Bibliotecas de Software Livre para Detecção de Esteganografia em Imagens Digitais

Érico Meger[1], **Eros Henrique Lunardon Andrade**[1], **Guilherme Werneck de Oliveira**[1]

[1]Campus Pinhais – Instituto Federal do Paraná (IFPR) Pinhais - PR - Brasil

Abstract. *This meta-paper describes the style to be used in articles and short papers for SBC conferences. For papers in English, you should add just an abstract while for the papers in Portuguese, we also ask for an abstract in Portuguese ("resumo"). In both cases, abstracts should not have more than 10 lines and must be in the first page of the paper.*

Resumo. *Este meta-artigo descreve o estilo a ser usado na confecção de artigos e resumos de artigos para publicação nos anais das conferências organizadas pela SBC. É solicitada a escrita de resumo e abstract apenas para os artigos escritos em português. Artigos em inglês deverão apresentar apenas abstract. Nos dois casos, o autor deve tomar cuidado para que o resumo (e o abstract) não ultrapassem 10 linhas cada, sendo que ambos devem estar na primeira página do artigo.*

1. Introdução

O movimento do software livre se estabelece como um paradigma essencial para promover transparência, colaboração e inovação no cenário tecnológico contemporâneo. Segundo a Free Software Foundation, software livre é definido pela sua capacidade de respeitar as liberdades e o controle dos usuários sobre o software: a liberdade de executar o programa para qualquer propósito, de estudá-lo e modificá-lo (acesso ao código-fonte é pré-requisito), de redistribuir cópias e de distribuir versões modificadas para a comunidade, conhecidas como as quatro liberdades essenciais [Foundation 2024].

Ao assegurar essas liberdades, o software livre não apenas fortalece a confiança nas soluções digitais, por permitir auditoria e aprendizado mútuo, mas também fomenta ambientes colaborativos dinâmicos, onde ferramentas podem ser aprimoradas coletivamente. Essa filosofia de abertura e colaboração se manifesta também no campo da inteligência artificial, por meio de bibliotecas como PyTorch, TensorFlow e scikit-learn. Essas ferramentas de código aberto democratizam o acesso a algoritmos de aprendizado de máquina, permitindo reprodutibilidade científica, auditoria de modelos e desenvolvimento colaborativo de soluções inovadoras [Team 2025a, Team 2025b].

No contexto da esteganografia, a disponibilidade dessas bibliotecas open source oferece grandes oportunidades para o avanço da área. A análise de imagens digitais, por exemplo, pode se beneficiar de recursos de detecção de padrões e classificação automática fornecidos por essas ferramentas, auxiliando tanto no desenvolvimento de técnicas esteganográficas mais robustas quanto na criação de métodos de detecção mais eficazes. Assim, a intersecção entre software livre, inteligência artificial e esteganografia evidencia como a filosofia do código aberto não só fortalece a confiança técnica, mas também amplia as possibilidades de pesquisa e aplicação prática neste campo.

A esteganografia pode ser compreendida como uma técnica utilizada para esconder informações em meios aparentemente comuns, de forma que um observador externo não consiga identificar a presença de dados ocultos [Fridrich 2010].

Essa área de estudo, portanto, não se limita apenas ao ato de esconder informações, mas constitui um campo de estudo mais amplo que abrange técnicas, algoritmos e aplicações destinadas a garantir a confidencialidade e a discrição da comunicação. Em contraste com a criptografia, que protege o conteúdo das mensagens mas não oculta sua existência, a esteganografia busca mascarar o próprio ato de comunicação [Fridrich 2010]. Essa característica a torna uma área estratégica tanto para aplicações legítimas, como autenticação de documentos e proteção da privacidade, quanto para usos maliciosos. Tal dualidade evidencia que a esteganografia deve ser compreendida não apenas sob uma perspectiva técnica, mas também dentro de um contexto social e político mais amplo.

