



UNIVERSITATEA NAȚIONALĂ DE
ȘTIINȚĂ ȘI TEHNOLOGIE
POLITEHNICA BUCUREȘTI



Scoala Doctorală de Electronică, Telecomunicații
și Tehnologia Informației

Decizie nr. 160 din 21-10-2025

REZUMAT TEZĂ DE DOCTORAT

Ing. Adina Elena LUPU (BLAJ)

CONTRIBUȚII PRIVIND TRANSMISIA CRIPTATĂ DE DATE CU
ACCENT PE FOLOSIREA TEORIEI HAOSULUI ÎN CRIPTOGRAFIE

CONTRIBUTIONS ON ENCRYPTED DATA TRANSMISSION WITH
EMPHASIS ON THE USE OF CHAOS THEORY IN
CRYPTOGRAPHY

COMISIA DE DOCTORAT

Prof.dr.ing. Gheorghe BREZEANU

Universitatea Națională de Știință și
Tehnologie POLITEHNICA București

Președinte

Prof. Dr. Ing. Adriana VLAD

Universitatea Națională de Știință și
Tehnologie POLITEHNICA București

Conducător de doctorat

Prof.dr.ing. Victor Adrian

GRIGORAȘ

Universitatea Tehnică „Gheorghe
Asachi” Iași

Referent

Professeur Mihai MITREA

Institut Polytechnique de Paris

Referent

Conf.dr.ing. Șerban Georgică

OBREJA

Universitatea Națională de Știință și
Tehnologie POLITEHNICA București

Referent

BUCUREȘTI 2025

Cuprins

| | |
|--|-----------|
| 1. Introducere | 1 |
| 2. Influența sistemelor dinamice în scheme de criptare bazate pe incluziunea mesajului și funcții de mixare | 3 |
| 2.1 Transformări de mixare și incluziunea mesajului în sisteme haotice | 3 |
| 2.1.1 Introducere | 3 |
| 2.1.2 O privire comparativă asupra sistemelor dinamice pe baza schemei propuse | 4 |
| 2.1.3 Transformări de mixare aplicate extern urmate de includerea mesajului..... | 6 |
| 2.1.4 Transformări de mixare prin includerea mesajului | 7 |
| 2.1.5 Concluzii | 8 |
| 2.2 Studiu asupra influenței parametrilor de control în construcția transformărilor de mixare..... | 9 |
| 2.2.1 Introducere | 9 |
| 2.2.2 Studiu experimental asupra influenței parametrilor de control | 9 |
| 2.2.3 Extinderea funcției de mixare | 10 |
| 2.2.4 Concluzii | 11 |
| 3. Analiza comportamentului statistic al unui sistem haotic în cazul incluziunii mesajului pentru aplicații în criptografie | 12 |
| 3.1 Introducere..... | 12 |
| 3.2 Descrierea schemei bazată pe comutatorul de decizie..... | 13 |
| 3.2.1 Descrierea funcțională a schemei..... | 13 |
| 3.2.2 Rolul comutatorului de decizie în schema de procesare | 13 |
| 3.3 Evaluarea impactului incluziunii asupra comportamentului statistic al sistemului haotic | 14 |
| 3.3.1 Descrierea modului de lucru | 14 |
| 3.3.2 Rezultate experimentale | 14 |
| 3.3.3 Determinarea limitei superioare a magnitudinii factorului de scalare..... | 15 |
| 3.4 Analiza comportamentului statistic al sistemului dinamic în vederea unor aplicații criptografice..... | 16 |
| 3.5 Concluzii..... | 17 |
| 4. Studiu comparativ asupra criptării prin includerea mesajului în sisteme haotice precedată de transformări externe..... | 18 |
| 4.1 Introducere..... | 18 |
| 4.2 Descrierea operațională a schemei de criptare cu transformări externe | 18 |
| 4.3 Studiu comparativ asupra metodelor de criptare | 20 |

| | |
|---|-----------|
| 4.3.1 Mod de lucru | 20 |
| 4.3.2 Evaluarea schemei de criptare folosind funcția Hénon | 20 |
| 4.3.3 Evaluarea schemei de criptare folosind funcția cort | 21 |
| 4.4 Concluzii..... | 21 |
| 5. Evaluarea pRNG-urilor bazate pe sisteme haotice folosind teste NIST, exponenți Lyapunov și diagrame de bifurcație | 22 |
| 5.1 Introducere..... | 22 |
| 5.2 Aprofundarea pRNG-ului bazat pe sistemul Hénon generalizat | 23 |
| 5.3 Extinderea studiului pentru alte pRNG-uri bazate pe haos din literatură | 24 |
| 5.4 Concluzii..... | 24 |
| 6. Concluzii | 25 |
| 6.1 Concluzii și contribuțiile personale | 25 |
| 6.2 Listă de publicații | 27 |
| Bibliografie | 28 |

Capitolul 1

Introducere

Subiectul principal al tezei cu titlul „Contribuții privind transmisia criptată de date cu accent pe folosirea teoriei haosului în criptografie” este aducerea de noi contribuții în domeniul criptografiei bazate pe sisteme haotice, cu scopul de a spori robustețea și gradul de încredere privind schemele de criptare bazate pe haos. Influența și analiza comportamentului sistemelor haotice în aplicațiile criptografice constituie tema principală de cercetare a acestei teze. Aplicațiile criptografice ale sistemelor haotice reprezintă un subiect de cercetare răspândit în literatura de specialitate [1]-[3]. Cele mai des întâlnite aplicații ale sistemelor haotice în criptografie sunt construcția de generatoare de numere pseudo-aleatoare (pRNG), spre exemplu [4]-[7] și criptarea imaginilor, spre exemplu [8]-[11].

