

Securizarea Informațiilor folosind Tehnici Steganografice

ABSOLVENT: ~~XXXXXXXXXXXX~~

PROFESOR COORDONATOR: DR. BORIGA RADU



Context Actual

VIAȚA ÎN ERA CONTEMPORANĂ ESTE MARCATĂ DE ACCESUL ȘI UTILIZAREA MEDIULUI ONLINE.

SE PRODUCE ȘI O CREȘTERE SEMNIFICATIVĂ A RISCULUI, ÎN MATERIE DE SECURITATE, LA CARE SUNTEM EXPUȘI ÎN SFERA VIRTUALĂ.

PROBLEMA ACTUALĂ, CARE REPREZINTĂ SUBIECTUL DISCUȚIEI DE AZI: SECURIZAREA INFORMAȚIILOR CU CARACTER SENSIBIL ASTFEL ÎNCÂT ACESTE SĂ NU FIE COMPROMISE.

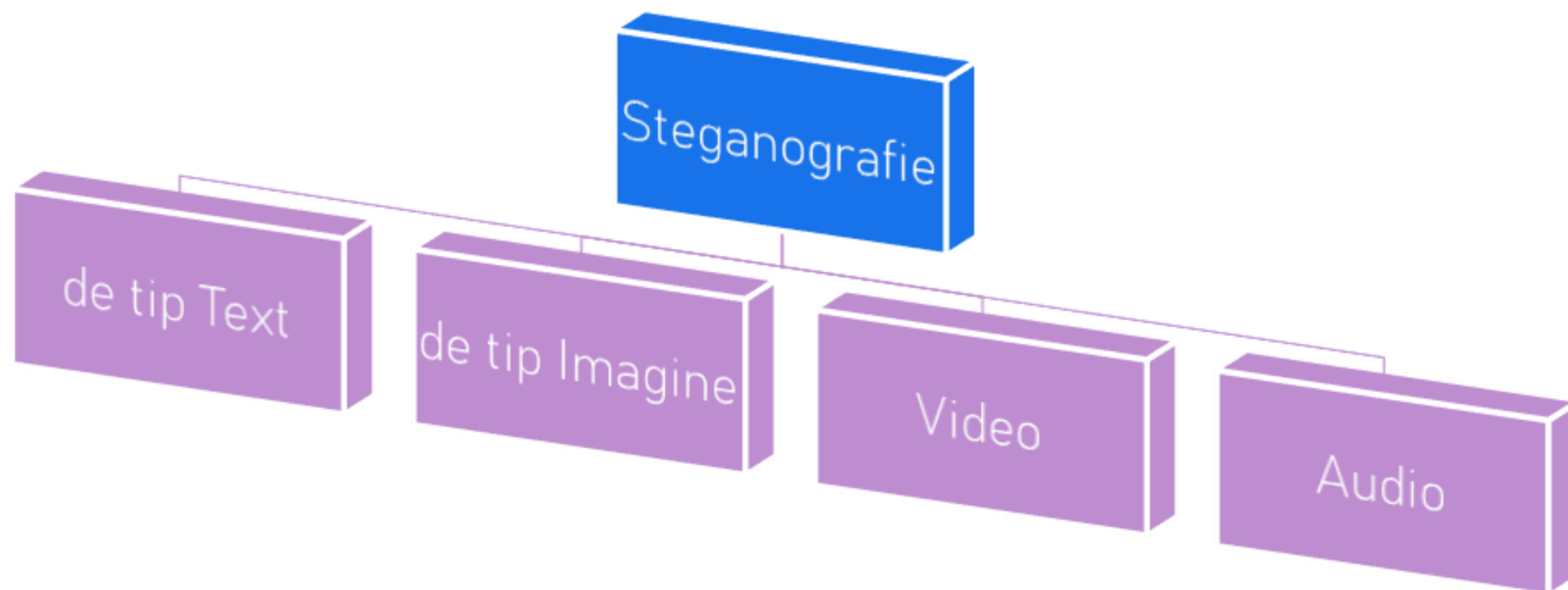
Criptografia vs Steganografia

CRIPTOGRAFIA ESTE O RAMURĂ A MATEMATICII APLICATE CARE ESTE UTILIZATĂ PENTRU SECURIZAREA ȘI MENȚINEREA CARACTERULUI PRIVAT AL INFORMAȚIILOR. ÎN TERMENI PRACTICI, ACEST LUCRU IMPLICĂ CONVERSIA UNUI TEXT (FIȘIER, ȘIR DE CARACTERE/BIȚI) ÎN CLAR (PLAIN TEXT) ÎNTR-UNUL CRIPTIC (NUMIT TEXT CIFRAT).

