na aplicação da esteganografia. Após isto, o método Histogram Attack foi aplicado. Pode-se perceber que quanto maior for a porcentagem que a mensagem ocupa dentro do objeto, melhores são os resultados do Histogram Attack. A acurácia geral do experimento foi de 62,5%.

PALAVRAS-CHAVE: Esteganografia. Esteganálise. LSB.

ABSTRACT

Steganography aims to convey a message without the others noticing, and steganalysis aims to unmask it. The most trivial method of steganography is LSB, which consists of exchanging the least significant bits of a cover object with those of the message. This method can be discovered by the Histogram Attack, a steganalysis method that uses histogram comparison. The objective of this study is the initiation in the study areas steganography and steganalysis, through the literature and application of methods considered basic. Twenty images of the base BOSSbase were chosen, for each of them four semi-random messages were generated, each message with a different size. It was also determined a semi-random path that must be traversed within the image in the application of steganography. After this, the Histogram Attack method was applied. It can be seen that the higher the percentage that the message occupies within the object, the better the Histogram Attack results.The overall accuracy of the experiment is 62.5%.

KEYWORDS: Steganography. Steganalysis. LSB.

INTRODUÇÃO

Recebido: 31 ago 2018.
Aprovado: 04 out 2018.

A esteganografia surgiu da necessidade de transmitir uma mensagem à um destinatário sem que terceiros percebessem que a mensagem sequer existe. A palavra esteganografia vem do grego: estegano - esconder, grafia - escrita. E bem como seu significado indica, esteganografia são técnicas utilizadas para esconder algum tipo de mensagem (escrita, imagem, áudio, etc.) em um objeto de cobertura. Em aplicações digitais este objeto pode ser uma imagem digital, áudio, vídeo e outros tipos de arquivos. Quando a mensagem é embutida no objeto de cobertura, tem-se um estego-objeto, pronto para ser entregue ao destinatário.

A mensagem só pode ser desvendada com uma chave de acesso (*stego key*) combinada entre o remetente e o receptor. Todavia, se uma pessoa de fora conseguir identificar que existe uma mensagem escondida, a esteganografia já é considerada quebrada (FRIDRICH, 2009).

A esteganálise por sua vez, tem a função de detectar se o objeto analisado carrega uma mensagem secreta ou não. Surgiu como adversário da esteganografia pois tendo em vista que mensagens secretas nem sempre têm boa intenção, é necessário que exista maneira de quebrá-la se preciso.

O objetivo deste projeto é a iniciação nas áreas de estudo esteganografia e esteganálise, através do estudo da literatura e da aplicação de métodos considerados básicos – LSB method e Histogram Attack.

LEAST SIGNIFICANT BIT

O método Least Significant Bit - ou Bit Menos Significativo - oculta a mensagem através da modificação de bits menos significativos do objeto digital de cobertura. Uma mensagem *m[i]* contém *i* bits que precisam ser inseridos no objeto de cobertura, precisa que este objeto tenha no mínimo *i* elementos. Se o objeto de cobertura for uma imagem colorida, esta irá conter 3 canais de cores (cada um dos canais representa uma cor base, e seu valor representa a intensidade que esta cor possui na imagem. O Sistemas de representação de cores em imagens digitais que é mais utilizado é o de adição, RGB - Red, Green, Blue - (ROCHA, 2011)), portanto cada pixel pode esconder até 3 bits da mensagem.

A escolha do caminho que a mensagem vai percorrer dentro da imagem para esconder cada elemento da mensagem é um passo muito importante. Uma mensagem que é escondida em sequência linear é pouco segura. Para maior dificuldade de descoberta pode-se escolher esconder a mensagem em locais da imagem que apresentam maior ruído, ou selecionar locais semi-aleatórios de maneira pré-estabelecida pelos interessados.

Outra coisa que deve ser levada em consideração é o tamanho da mensagem em relação à imagem de cobertura. A taxa de incorporação da imagem é determinado por:

$$\alpha = m/n, \quad (1)$$

sendo *m* o número de bits da mensagem e *n* o número de elementos da imagem de cobertura. Existem alguns métodos de esteganálise – como o Histogram Attack – que tem acurácia relevante apenas em estego-imagens com próximo à 1,0, logo, escolher uma imagem que diminua este fator pode ser decisivo entre ser descoberto ou não.

HISTOGRAM ATTACK

O método de esteganálise Histogram Attack utiliza o teste qui-quadrado de Pearson para comparação de histogramas. Este teste verifica se os valores de escala cinza de índices pares estão seguindo a distribuição esperada, fazendo o somatório *S* das comparações entre os valores de escala cinza par com a média entre este mesmo valor e o próximo valor ímpar. O valor de *S* tende a ser pequeno se os valores seguirem o esperado, e grande se os valores divergirem. Para analisar se uma imagem possui uma mensagem embutida basta definir um valor limiar γ, de modo que será considerada uma estego-imagem se $S < \gamma$.

