FIEL – Faculdades Integradas Einstein Limeira

Fabio Augusto Pilon – 0391/22-1

Bruno Perissoto Ferreira – 0063/22-1

Resumo:

DETECÇÃO DE ESTEGANOGRAFIA EM IMAGENS UTILIZANDO APRENDIZADO DE MÁQUINA

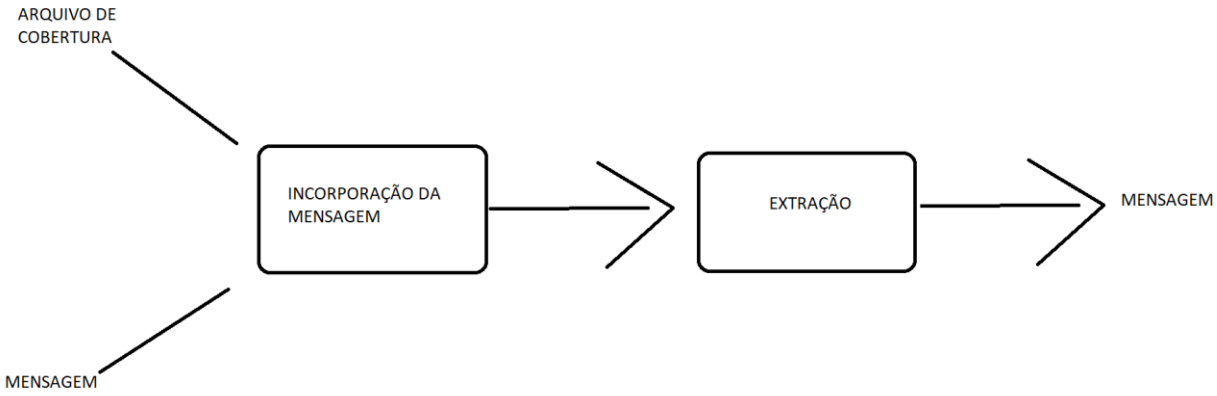
Limeira

2023

Esteganografia em imagens se refere ao processo de incorporação de uma mensagem secreta em um arquivo de imagem sem causar mudança visual perceptível a quem tenha acesso a essa imagem. Devido ao contínuo desenvolvimento de novas técnicas de esteganografia, há necessidade de desenvolvimento de novas formas de detecção dessas técnicas.

Enquanto as técnicas de criptografia têm como objetivo impedir a leitura do conteúdo real da mensagem por invasores, a finalidade da esteganografia é esconder a própria existência da mensagem.

O receptor, possuindo conhecimento prévio da existência da mensagem, é capaz de extrai-la.



A figura exibe o funcionamento de um processo de esteganografia. Uma mensagem é incorporada a um arquivo de cobertura, resultando em um arquivo que poderá ser submetido ao processo de extração para que a mensagem seja recuperada.

Como a esteganografia consiste em ocultar uma mensagem dentro de um arquivo digital sem que isso seja perceptível a olho nu, arquivos com muitos bits redundantes, como imagens, são mais adequados.

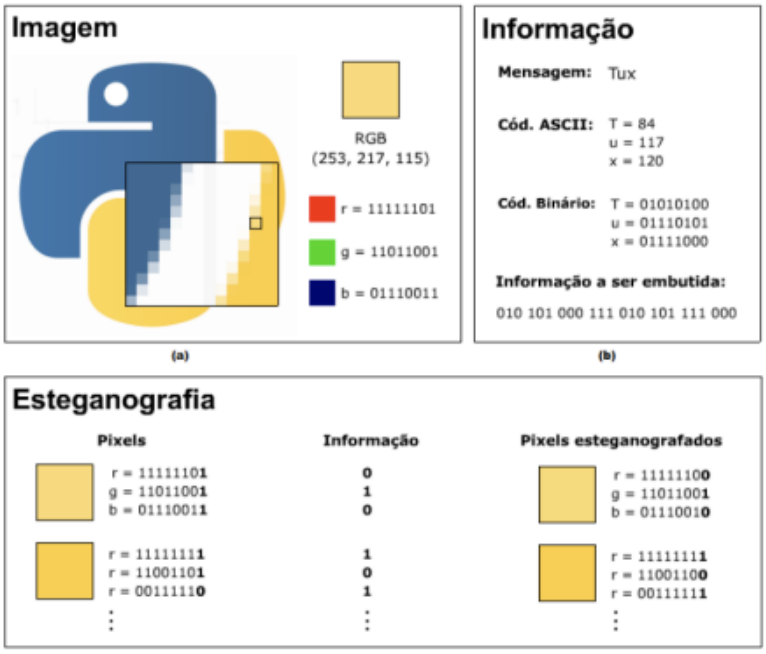
Existem duas formas de detectar a esteganografia: análise visual e análise estatística. A análise estatística é mais efetiva e utiliza técnicas de aprendizado de máquina para analisar as propriedades estatísticas de arquivos de imagem a fim de detectar a presença de uma mensagem oculta.

Existem diversas ferramentas capazes de esconder mensagens em uma imagem utilizando esteganografia. Apesar dessa facilidade ser benéfica para usos legais, organizações criminosas e terroristas já utilizaram esteganografia para se comunicar através da internet pública sem levantar suspeitas.