STEGANOGRAFIA ESTE ARTA ȘI ȘTIINȚA COMUNICĂRII ÎNTR-UN MOD PRIN CARE EXISTENȚA UNUI MESAJ SECRET SĂ NU POATĂ FI DETECTATĂ.

	Steganography	Cryptography
Definition	Depend on hiding the message existence	Depend on hiding the message meaning
Purpose	Keep communication secure.	Provide protection for data
Visibility	Never	Always
Failure	When discover the presence of a hidden message	When able to decrypt and read the message
Concern	Embedding capacity and detectability of cover object	Robustness against deciphering.
Carrier	Any type of digital media	Depend on text as a carrier
Key	Optional, but provide more security	Necessary

În funcție de natura
obiectului de acoperire:



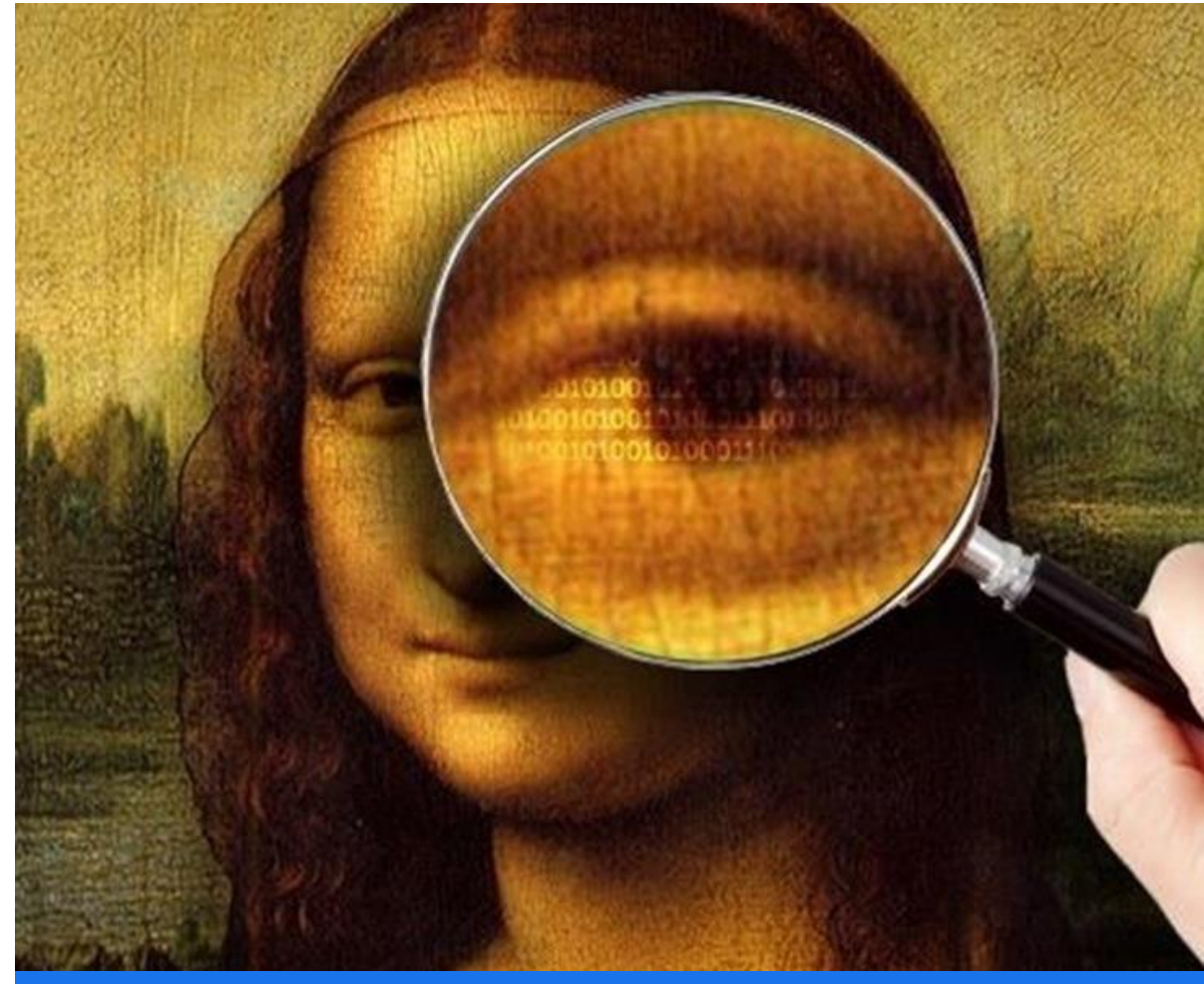
ALGORITMI STEGANOGRAFICI

IMAGINE -> PIXEL -> RGB -> OCTEȚI (24 DE BIȚI) -> *TEHNICI DE SUBSTITUȚIE*

- PRINCIPALUL DEZAVANTAJ PENTRU O ASTFEL DE ABORDARE ESTE SLĂBICIUNEA RELATIVĂ LA MODIFICĂRILE PRODUSE MEDIULUI DE ACOPERIRE.

TEHNICI DE TRANSFORMARE A DOMENIULUI -
> DOMENIUL DE FRECVENȚĂ

- ELE RĂMÂN IMPERCEPTIBILE PENTRU SISTEMUL SENZORIAL UMAN, DAR SUNT MAI COMPLEXE DIN PERSPECTIVA CALCULULUI ȘI PREZINTĂ O CAPACITATE DE ÎNCORPORARE MAI MICĂ.

