

Image Encryption Using 2D Henon-Sine Map and DNA Approach

342C2, Simionescu Marina-Ilariana



Contents

[1. Introducere 2](#_Toc124884000)

[1.1 Criptarea 3](#_Toc124884001)

[1.2 Algoritm 4](#_Toc124884002)

[2. Rezultate 5](#_Toc124884003)

[2.1 Rezultate paper 5](#_Toc124884004)

[2.2 Rezultate implementare 7](#_Toc124884005)

[Test 1 7](#_Toc124884006)

[Test 2 7](#_Toc124884007)

[Test 3 8](#_Toc124884008)

[Test 4 8](#_Toc124884009)

[Test 5 9](#_Toc124884010)

[3. Alte metode de criptare 9](#_Toc124884011)

[3.1 AES (Advances Encryption Standard) 9](#_Toc124884012)

[3.2 RSA (Rivest-Shamir-Adleman) 10](#_Toc124884013)

[3.3 TEA (Tiny Encryption Algorithm) 10](#_Toc124884014)

[4. Concluzii 10](#_Toc124884015)

[Referinte 11](#_Toc124884016)

# Introducere

Dezvoltarea tehnologiei si popularizarea internetului au usurat viata oamenilor in ultimele decenii. Totusi, odata cu aceasta dezvoltare, a crescut si numarul de interceptari rau intentionate ale informatiilor. Prin urmare, s-a dovedit necesar dezvoltarea unei tehnologii de transmitere a datelor in mod sigur.

Una din cele mai importante forme de transmitere a informatiilor, si totodata printre cele mai raspandite, o reprezinta imaginile digitale. Prin urmare, pentru transmiterea datelor in siguranta, este nevoie de o modalitate de criptare a acestor imagini.

Datorita capacitatii mari de date si corelarea puternica a pixelilor, algoritmii clasici de criptare (ex. DES si AES) necesita mult timp de calcul, cee ace ii face ineficienti. Pentru a rezolva aceasta problema au aparut un numar mare de algoritmi dedicati criptarii imaginilor pe baza unor harti haotice (chaotic map).

Desi multi cercetatori au propus algoritmi de criptare a imaginilor pe baza haosului, unii s-au dovedit a nu avea o securitate suficienta. De exemplu, scheme de criptare de tip 1D pot fi decriptate folosind brute-force.

Henon-Sine map (2D-HSM) este o metoda de criptare a imaginilor, bazandu-se pe Henon map si Sine map. Sine map este un map haotic de tip 1D, definit de ecuatia: xn+1 = µ\*sin(Π\*x­n). Desi µ poate sa ia valori in intervalul [0, 1], Sine map este haotic doar atunci cand µ are valori intre 0.87 si 1. Henon map este un map haotic 2D, definit de ecuatiile

xn+1 = 1 – a\*xn2 + yn

yn+1 = b\*xn

De asemenea, pentru a imbunatati eficienta de calcul a criptarii, algoritmul se foloseste de o abordare ADN (descompunerea fiecarui pixel gri pe 8 biti in 4 coduri ADN pentru a se reduce complexitatea de timp a permutarii).

Henon-Sine map este definite de urmatoarele ecuatii(3):

xn+1 = (1 – a\*sin2(xn) + yn)

yn+1 = b\*xn

## Criptarea

Step 1: Se vor alege chei secrete care vor fi parametrii si valorile initiale pentru 2D-HSM.

Step 2: Se vor obtine chei haotice folosindu-se ecuatia 3

Step 3: Se va citi o imagine Imxn si se va redimensiona aceasta imagine intr-un vector P de dimensiune m\*n

Step 4: Se va folosi algoritmul de difuzie pentru a se obtine o noua secventa New\_P

Step 5: Se va folosi algoritmul de permutare pentru a se obtine secventa finala criptata C

Text

Description automatically generatedGraphical user interface, text, application, email

Description automatically generatedStep 6: Se va redimensiona C in Ic de dimensiune m\*n