În Capitolul 2, în Secțiunea 2.1 ne propunem să determinăm care este aportul sistemelor dinamice în scheme de criptare bazate pe incluziunea mesajului [15], [16]. Sunt adresate următoarele două aspecte: 1) Care este aportul individual al sistemului dinamic în schema de criptare cu incluziunea mesajului? și 2) Cum se poate realiza o bună criptare într-un cadru de lucru cu funcții de mixare și incluziunea mesajului și în aceste condiții, care este contribuția incluziunii mesajului? Pentru exemplificare au fost alese trei sisteme haotice des întâlnite în literatură: funcția Hénon, funcția logistică, funcția cort și au fost folosite funcțiile de mixare sugerate de Shannon [17] pentru a realiza procesările adiționale ale mesajului. În Secțiunea 2.2 este urmărită construcția funcțiilor de mixare cu sisteme haotice având în vedere influența parametrilor de control asupra performanțelor de criptare. Sistemele haotice alese pentru construcția funcției de mixare sunt funcția logistică și funcția Hénon, dar pot fi folosite și alte sisteme dinamice. Alegerea parametrilor de control ai sistemului dinamic este de interes și a fost urmărită în acest studiu, întrucât în criptografia bazată pe haos, parametrii de control pot fi componente ale cheii secrete [18]. Creșterea securității schemelor de criptare bazate pe transformări de mixare cu sisteme dinamice prin extinderea spațiului cheilor este principala contribuție a acestei cercetări.

Capitolul 3 analizează din punct de vedere statistic proprietățile unui sistem haotic în cazul incluziunii mesajului pentru aplicații în criptografie. Păstrarea proprietăților sistemului haotic este esențială pe tot parcursul procesului de criptare [19]. O contribuție importantă a acestui capitol este ilustrarea unei modalități de evaluare statistică a schemelor de procesare cu sisteme dinamice bazate pe incluziunea mesajului și propunerea unui cadru de lucru pentru păstrarea comportamentului dinamic al sistemului. Ilustrarea este realizată pe sistemul dinamic descris de funcția logistică, în aplicații criptografice bazate pe imagini. Pentru a verifica dacă proprietățile statistice ale noului sistem obținut sunt sau nu afectate de incluziune este efectuată analiza Monte Carlo a testului statistic Kolmogorov-Smirnov. De asemenea, este determinată limita superioară a magnitudinii factorului de scalare, pentru care proprietățile statistice ale sistemului nu se modifică prin incluziune. Analiza statistică este aplicată și în cazul în care se adaugă în schemă funcții criptografice de mixare aplicate intern cu scopul utilizării acestei scheme în aplicații criptografice. Astfel prin utilizarea funcțiilor de mixare și adăugarea unui comutator de decizie, schema de criptare propusă și analizată în acest capitol este una completă oferind rezultate optime din punct de vedere criptografic și, în același timp păstrând proprietățile statistice ale sistemului dinamic [29].

În Capitolul 4 al tezei este prezentat un studiu comparativ asupra criptării imaginilor prin incluziunea mesajului în sisteme haotice precedată de procesări externe. Este propusă o schemă generică de criptare ce cuprinde un bloc de pre-procesare a mesajului original, un bloc de discretizare a sistemului haotic și în final procesul de incluziune al mesajului în evoluția sistemului haotic. Scopul acestui studiu este de a evalua care sunt configurațiile adecvate ale acestei scheme (din punct de vedere al alegerii sistemului haotic folosit și al metodei de pre-procesare) pentru a obține o criptare sigură și eficientă a imaginilor. Se propun spre analiză sistemul Hénon 3D și funcția cort, iar pentru blocul de pre-procesare externă funcțiile de mixare și transformările wavelet. Pentru a evalua și compara rezultatele imaginilor criptate se folosesc metrici de analiză precum: histograma, corelația pixelilor adiacenți și entropia.

Capitolul 5 abordează subiectul generatoarelor de numere pseudo-aleatoare bazate pe haos în contextul utilizării acestora în aplicații criptografice. Ne propunem să validăm corelația dintre rezultatele testelor NIST și metricile specifice teoriei haosului precum diagrama de bifurcație [12] și exponenții Lyapunov [13] pornind de la un studiu existent [14]. În Secțiunea 5.2 este extinsă o analiză a spațiului seed-urilor (condițiile inițiale și parametrii de control) pentru pRNG-ul bazat pe Hénon map din [14] prin determinarea exponenților Lyapunov pentru alte intervale ale parametrilor de control și micșorarea pasului de calcul. Pentru secvențele generate se aplică testele NIST și se evaluează corespondența dintre rezultatele suitei de teste și valoarea celui mai mare exponent Lyapunov. Secțiunea 5.3 urmărește aplicarea acestei metode și pentru alte trei pRNG-uri bazate pe haos din literatură. Se urmărește corelația dintre metricile specifice haosului și rezultatele testelor NIST. De asemenea, aceste pRNG-uri sunt evaluate în aplicații criptografice în scheme de tip one-time-pad, ilustrate pe imagini. Studiul din acest capitol este folositor utilizatorilor de pRNG-uri bazate pe haos pentru stabilirea unui spațiu extins și corect de selecție a seed-urilor.

În Capitolul 6 sunt prezentate concluziile, contribuțiile personale și lista lucrărilor publicate.

Capitolul 2

Influența sistemelor dinamice în scheme de criptare bazate pe incluziunea mesajului și funcții de mixare

Acest capitol analizează influența sistemelor dinamice în scheme de criptare bazate pe incluziunea mesajului și funcții de mixare. Rezultatele cercetării au fost publicate în două articole de conferință [25], [26].