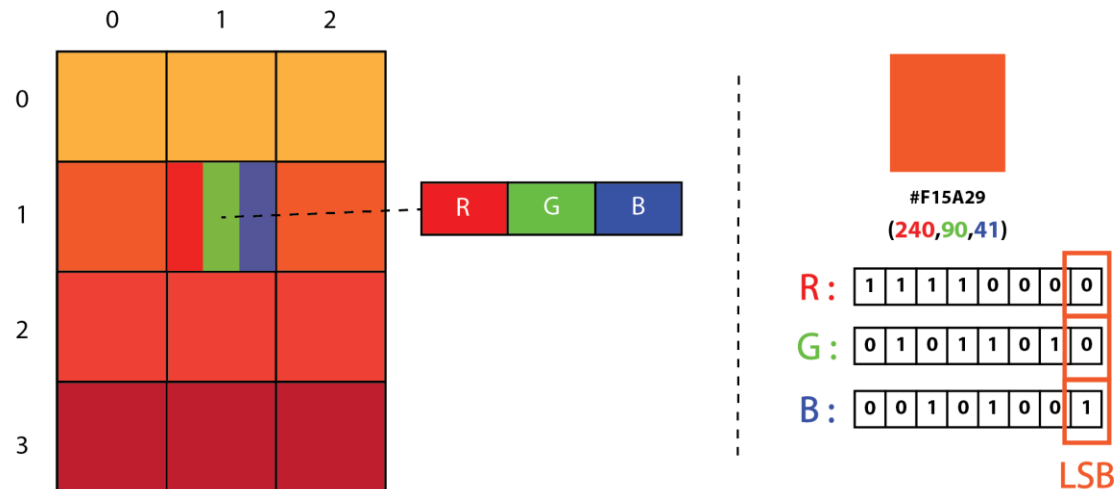


LSB

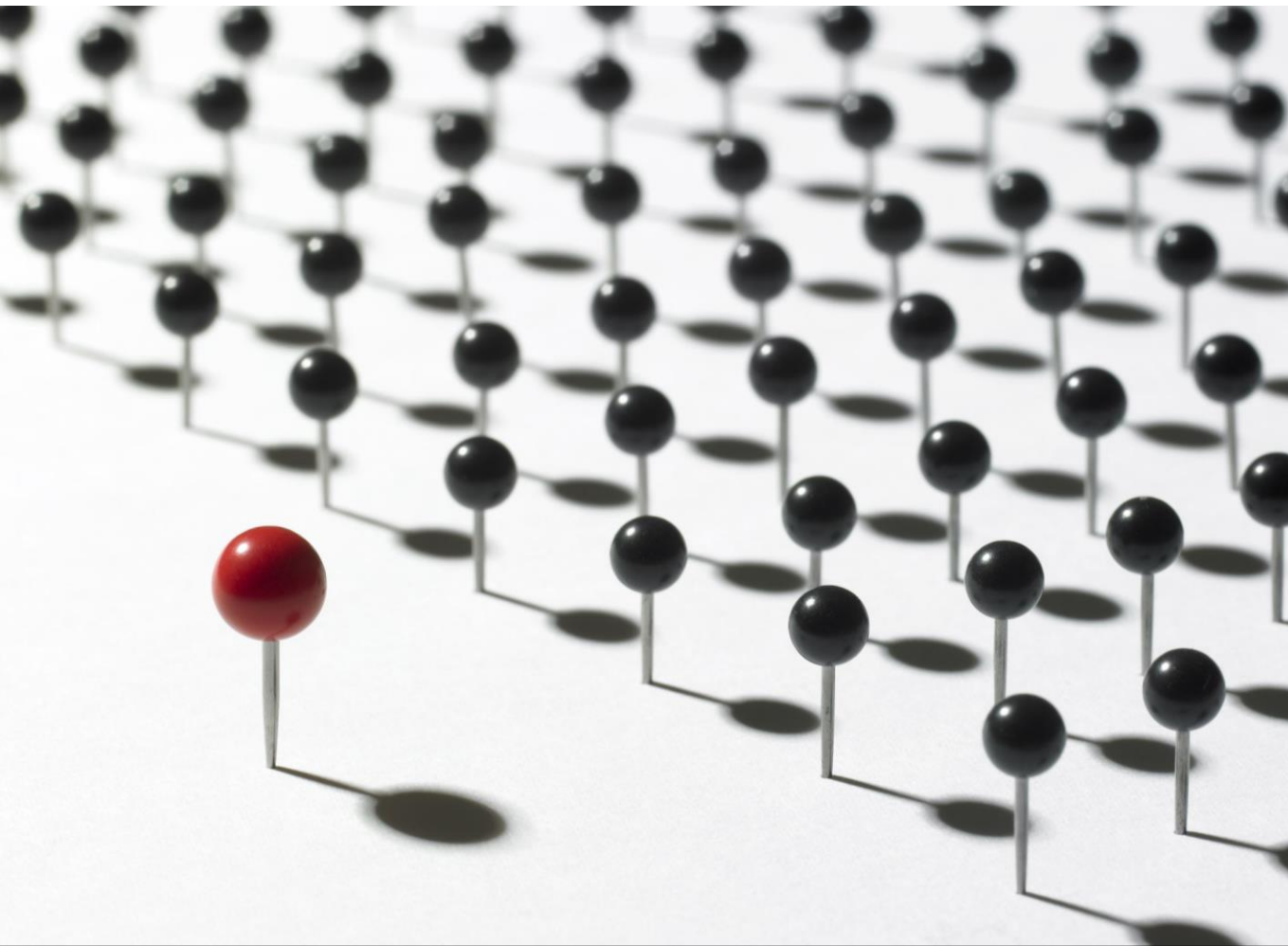
Mesajul secret va fi încorporat în bitul cel mai nesemnificativ din fiecare canal al culorii unui pixel.

Mai multe variații (îmbunătățiri):

- Algoritmul LSB folosind conceptul de liste înlanțuite;
- Algoritmul LSB folosind K-means clustering
- Algoritmul LSB îmbunătățit cu filtrarea pixelilor după MSB



ALGORITMUL PROPUȘ



Aspectul 1: Criptarea mesajului folosind AES. Ne putem gândi că acest aspect servește drept ultimă soluție în cazul în care un atac de steganaliză are succes.