## Algoritm

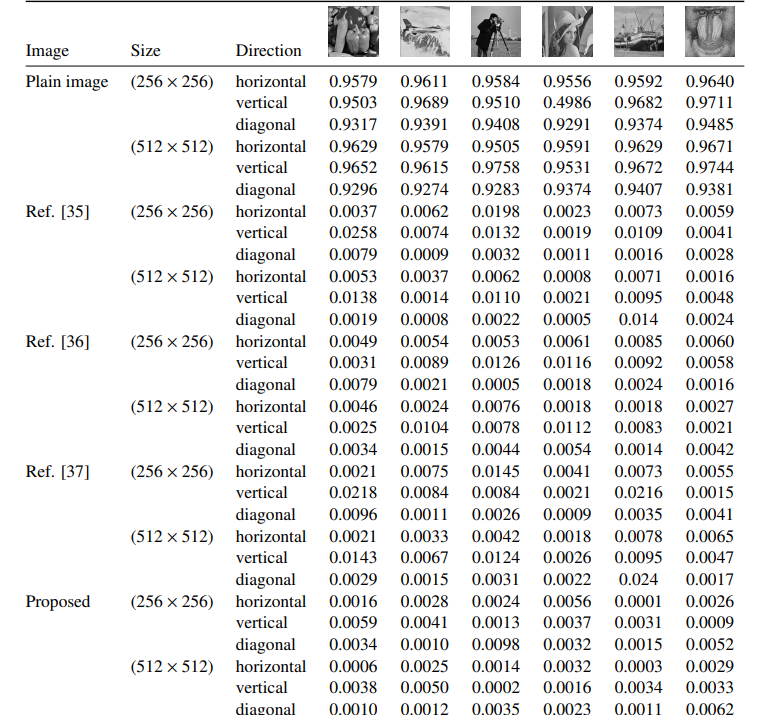
Diagram

Description automatically generated

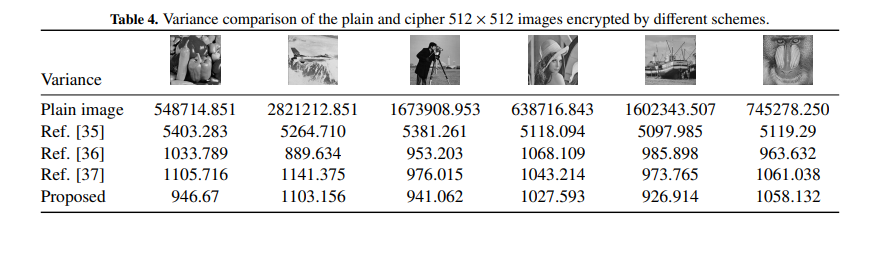
# Rezultate

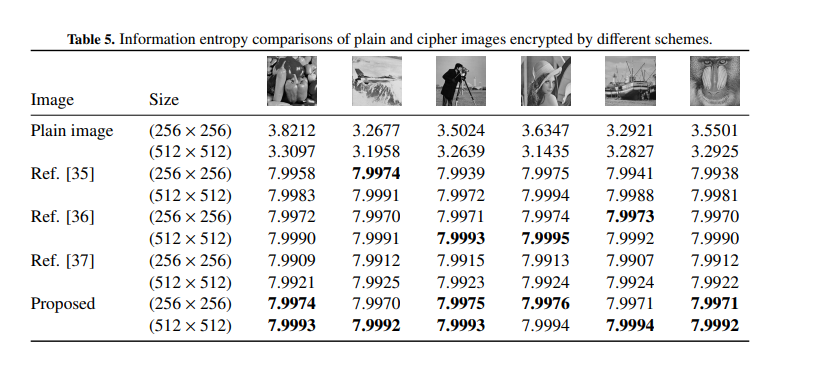
## Rezultate paper

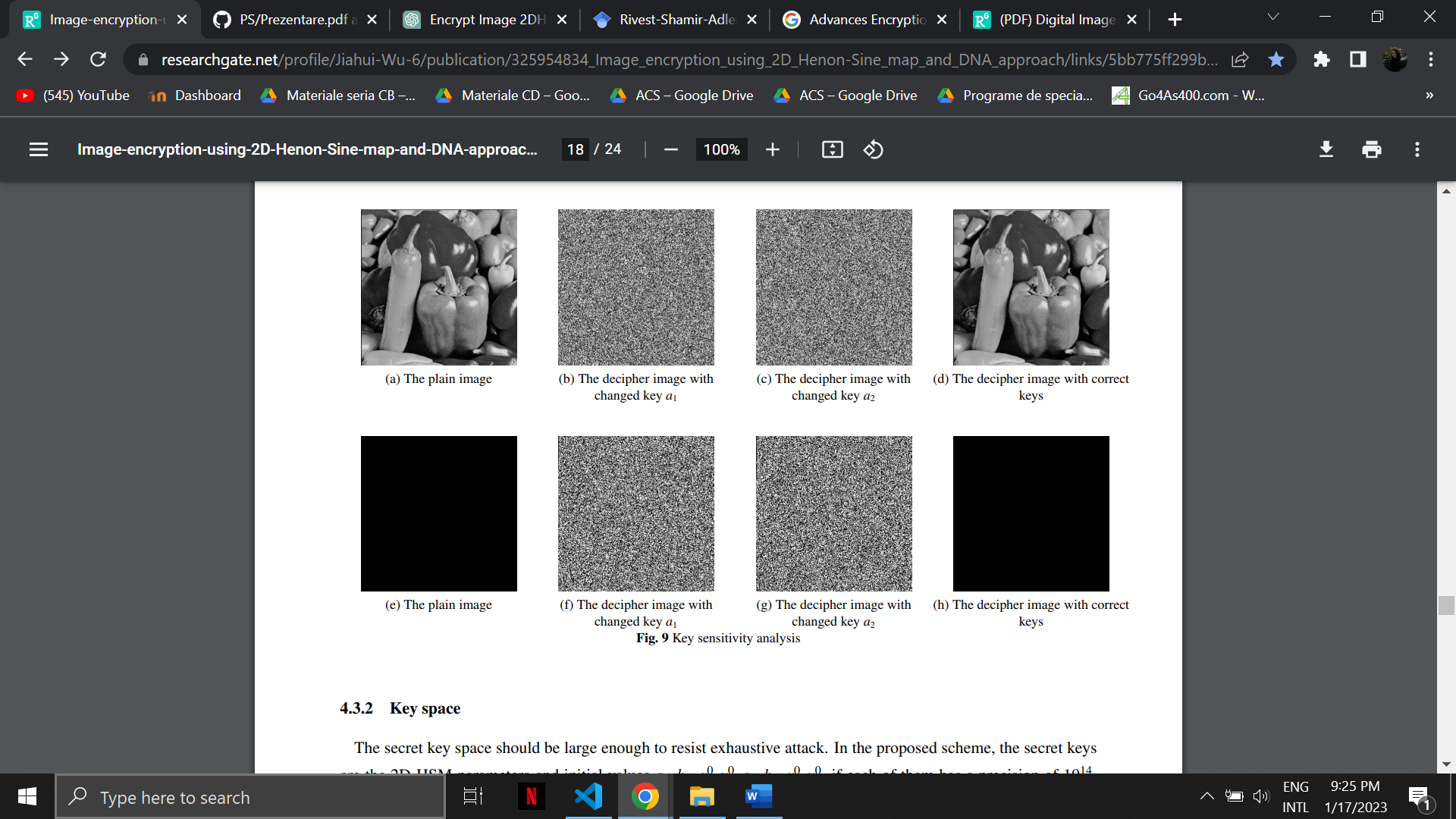
Corelatiile dintre 2 pixeli adiacenti orizontal, vertical si diagonal sunt numite coeficient de corelatie, acesta fiind una dintre cele mai importante metode de evaluare a eficientei cripratii unei imagini. In urma folosirii algoritmului 2D-HSM se asteapta obtinerea unui coeficient de corelatie aproximativ egal cu 0.



Histograma este o caracteristica statistica din zona de criptare a imaginilor, aceasta aratand frecventa diferitor valori ale pixelilor la diferite valori de intensitate. In urma folosirii schemei propuse, histograma ar trebui sa aiba o distributie mai uniforma si astfel sa poata rezista mai bine atacului statistic.



Entropia testeaza caracterul aleatoriu al unei imagini. Pentru o imagine cu 256 de niveluri de gri, valoarea entropiei este 8.

