Steganografie

Agape Ioan, Apostol Bianca
Universitatea Tehnica "Gheorghe Asachi" , Iasi

Introducere

Steganografia reprezintă arta de a ascunde un mesaj într-un altul, astfel încât existența acestuia să nu poată fi detectată de o persoană neautorizată. În cadrul acestui proiect, ne-am concentrat pe tehnici avansate de steganografie bazate pe rețele neuronale, mai precis pe utilizarea rețelelor de tip **Cs-FNN** (Cover-separable Fixed Neural Networks).

Aceste rețele permit ascunderea informațiilor într-un mod subtil și eficient, depășind metodele tradiționale, precum LSB (Least Significant Bit), care sunt mai ușor de detectat. Am explorat și testat mai multe arhitecturi de rețele neuronale bazate pe FNNs, dezvoltând module de encoding și decoding pentru a ascunde și extrage mesaje secrete din imagini.

Prin această abordare, am reușit să îmbunătățim procesul de steganografie, asigurându-ne că mesajele sunt bine camuflate și greu de descifrat, chiar și pentru cele mai avansate tehnici de analiză. Astfel, am adus o contribuție semnificativă la dezvoltarea unui sistem mai sigur și mai eficient de ascundere a informațiilor.

Metode si materiale

În acest proiect, am utilizat rețele neuronale de tip Cover-separable Fixed Neural Networks (Cs-FNN) pentru a ascunde mesaje în imagini. Rețeaua este antrenată să învețe cum să integreze mesajele secrete în imagini într-un mod care minimizează detectabilitatea acestora.

Am folosit un set de imagini publice și private, preprocesate și normalizate pentru a se potrivi inputurilor rețelei. Procesul de encoding presupune ascunderea mesajelor în caracteristici ale imaginii, iar procesul de decoding permite extragerea acestora din imagini procesate.

Pentru implementare, am folosit Python, cu biblioteci precum **numpy, pytorch, tensorflow** pentru rețele neuronale si **PIL** pentru procesarea imaginilor.

Rezultate

Fig. 1. Imagine originală

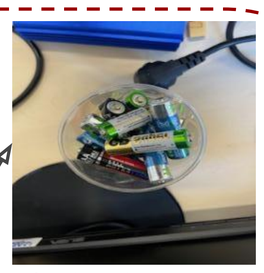


Fig. 2.1. Secret nr. 1

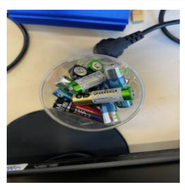
Fig. 2.2. Secret nr. 2

Fig. 2.3. Secret nr. 3

Fig. 3.1. Imagine steganografică

Fig. 3.2. Secret key

Secrete recuperate



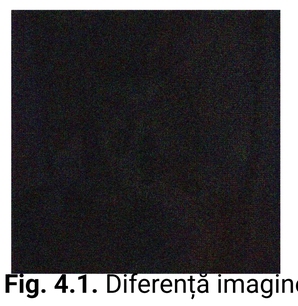


Fig. 4.1. Diferență imagine cover

Fig. 4.1. Diferență imagine secret

	PSNR	SSIM
Test 1	**27.38**	**0.9482**
Test 2	**28.45**	**0.9520**
Test 3	**26.53**	**0.9446**
Kishore et al	22.79	0.7827
Luo et al	21.20	0.7413
Cs-FNNs	33.01	0.9156

Table 2. secret-rev metrics

	PSNR	SSIM
Test 1	**37.24**	**0.9019**
Test 2	**38.17**	**0.9191**
Test 3	**36.25**	**0.8823**
Kishore et al	22.24	0.5254
Luo et al	23.42	0.5762
Cs-FNNs	41.89	0.9799

Table 1. stego metrics

Concluzii

Rezultatele obținute demonstrează eficiența și robustețea soluției implementate.
Metricele de calitate, cum ar fi **PSNR** și **SSIM**, indică faptul că imaginea stego păstrează o similitudine înaltă cu imaginea de acoperire, asigurându-se astfel că modificările sunt aproape imperceptibile pentru observatorul uman.

Scopul principal al acestui proiect a fost explorarea și implementarea unor tehnici avansate de steganografie utilizând rețele neuronale, în special arhitecturi bazate pe **Cs-FNNs**.
Prin utilizarea acestor rețele neuronale, am reușit să îmbunătățim semnificativ securitatea procesului de steganografie, depășind limitările metodologiilor tradiționale care sunt vulnerabile la analize de tip forensică.

Contact

Agape Ioan
Email: ioan.agape@student.tuiasi.ro
Apostol Bianca
Email: bianca-cristina.apostol@student.tuiasi.ro

References

1. https://arxiv.org/pdf/2407.11405
2. https://www.researchgate.net/publication/312826532_Digital_image_steganography_techniques_in_spatial_domain_A_study
3. https://wizardcyber.com/unlocking-the-secrets-of-steganography-in-cybersecurity/
4. https://ieeexplore.ieee.org/document/7764399