2.1 Transformări de mixare și incluziunea mesajului în sisteme haotice

2.1.1 Introducere

În cadrul acestui studiu este realizată o cercetare referitoare la utilizarea în criptografie a funcțiilor de mixare, beneficiind și de includerea mesajului într-un sistem dinamic. Studiul vizează următoarele aspecte principale: 1) care este aportul individual al sistemului dinamic în schema de criptare cu incluziunea mesajului ? și 2) cum se poate realiza o bună criptare într-un cadru de lucru cu funcții de mixare și incluziunea mesajului și în aceste condiții, care este contribuția incluziunii mesajului?

Rezultatele acestei cercetări pot fi utilizate în aplicații criptografice bazate pe haos [27], sau pentru construirea funcțiilor de mixare. Studiul este exemplificat pe imagini, dar poate fi aplicat și pe alt conținut multimedia. Cele trei sisteme haotice selectate pentru studiu sunt: funcția Hénon [31], funcția logistică [12] și funcția cort [32].

2.1.2 O privire comparativă asupra sistemelor dinamice pe baza schemei propuse

În continuare este evaluată și comparată performanța independentă a celor trei sisteme haotice descrise anterior în procesarea de imagini. Pentru acest studiu a fost propusă următoarea schemă ilustrată în Figura 2.1.

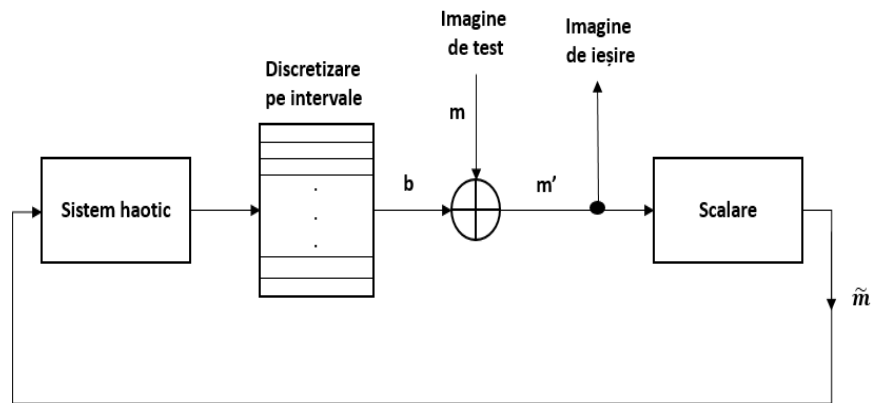


Figura 2.1 Schema de procesare (cu includerea mesajului) propusă

Funcționarea schemei de procesare este descrisă de pașii următori. Pornind de la un set de condiții inițiale, sistemul haotic este iterat. La fiecare iterație valoarea de ieșire a sistemului haotic este transformată într-un octet, b . Se efectuează o operație XOR pe biți între octetul b și reprezentarea pe 8 biți a unui pixel din mesaj, m . Rezultatul operației XOR, notat cu m' , este considerat ieșirea schemei de procesare. Rezultatul m' este scalat cu un factor v . Mesajul procesat și scalat este inclus în evoluția sistemului haotic și se continuă iterarea sistemului.

Pentru exemplificare a fost aleasă o imagine de test cu entropie mică, ilustrată în Figura 2.2.

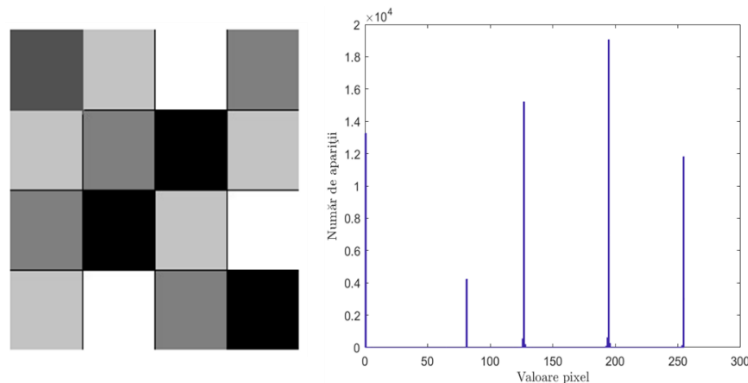


Figura 2.2 Imaginea de test și histograma sa corespunzătoare

Rezultatele procesării imaginii folosind fiecare dintre cele trei sisteme haotice sunt prezentate în Figura 2.3, Figura 2.4 și Figura 2.5. Această etapă de procesare este ilustrată doar pentru a evidenția contribuția sistemului dinamic prin incluziunea mesajului. Se poate observa ca rezultat o transformare vizuală, mai accentuată pentru funcția logistică și funcția cort și scăzută pentru funcția Hénon.

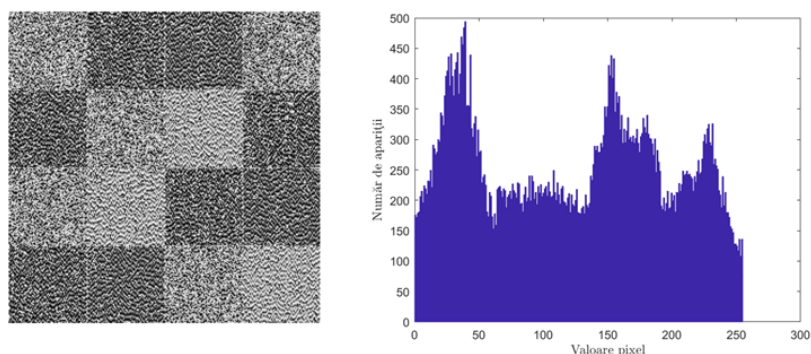


Figura 2.3 Imaginea criptată (procesată) folosind funcția Hénon și histograma corespunzătoare