Se asteapta ca metoda de criptare a imaginii prin 2D-HSM sa reziste la 4 tipuri de atacuri: exhuasiv (spatiu mare de taste si extrem de sensibila), statistic (histograma uniforma, coeficient de corelatie aprox. 0, entropia aprox. 8 pentru o imagine pe 8 biti), diferential si de zgomot (UACI – the unified average changing intensity – si NPCR – the number of pixel change rate – aproape de valoarea lor ideala)

## Rezultate implementare

### Test 1

Tip: Color

Timp executie: 1.0707881450653076

Dimensiune: 512 x 384

### Background pattern Description automatically generatedTest 2

Tip: Color

Timp executie: 2.3531334400177

Dimensiune: 800 x 532

### Background pattern Description automatically generatedTest 3

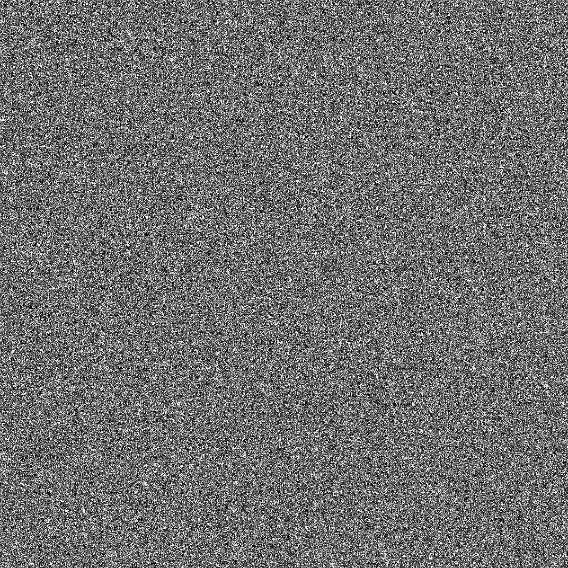


Tip: Color

Timp executie: 10.439038515090942

Dimensiune: 1600 x 1064

### Test 4

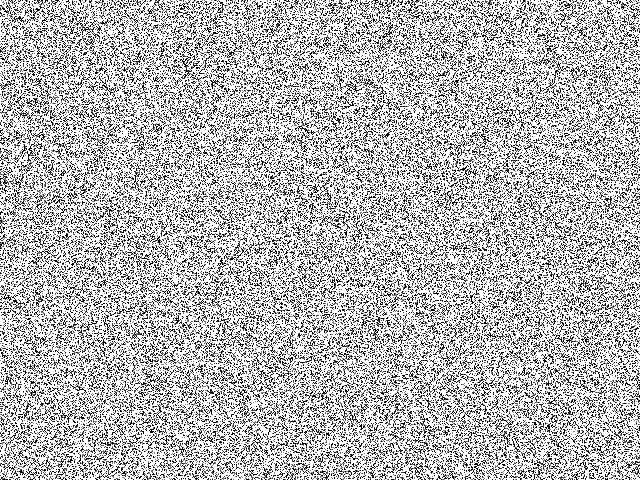


Tip: Alb-Negru

Timp executie: 8.341850757598877

Dimensiune: 1200 x 1200

### Test 5

A picture containing dark

Description automatically generated

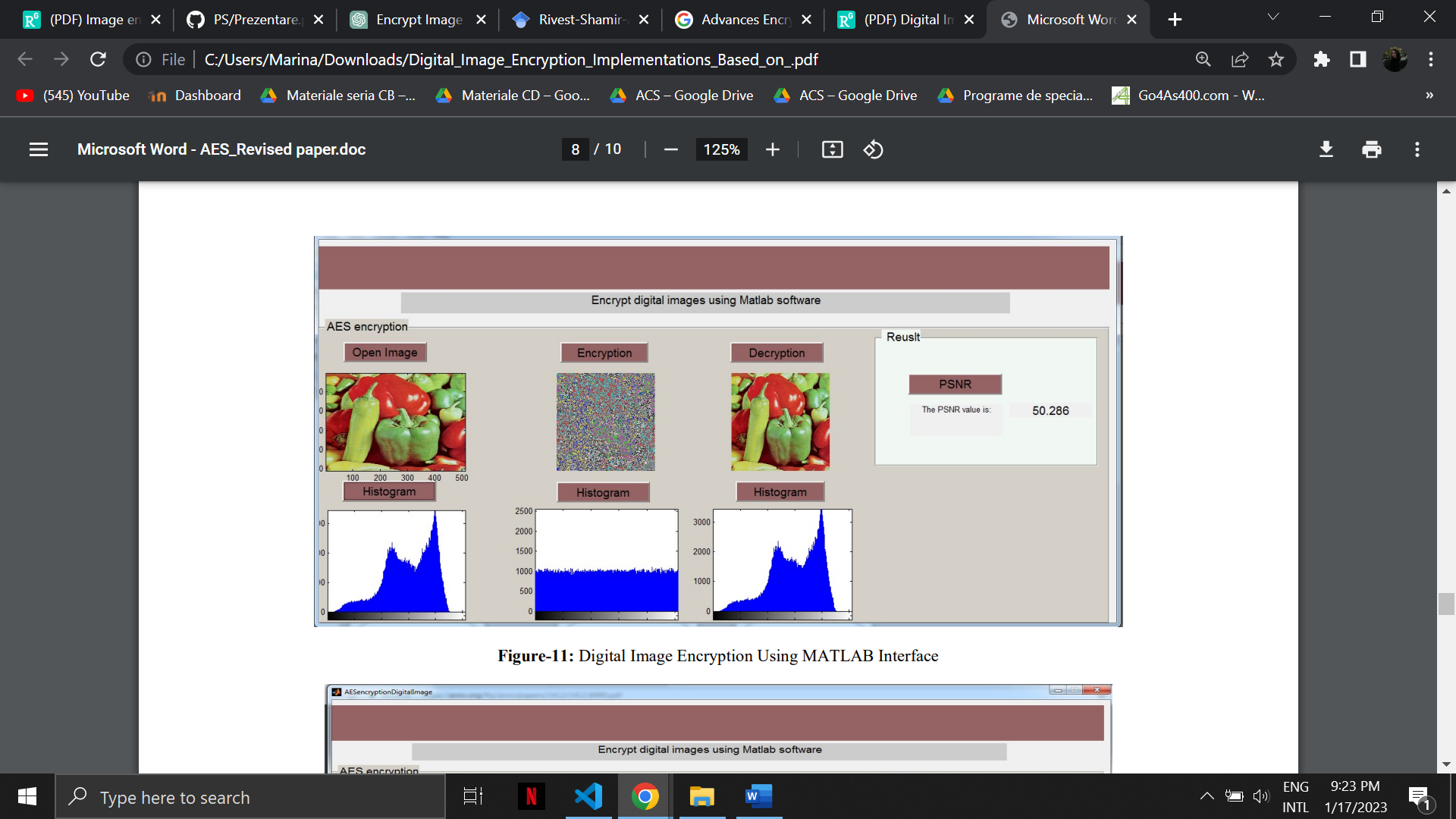
Tip: Alb-Negru

Timp executie: 1.5802960395812988

Dimensiune: 640 x 480

# Alte metode de criptare

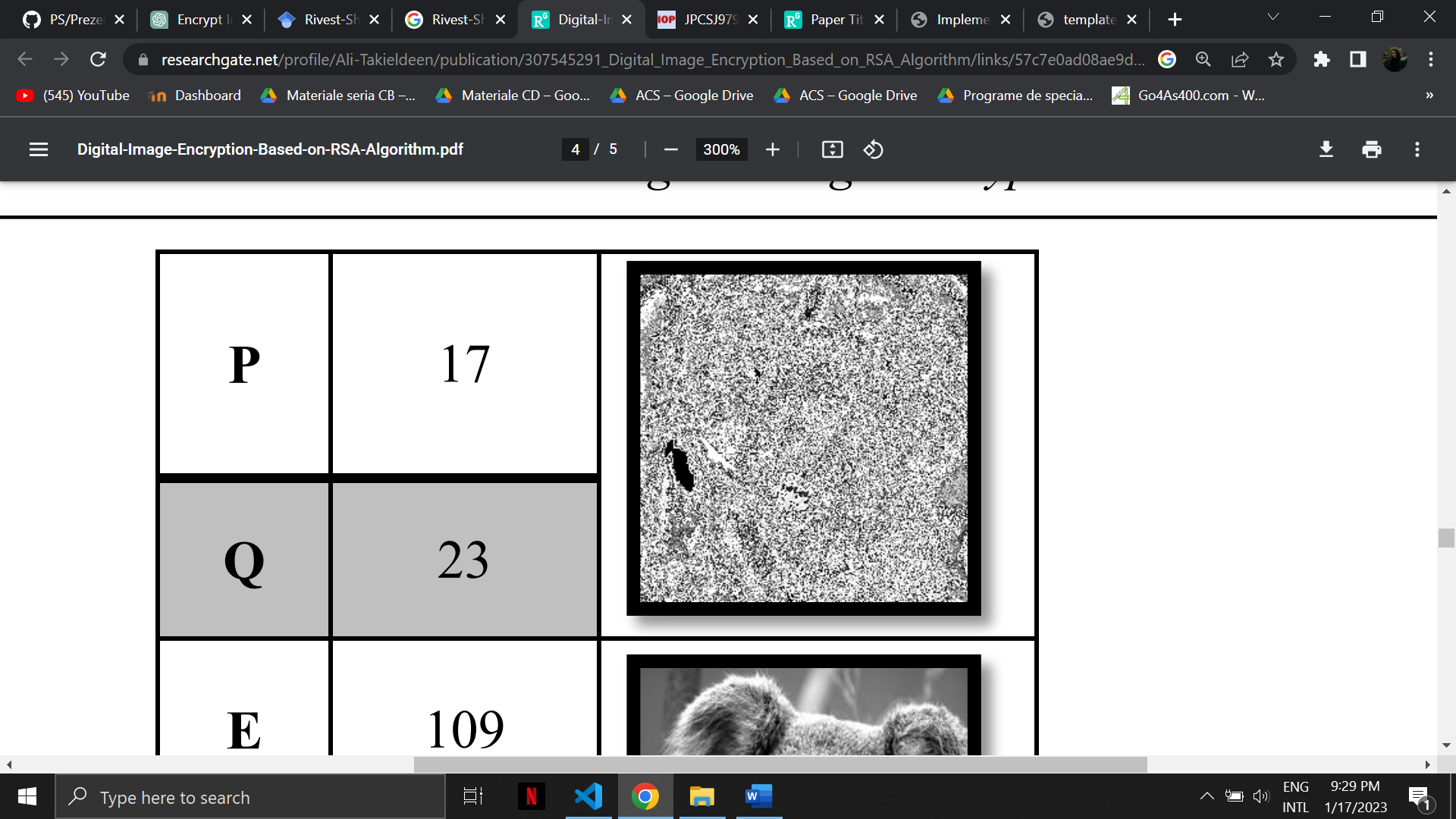
## AES (Advances Encryption Standard)