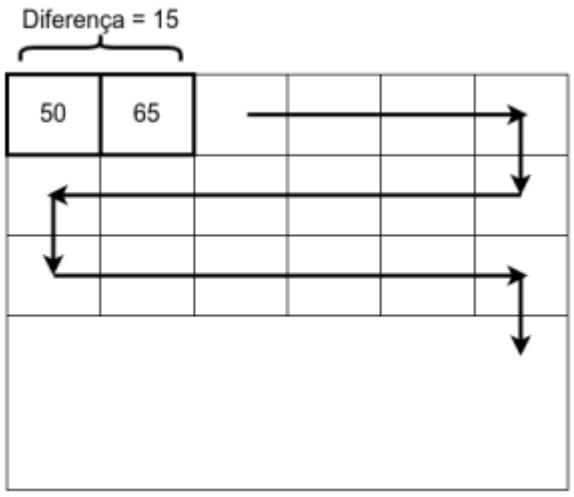
Dessa forma, o estudo de métodos de detecção automática de esteganografia é justificado através da sua importância no monitoramento de comunicações ilegais através de uma rede.

As técnicas de esteganografia podem ser classificadas em relação à dimensão da imagem de cobertura, natureza de recuperação e domínio de incorporação. As técnicas mais comuns são a esteganografia no domínio espacial e no domínio de frequência.

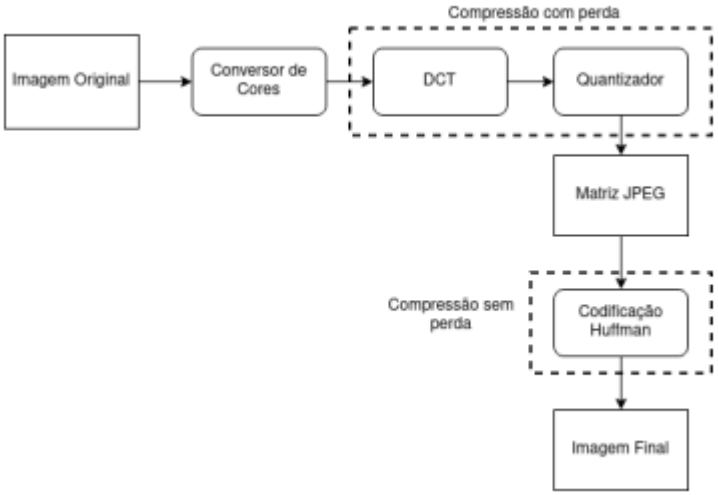
Substituição LSB: Consiste em utilizar os bits menos significativos dos pixels de uma imagem para armazenar uma mensagem secreta, sendo uma das técnicas mais simples e populares.



PVD: Utiliza a comparação das diferenças dos valores de dois pixels sucessivos para ocultar a mensagem, e tem como vantagem a possibilidade de incorporar mais bits em regiões menos perceptíveis pelo sistema visual humano.



JSteg: É utilizado em imagens JPEG no domínio de frequência, consiste em realizar a substituição de bits menos significativos dos coeficientes DCT de forma a não causar mudança perceptível quando a imagem é convertida para o domínio espacial.



Para fazer a detecção, foi utilizada a abordagem de construção de um classificador binário específico para cada técnica. A técnica de aprendizado de máquina escolhida foi o SVM (Support Vector Machine), é um algoritmo capaz de encontrar um hiperplano que separa as amostras de uma classe das amostras de outra classe, podendo utilizar esse hiperplano para classificar novas amostras).

As imagens em formato PNG foram usadas para construir os conjuntos de treinamento e teste relativos às técnicas LSB e PVD, enquanto a base de imagens em JPEG foi utilizada para a técnica JSteg.

Foram criados conjuntos de imagens com diferentes capacidades para cada técnica utilizada (LSB, PVD e JSteg) e, em seguida, foram extraídas características das imagens e utilizadas para treinar e testar um classificador. O conjunto de imagens de cada técnica foi dividido em 70% para treinamento e 30% para teste.

Tabela de resultados dos testes:

Tabela 1 – Acurácia, precisão e recall dos classificadores

técnica	elementos	acurácia	precisão	recall
LSB 10%	1545	53.33%	52.56%	55.55%
LSB 25%	1545	57.22%	55.23%	64.54%
LSB 50%	1545	67.77%	65.54%	73.76%
LSB 75%	1545	72.56%	70.96%	76.29%
LSB 100%	1545	79.16%	76.98%	82.53%
DVP	1545	59.42%	60.50%	56.00%
JSteg	1534	52.02%	54.66%	32.35%

Analisando os resultados, observa-se que para a técnica LSB a precisão aumenta conforme a quantidade de informação incorporada à imagem, já as técnicas PVD e JSteg tem uma eficácia menor pelo fato de conseguirem suportar menos informação.

Os resultados sugerem que essa abordagem é eficaz nos casos em que a quantidade de informação incorporada em uma imagem por esteganografia é grande, porém a eficiência é reduzida nos casos em que a informação é mínima.

Referências Bibliográficas:

Polachini, Matheus Esquinelato Detecção de esteganografia em imagens utilizando aprendizado de máquina. Universidade Estadual Paulista (Unesp), 2022. Disponível em: <http://hdl.handle.net/11449/236100>.