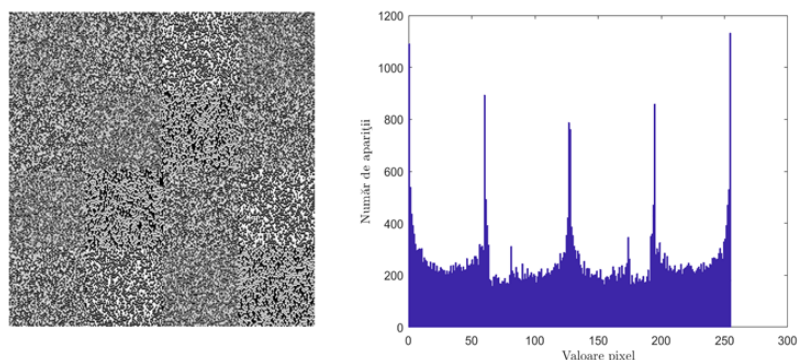


Figura 2.4 Imaginea criptată (procesată) folosind funcția logistică și histograma corespunzătoare

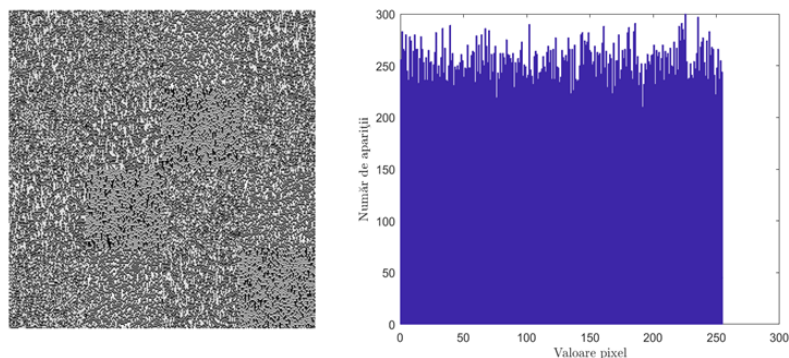


Figura 2.5 Imaginea criptată (procesată) folosind funcția cort și histograma corespunzătoare

2.1.3 Transformări de mixare aplicate extern urmate de includerea mesajului

Problema lipsei de difuzie, observată anterior, este abordată prin adăugarea unui bloc de preprocesare pe baza sugestiilor lui Shannon, folosind transformările de mixare [17]. Imaginea de test din Figura 2.2 este procesată folosind următorul lanț de transformări:

$$T_k F S_j \quad (2.1)$$

unde T_k și S_j pot fi cifruri simple de tip transpoziție sau substituție, urmate de funcția de mixare F , care asigură difuzia și confuzia. Procesul de incluziune poate fi considerat ca fiind punctul final al lanțului de criptare, în care sistemul dinamic acționează ca o metodă de substituție. Pentru funcția de mixare F , considerăm mai întâi o formulă simplificată:

$$F = SLT \quad (2.2)$$

și apoi o extindem în conformitate cu sugestiile lui C.E. Shannon [17]:

$$F = LSLSLT \quad (2.3)$$

unde T și S reprezintă tehnici de transpoziții și substituții, iar L este un operator de mediere liniară, construit pornind de la sugestiile lui Shannon și aplicat în forma descrisă în [28]:

$$y(j) = \sum_{i=0}^{P-1} x_{j+i} \bmod q; j=1, \dots, N-P \quad (2.4)$$

și pentru ultimele P caractere (pixeli), $y(j) = x(j)$, $j=N-P+1, \dots, N$.

Schema de criptare cu transformări de mixare aplicate extern și includerea mesajului este exemplificată în Figura 2.6.

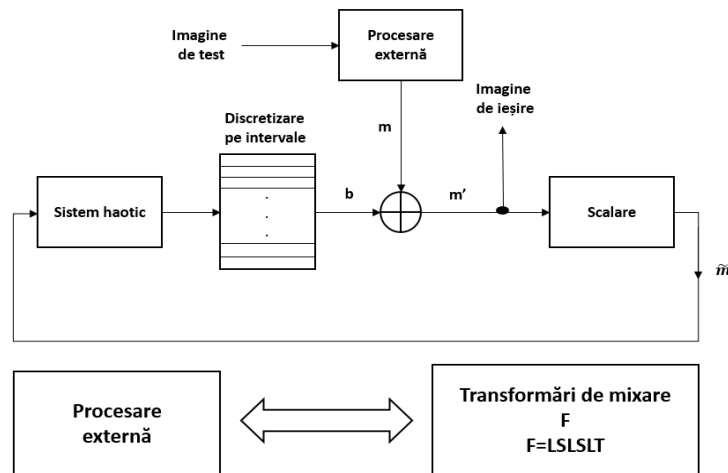


Figura 2.6 Schema de procesare cu transformări de mixare aplicate extern urmată de incluziunea mesajului

Studiul experimental a arătat că performanțele criptării s-au îmbunătățit semnificativ când se utilizează funcții de mixare extinse (2.3), histogramele rezultate sunt uniforme indiferent de sistemul haotic utilizat. În această etapă, rolul sistemului

dinamic este acela de bloc de criptare în extinderea transformărilor de mixare, în care condițiile inițiale și parametrii de control fac parte din cheia secretă.

2.1.4 Transformări de mixare prin includerea mesajului

În această secțiune funcția de mixare este realizată intern. Este folosit doar operatorul de mediere liniară L , restul transformărilor fiind asigurate de sistemul dinamic care funcționează ca o substituție multiplă. Această schemă de procesare este ilustrată în Figura 2.7.