Nesse sentido, ao longo da história, e de forma ainda mais acentuada no cenário contemporâneo, observa-se o fortalecimento de mecanismos de vigilância e controle sobre a comunicação digital. Na Europa, por exemplo, esse movimento se materializa tanto em iniciativas de remoção massiva de conteúdos, com mais de 41 milhões de postagens bloqueadas apenas no primeiro semestre de 2025 [Poder360 2025], quanto em pressões políticas para enfraquecer a segurança criptográfica, como a exigência de um backdoor no iCloud, que levou a Apple a retirar a opção de criptografia de ponta a ponta de seus serviços no Reino Unido [Guardian 2025]. Embora tais medidas sejam frequentemente justificadas em nome da segurança pública, a ausência de transparência sobre os critérios de censura e o impacto direto na privacidade digital levantam sérias preocupações. Nesse contexto, a esteganografia age como uma alternativa tecnológica de resistência, capaz de proporcionar meios de comunicação discretos e seguros, reforçando sua relevância sociopolítica e justificando o aprofundamento de seu estudo.

1.1. Objetivo

Explorar o uso de bibliotecas de software livre no desenvolvimento de modelos de inteligência artificial para a detecção de esteganografia em imagens digitais.

2. Revisão bibliográfica

Essa seção revisará os principais trabalhos relacionados, destacando contribuições, métodos e limitações que fundamentam o desenvolvimento desta pesquisa.

O trabalho *"An Ensemble Model using CNNs on Different Domains for ALASKA2 Image Steganalysis"* de Chubachi [Chubachi 2020] surge da constatação de que muitos detectores de esteganografia baseados em aprendizado profundo não generalizam bem em cenários reais devido ao uso de conjuntos de dados simplificados. A competição ALASKA2 ofereceu um ambiente mais realista, com imagens JPEG coloridas de diferentes origens e processos, estimulando soluções mais aplicáveis. Nesse contexto, o objetivo do autor foi desenvolver um modelo de detecção baseado em um ensemble de redes convolucionais que combinasse informações tanto do domínio espacial (RGB, YUV e Lab) quanto do domínio da frequência (coeficientes DCT).

A metodologia proposta envolveu CNNs construídas sobre arquiteturas EfficientNet, com ajustes para lidar com as especificidades de cada domínio. No caso dos coe-

ficientes DCT, foram aplicadas codificações one-hot, recortes de valores e convoluções dilatadas para capturar padrões sutis. Para integrar os modelos, além da simples média de previsões, foi desenvolvido um perceptron multicamada capaz de combinar os mapas de características. Também se utilizaram técnicas auxiliares, como pseudo-rotulagem e stacking com LightGBM. Em experimentos conduzidos com 300 mil imagens, o uso combinado dos modelos trouxe ganhos consistentes, resultando em uma performance de AUC ponderado próxima de 0,94 e garantindo a terceira colocação na competição.

O estudo apresenta como pontos fortes a inovação de combinar diferentes domínios e a validação em um cenário competitivo e realista. Contudo, o alto custo computacional e a limitação de testar apenas algoritmos de esteganografia já conhecidos restringem sua aplicabilidade prática. Em contraste, a proposta desenvolvida neste trabalho busca explorar o uso de bibliotecas de software livre para a construção de modelos de inteligência artificial em esteganálise. Diferente de [Chubachi 2020], que enfatiza ganhos técnicos com arquiteturas avançadas, nossa abordagem objetiva democratizar a área ao garantir reprodutibilidade, baixo custo e acessibilidade, sem deixar de buscar acurácia.

3. Metodologia

4. Resultados e discussões

5. Conclusão

Referências

Chubachi, K. (2020). An ensemble model using cnns on different domains for alaska2 image steganalysis. *IEEE International Workshop on Information Forensics and Security (WIFS)*.

Foundation, F. S. (2024). What is free software? `https://www.gnu.org/philosophy/free-sw.html`. Acesso em: 27 ago. 2025.

Fridrich, J. (2010). *Steganography in Digital Media Principles, Algorithms, and Applications*. Springer.

Guardian, T. (2025). Apple pulls encrypted icloud storage from uk after government demands back door access. Acesso em: 26 ago. 2025.

Poder360 (2025). Europa barrou 41,4 mi de posts via usuários no 1º semestre de 2025. Acesso em: 26 ago. 2025.

Team, P. (2025a). About pytorch. `https://pytorch.org/projects/pytorch/`. Acesso em: 27 ago. 2025.

Team, T. (2025b). About tensorflow. `https://www.tensorflow.org/about/`. Acesso em: 27 ago. 2025.