Este método apresenta bons resultados quando a taxa de incorporação $\propto$ está próximo à 1,0, ou seja quando a mensagem embutida ocupa a maior parte da imagem de cobertura. Em casos que o $\propto$ é pequeno porém o Path da mensagem é sequencial este método também apresenta bons resultados (FRIDRICH, 2009).

Neste estudo foi aplicado o Histogram Attack em caso de mensagens com $\propto$ variados e *Path* aleatório, a título de verificação empírica dos resultados.

MATERIAS E MÉTODOS

Para aplicação dos métodos estudados foram escolhidas 20 imagens do BOSSbase – uma base de imagens com 9074 imagens 512x512 em escala cinza no formato pgm (COELHO; BENTO, 2004). Para cada imagem, foram geradas quatro mensagens *m* semi-aleatórias, sendo estas em binário, ou seja cada *m[i]* recebe o valor de 0 ou 1 – sem se preocupar com uma mensagem significativa ou coerente, visto que a funcionalidade da mensagem é puramente ser utilizada neste experimento. E quatro caminhos *Path* também semi-aleatórios, sendo *Path* uma lista de tuplas que contém a sequência de coordenadas dentro da imagem que a mensagem deve seguir no processo de embutir a mensagem *m*. Os quatro casos possuem diferentes tamanhos, sendo a primeira mensagem e caminho gerados equivalentes a 25% da imagem ($\propto$ = 0,25), a segunda 50% da imagem ($\propto$ = 0,5), a terceira 75% da imagem ($\propto$ = 0,75) e a quarta 100% da imagem ($\propto$ = 1,0).

O método de esteganografia utilizado foi o LSB, previamente apresentado. Após o processo de embutir as mensagens, foi aplicado, à cada uma das estego-imagens resultantes, o método de esteganálise Histogram Attack. Ambas as implementações foram feitas em linguagem de programação Python.

RESULTADOS E DISCUSSÕES

O método LSB é considerado bem sucedido se a estego-imagem cumprir a missão de esconder uma mensagem e não deixá-la aparente.

O método Histogram Attack é analisado a partir do limiar γ igual à 126, determinado com base nas informações da amostra de maneira que nenhuma imagem de cobertura fosse considerada estego-imagem. É considerado bem sucedido em cada caso se o método detectar a existência de uma mensagem escondida. O parâmetro definido para avaliação dos resultados gerais deste método é o de Acurácia. Esta avaliação se dá pela divisão da quantidade de casos

bem sucedidos pela quantidade estego-imagens total da amostra (WITTEN; FRANK; HALL, 2011).

Em todas as imagens da amostra temos os resultados esperados da aplicação do método LSB em todos os quatro casos: todas as estego-imagens resultantes aparentam normalidade, nenhuma das mensagens embutidas pode ser percebida a olho nu.

Estudando os resultados do Histogram Attack para os diferentes valores de $\propto$, foi possível calcular a seguinte relação de acurácia: para $\propto$ = 1.00 a porcentagem de acerto foi 100%; para $\propto$ = 0.75 a porcentagem de acerto foi 95%; para $\propto$ = 0.50 a porcentagem de acerto foi 45%; para $\propto$ = 0.25 a porcentagem de acerto foi 10%.

O método apresentou, portanto, uma acurácia de 62,5% neste estudo, uma vez que foram 50 resultados bem sucedidos em 80 estego-imagens testadas.

CONCLUSÕES

Este projeto cumpriu com seu objetivo inicial de iniciação nas áreas de esteganografia e esteganálise. Tanto a pesquisa da literatura quanto às implementações tiveram papel importante no entendimento destas áreas.

A acurácia geral do experimento foi 62,5%. Tendo em vista que o limiar foi controlado e determinado em função das informações sobre a amostra, e que a porcentagem de acertos variou muito de acordo com o valor de $\propto$, este é um dado que evidencia a fraqueza do método contra estego-imagens com taxa de incorporação baixa.

REFERÊNCIAS

COELHO, L. C. M. ; BENTO, R. J. **Ferramentas de esteganografia e seu uso na infowar**. in: ICCyber'2004, p.14, 2004.

FRIDRICH, J. **Steganography in Digital Media**: Principles, Algorithms, and Applications. Cambridge University Press, 2009.

ROCHA, J, C. **Cor luz, cor pigmento e os sistemas rgb e cmy**. Revista Belas Artes, 2011.

WITTEN, I. H.; FRANK, E. ; HALL, M. **Data mining**: Pratical machine learning tools and technique. In: San francisco: Morgan Kaufmann, 3 ed, 2011.

AGRADECIMENTOS

Agradeço ao meu orientador Prof. Dr. Fabio Antonio Dorini, pela grande oportunidade e pelo voto de confiança, ao órgão envolvido neste processo, o CNPQ, à instituição UTFPR e todos os meus colegas e professores que apoiaram e contribuíram de alguma forma para que este estudo pudesse ser realizado.