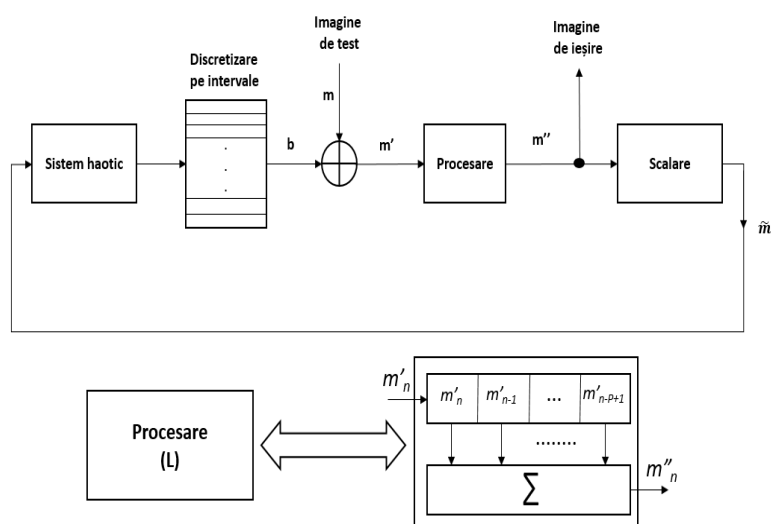


Figura 2.7 Schema de procesare cu transformări de mixare aplicate intern

Rezultatele sunt prezentate în Figura 2.8, Figura 2.9 și Figura 2.10. Schema cu transformări de mixare aplicate intern asigură o difuzie și o confuzie sporită, indiferent de sistemul haotic utilizat. Această schemă este mai eficientă decât cea din Secțiunea 2.1.3, deoarece funcția de mixare constă într-o singură operație de mediere liniară.

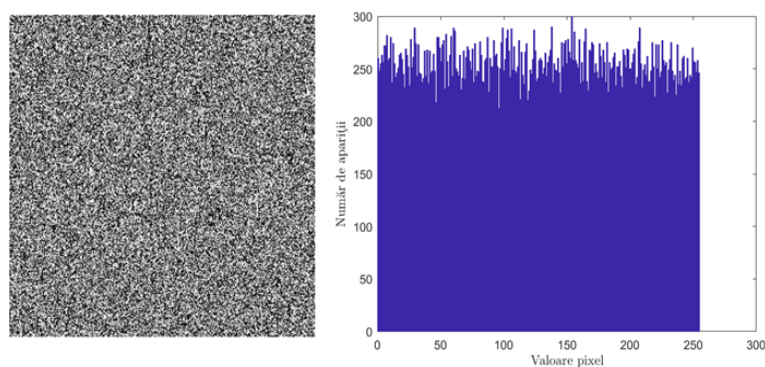


Figura 2.8 Imaginea criptată cu funcții de mixare aplicate intern folosind funcția Hénon și histograma corespunzătoare

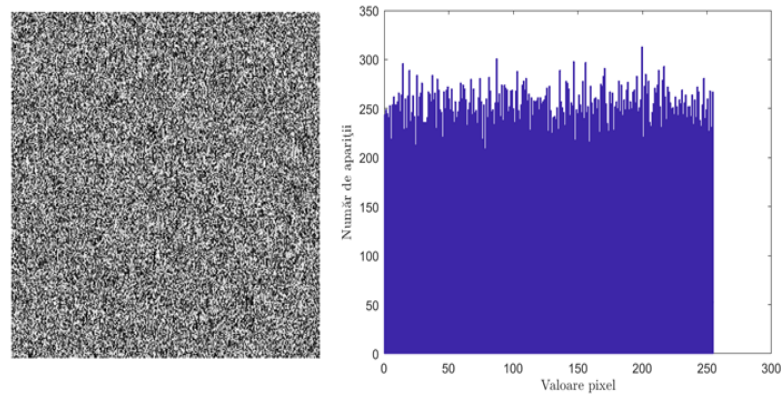


Figura 2.9 Imaginea criptată cu funcții de mixare aplicate intern folosind funcția logistică și histograma corespunzătoare

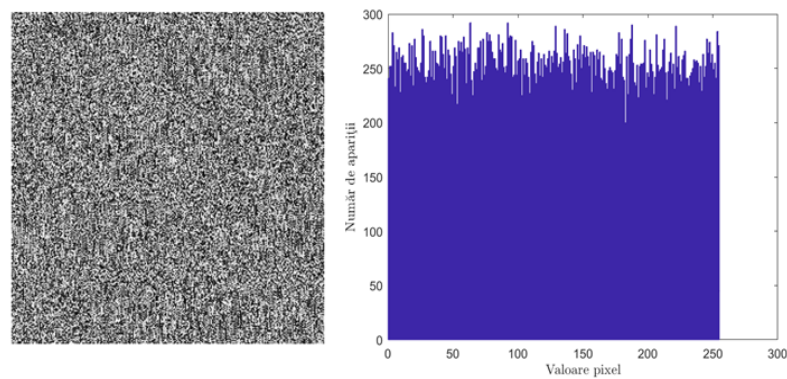


Figura 2.10 Imaginea criptată cu funcții de mixare aplicate intern folosind funcția cort și histograma corespunzătoare

2.1.5 Concluzii

Studiul a arătat că există unele diferențe între sistemele dinamice în care se realizează includerea mesajului. Aceste diferențe se atenuează pe măsură ce se adaugă în schema de procesare funcții criptografice de mixare care sporesc confuzia și difuzia. Se propune o construcție diferită a funcțiilor de mixare, păstrând din sugestiile lui Shannon doar operatorul de mediere liniară, L , restul transformărilor fiind asigurate de contribuția sistemului dinamic. Astfel, s-a obținut un rezultat care poate fi interesant din perspectiva obținerii unor funcții de mixare eficiente folosind participarea directă a sistemului dinamic în arhitectura acestor funcții.