AES este un algoritm de criptare cu cheie simetrica care este utilizat pe scara larga pentru criptarea imaginilor. Utilizeaza o dimensiune fixa a blocului de 128 de biti si o dimensiune a cheii de 128, 192 sau 256 biti.

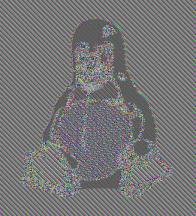
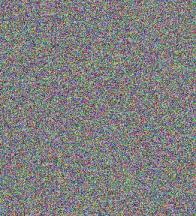
## RSA (Rivest-Shamir-Adleman)

RSA este un algoritm de criptare asimetrica utilizat in mod obisnuit pentru criptarea imaginilor. Foloseste doua chei, o cheie publica pentru criptarea imaginii si o cheie private pentru decriptare.

Graphical user interface

Description automatically generated

## TEA (Tiny Encryption Algorithm)

TEA este un algoritm de criptare cu cheie simetrica care este conceput pentru a fi utilizat in medii cu resurse limitate. Utilizeaza o cheie de 128 de biti si o dimensiune de bloc de 64 de biti.

# Concluzii

Procesul de criptare a unei imagini folosind Hénon-Sine 2D si abordarea DNA implica conversia imaginii intr-o matrice 1D de pixeli, aplicarea unei permutari folosind Hénon-Sine map si apoi DNA mapping pentru a converti pixelii permutati intr-o noua secventa.

Este important de retinut ca aceasta metoda de criptare nu este o metoda utilizata pe scara larga sau consacrata in domeniul criptarii imaginilor si nu ofera o metoda de criptare sigura. In plus, reconstructia imaginii originale este dificila, iar rezultatul acestei metode poate sa isi piarda din calitate.

In locul acestui procedeu, este recomandata folosirea metodei de criptare bazata pe AES, RSA sau alte metode verificate si revizuite de experti in domeniu si sunt considerate sigure.

# Referinte

<https://www.researchgate.net/publication/325954834_Image_encryption_using_2D_Henon-Sine_map_and_DNA_approach>

<https://www.geeksforgeeks.org/advanced-encryption-standard-aes/>

<https://www.geeksforgeeks.org/rsa-algorithm-cryptography/>

<https://www.researchgate.net/publication/320631771_Digital_Image_Encryption_Implementations_Based_on_AES_Algorithm>

<https://www.researchgate.net/publication/307545291_Digital_Image_Encryption_Based_on_RSA_Algorithm>