Aspectul 2: Generarea unei secvențe unice, aleatoare de pixeli a unei imagini, folosind algoritmul modern de amestecare Fisher-Yates (versiunea lui Durstenfeld).

- Metoda propusă nu este foarte eficientă din punct de vedere al memoriei deoarece trebuie să trimitem secvența criptată de pixeli, alături de imaginea rezultată prin tehnica steganografică, dar facem acest compromis pentru a obține o mai bună securitate.
- Recomandări: utilizarea fotografiilor care nu se găsesc online, utilizarea a 2 parole diferite, transmiterea sigură a parolelor...

Codare

Decodare

Date de Intrare: I = imaginea; M = mesajul secret; P1 = parolă pentru mesajul secret; P2 = parolă pentru secvența de Pixeli

Date de Iesire: S = imaginea modificată; Pix = secvența criptată de pixeli

Pas 1: Se criptează mesajul secret (M) cu AES folosind parola secretă, P1, rezultând N.

Pas 2: Se generează secvența aleatoare de pixeli, P, pornind de la lungimea mesajului secret criptat și de la mărimei imaginii de acoperire, I.

Pas 3: Se încorporează N în pixelii generați aleatoriu în P, folosind LSB și obținem S.

Pas 4: Se criptează P cu AES, folosind P2 și obținem Pix.

Pas 5: Returnăm S și Pix.

Date de Intrare: S = imaginea modificată; Pix = secvența criptată de pixeli; P1 = parolă pentru mesajul secret; P2 = parolă pentru secvența de Pixeli

Date de Iesire: M = mesajul secret

Pas 1: Se decriptează Pix folosind P2 (AES) și obținem P.

Pas 2: Din S extragem biții din pixelii marcați, din P, și obținem N.

Pas 3: Se decriptează N folosind P1 (AES) și obținem M.

Pas 4: Se returnează M.

ANALIZA PERFORMANȚEI

1) Vizual, imaginile rezultate sunt identice cu cele originale.



Figură 3.2. 8 – Stego LSB Original

2) Capacitatea de codare este mare, deoarece folosim toți pixelii imaginii alese.


3) Timpul de codare/decodare este puțin mai mare decât în cazul unor algoritmi de LSB banali deoarece avem pași de criptare/decriptare, dar și cei de amestecare/aranjare a pixelilor.

4) PSNR (56.1), MSE (0.6) și SSIM (0.99) ating rezultate bune, în comparație cu ceilalți algoritmi discutați.

5) Histogramele prezintă deviație mai mare cu cât dimensiunea mesajului transmis este mai mare și dimensiunea imaginii este mai mică.

- 1) E. Cole, Hiding in Plain Sight: Steganography and the Art of Covert Communication, Statele Unite ale Americii: Bob Ipsen, 2003
- 2) S. Katzenbeisser și F. A. P. Peticolas, Information Hiding Techniques for Steganography and Digital Watermarking, Statele Unite ale Americii: Artech House INC., 2000.
- 3) A. Choudary, „edureka!,” 25 Noiembrie 2020. [Interactiv]. Available: <https://www.edureka.co/blog/steganography-tutorial>. [Accesat 01 Iunie 2021].
- 4) R. C. Gonzalez și R. E. Woods, Digital Image Processing – Third Edition, New Jersey: Prentice Hall, 2007.
- 5) United States National Institute of Standards and Technology (NIST), „Announcing the ADVANCED ENCRYPTION STANDARD (AES),” Federal Information Processing Standards Publication 197 , 2001.
- 6) R. Durstenfeld, „Algorithm 235: Random permutation,” *Communications of the ACM*, vol. 7, nr. 7, pp. 420-421, 1964.
- 7) R. Popa, 1998. [Interactiv]. Available: <https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.88.9413&rep=rep1&type=pdf>. [Accesat 01 Iunie 2021].

BIBLIOGRAFIE SELECTIVĂ



The End.

Vă mulțumesc pentru atenție!