2.2 Studiu asupra influenței parametrilor de control în construcția transformărilor de mixare

2.2.1 Introducere

Contribuția acestui studiu este de a evalua experimental comportamentul schemelor de criptare descrise în 2.1.2 și 2.1.4 pentru diferite valori ale parametrilor de control, măbind astfel spațiul cheilor secrete. De asemenea, este propusă dezvoltarea construcției unei funcții de mixare extinse pentru a îmbunătăți securitatea schemei de criptare. Sistemele haotice analizate sunt funcția logistică și funcția Hénon. Au fost alese alte valori ale parametrilor de control decât cele uzuale din literatură, pentru care sistemul dinamic are comportament haotic: pentru funcția logistică $R \in \{3.7, 3.8, 3.9\}$, iar pentru funcția Hénon, perechile de parametri de control $(a, b) \in \{(1.5, 0.1); (1.6, 0.1); (1.7, 0.1)\}$.

2.2.2 Studiu experimental asupra influenței parametrilor de control

Studiul este analizat progresiv în două scenarii. În primul scenariu este evaluată contribuția individuală a sistemului dinamic în procesul de criptare. În al doilea scenariu sistemul dinamic lucrează ca parte a funcției de mixare. În ambele cazuri schemele de procesare folosite sunt cele din [25], descrise în secțiunea 2.1.2 și 2.1.4.

Pentru primul scenariu, s-a observat că atât pentru funcția Hénon, cât și pentru funcția logistică, rolul sistemului dinamic nu este semnificativ pentru valorile parametrilor de control selectate. Difuzia și confuzia imaginii criptate lipsesc. Aportul individual al sistemului dinamic în criptarea imaginii este scăzut chiar dacă sistemul funcționează în regimul haotic.

În al doilea scenariu este introdusă o operație de mediere liniară L care împreună cu sistemul haotic formează o nouă funcție de mixare $F = SL$ unde substituția este asigurată de operația XOR care este influențată de valorile sistemului dinamic. Rezultatele experimentale obținute pentru funcția logistică sunt ilustrate în Figura 2.11, iar cele pentru funcția Hénon în Figura 2.12. Putem observa că distribuția pixelilor este uniformă pentru funcția logistică $R = 3.9$ și pentru funcția Hénon pentru perechea $(a, b) = (1.7; 0.1)$. Pentru celelalte valori ale parametrilor de control considerate în studiu, histograma imaginilor criptate nu prezintă o distribuție uniformă.

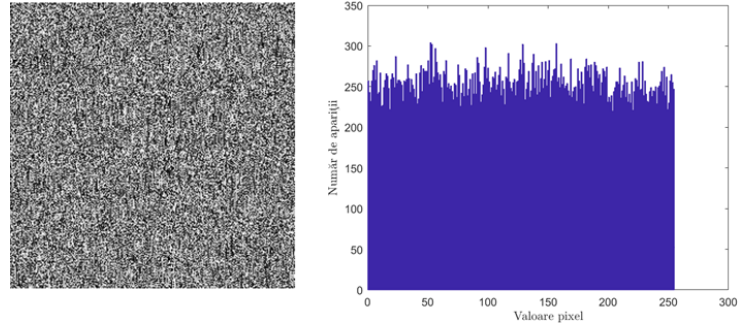


Figura 2.11 Rezultate Scenariu 2 pentru funcția logistică: $R=3.9$

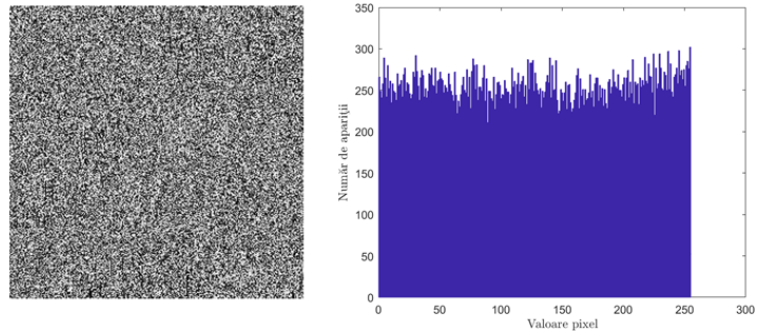


Figura 2.12 Rezultate scenariu 2 pentru funcția Hénon: $a=1.7$

2.2.3 Extinderea funcției de mixare

Pentru a obține o bună criptare pentru toate valorile parametrilor de control evaluate, se introduce în schema de procesare un nouă operație de mediere liniară L , obținând schema din Figura 2.13. Această operație este introdusă înaintea operației de substituție. Astfel se obține o nouă funcție de mixare definită ca $F = LSL$.

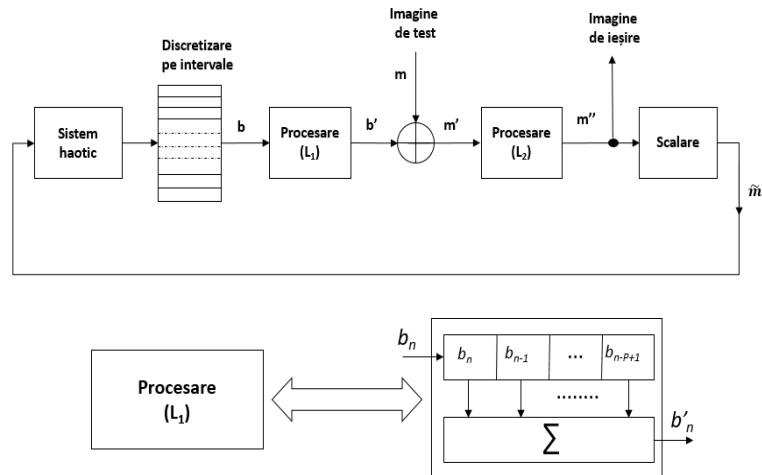


Figura 2.13 Schema de procesare cu funcția de mixare extinsă

Rezultatele criptării imaginii de intrare sunt prezentate în Figura 2.14 pentru funcția logistică pentru $R = 3.7$ și în Figura 2.15 pentru funcția Hénon pentru perechea $(a, b) = (1.5, 0.1)$. Prin extinderea funcției de mixare cu încă o operație de mediere liniară L_1 , rezultatele criptării sunt bune pentru tot setul de parametri de control considerați.

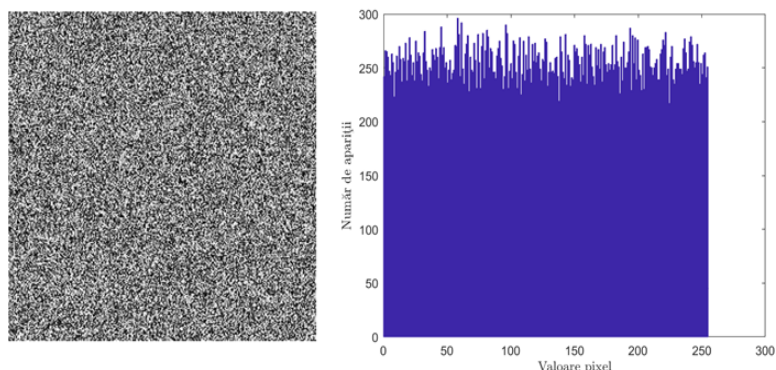


Figura 2.14 Rezultate funcție extinsă pentru funcția logistică: $R=3.7$

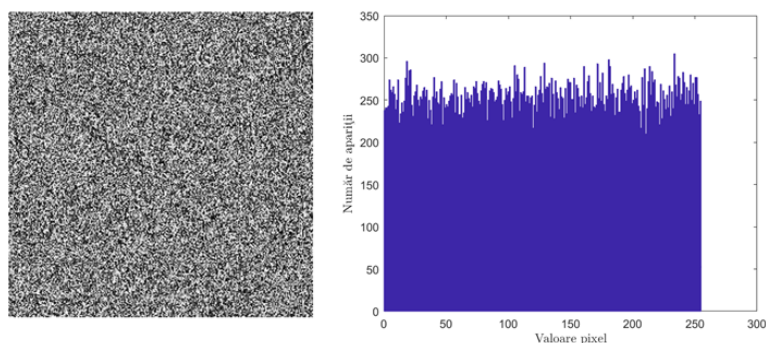


Figura 2.15 Rezultate funcție extinsă pentru funcția Hénon: $a=1.5$

2.2.4 Concluzii

În cazul în care procesarea în schema de criptare este asigurată doar de sistemul haotic, se poate observa că rezultatele criptării sunt diferite în funcție de alegerea parametrului de control, iar criptarea imaginii este slabă, chiar dacă sistemul funcționează în regimul haotic. Adăugând în schema de procesare o operație de mediere liniară L , rezultatele experimentale arată că alegerea parametrilor de control nu mai influențează în aceeași măsură rezultatele criptării, însă rezultatele pot fi îmbunătățite. În final, schema de procesare este îmbunătățită prin utilizarea a două operații de mediere liniară și o substituție, obținând astfel o funcție de mixare extinsă $F = LSL$ care oferă performanțe bune pentru diferite valori ale parametrilor de control. Securitatea schemei de criptare este sporită astfel prin creșterea spațiului cheilor. Aceste rezultate încurajează utilizarea și a altor sisteme haotice în construcția funcțiilor de mixare.

Capitolul 3

Analiza comportamentului statistic al unui sistem haotic în cazul incluziunii mesajului pentru aplicații în criptografie

În acest capitol este realizată o analiză statistică asupra comportamentului unui sistem dinamic în cazul incluziunii mesajului. Rezultatele cercetării au fost publicate într-un articol de revistă [29].

3.1 Introducere

Păstrarea proprietăților sistemului haotic este esențială pe tot parcursul procesului de criptare [19]. Măsura în care comportamentul sistemului dinamic este afectat de incluziune este importantă. Astfel, un obiectiv principal al cercetării prezentate în acest capitol este de a clarifica impactul incluziunii asupra comportamentului statistic al semnalului haotic. Toată analiza de detaliu este efectuată pe o schema de criptare originală. În schema propusă, sistemul dinamic ales este funcția logistică, deoarece este ilustrativă pentru analiza statistică prin raportarea la cunoașterea legii de probabilitate pentru $R = 4$ (densitatea de probabilitate și funcția de repartiție sunt cunoscute).

3.2 Descrierea schemei bazată pe comutatorul de decizie

3.2.1 Descrierea funcțională a schemei

În Figura 3.1, la fiecare iterație, ieșirii x'_{k+1} a sistemului haotic îi este asociat un octet s_k . Se efectuează o operație XOR pe biți între s_k și octetul m_k al mesajului de intrare. Se obține octetul m'_k , acesta reprezentând ieșirea schemei de procesare. Octetul m'_k este transformat în număr întreg și scalat cu factorul F , pentru a putea fi reintrodus în evoluția sistemului dinamic. Valoarea obținută este notată cu \tilde{m}'_k . Următorul pas este cel de efectuare a deciziei de incluziune a mesajului procesat și scalat \tilde{m}'_k . Decizia depinde de valoarea x'_{k+1} .

$$\tilde{m}_k = \begin{cases} \tilde{m}'_k, & \text{dacă } x'_{k+1} \in [0, D) \\ 0, & \text{dacă } x'_{k+1} \in [D, 1) \end{cases}, \quad \text{unde } D = 1 - 255 \cdot F \quad (3.1)$$

În continuare, \tilde{m}_k este adăugat în evoluția sistemului. Astfel, se obține un nou sistem, unde $x_0, x_1, x_2, \dots, x_k$ reprezintă valorile de intrare, iar $x'_1, x'_2, x'_3, \dots, x'_{k+1}$, sunt valorile intermediare de ieșire ale acestuia.

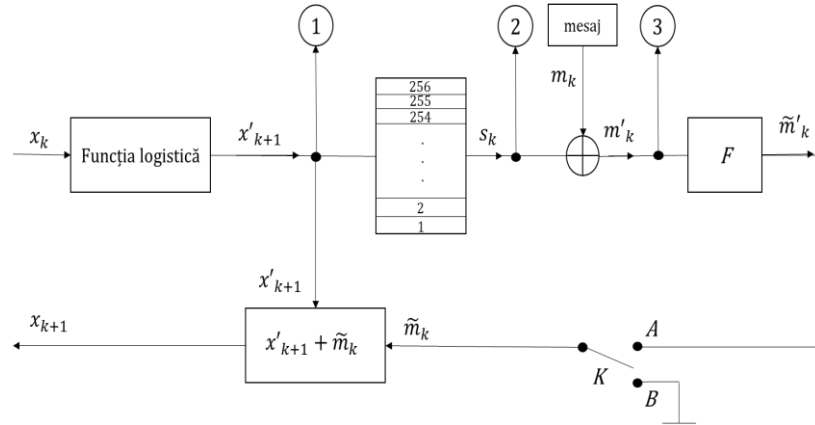


Figura 3.1 Schema de incluziune a mesajului

3.2.2 Rolul comutatorului de decizie în schema de procesare

Pentru a ne asigura că sistemul dinamic își menține comportamentul haotic după incluziunea mesajului (procesat și scalat), este necesar ca valorile $x_1, x_2, x_3, \dots, x_{k+1}$ să se mențină în domeniul de definiție $[0, 1]$ al funcției logistice. Din acest motiv, a fost introdus în schema de procesare un comutator de decizie K care este activat de pragul de decizie D . Acest comutator controlează incluziunea și determină valorile lui \tilde{m}_k . Astfel:

- Dacă $x'_{k+1} \in [D, 1)$, atunci $\tilde{m}_k = 0$, nu se face incluziune; comutatorul K este în poziția B
- Dacă $x'_{k+1} \in (0, D)$, atunci, $\tilde{m}_k = \widetilde{m}'_k = m'_k \cdot F$ se face incluziune; comutatorul K este în poziția A

Valoarea pragului de decizie D este egală cu valoarea maxim admisibilă a lui x'_{k+1} pentru care adăugând valoarea maxima a lui \tilde{m}_k , x_{k+1} să nu depășească 1.

3.3 Evaluarea impactului incluziunii asupra comportamentului statistic al sistemului haotic

3.3.1 Descrierea modului de lucru

Pentru început vom considera că valoarea mesajului extern este 0 și bucla de incluziune nu este luată în considerare (întrerupătorul K din Figura 3.1 este în poziția B). Acest scenariu reprezintă *scenariul de referință*, deoarece în acest caz schema reprezintă sistemul dinamic descris de funcția logistică fără nicio altă intervenție. Rezultatele acestui scenariu (punctele de observație marcate pe schemă cu **1** și **2**) vor fi folosite pentru comparație în *scenariul de studiu* care va lua în considerare afectarea sistemului dinamic prin incluziune.

În punctul de observație **1** se poate urmări procesul aleator asociat funcției logistice, mai exact, urmărim traiectoriile (realizările particulare ale procesului aleator). Analiza urmărește dacă prin incluziune este afectată legea de probabilitate a sistemului haotic prin realizarea unei analize Monte Carlo a testului Kolmogorov-Smirnov. În acest studiu am ales $N = 10000$ traiectorii, $k = 150$ și pragul de semnificație statistică al testului Kolmogorov-Smirnov, $\alpha = 0.05$. Conform teoriei estimării [30], pentru $\alpha = 0.05$ și folosind analiza Monte Carlo prin reluarea testului statistic pentru $L = 500$ de ori, intervalul de proporții acceptate este $[0.93; 0.97]$.

În punctul de observație **2** achiziționăm datele reprezentând traiectoria sistemului haotic după discretizare. Această traiectorie apare ca o succesiune de octeți și o reprezentăm ca imagine și analizăm histograma corespunzătoare. În punctul de observație **3** se inspectează vizual imaginea de ieșire a schemei de criptare și histograma acesteia.

3.3.2 Rezultate experimentale

Pentru *scenariul de referință* procentul de acceptare a ipotezei H_0 obținut a fost de 94,8%. Acesta se află în intervalul de estimare $[0.93; 0.97]$. Așadar, putem afirma cu o încredere statistică de 95% că datele experimentale provin de la legea de probabilitate teoretică a funcției logistice pentru $R = 4$.

Pentru exemplificarea *scenariului de studiu* considerăm mesajul extern o imagine de dimensiune 256 x 256 pixeli. Pentru *scenariul de studiu* procentul de acceptare a ipotezei H_0 obținut a fost de 95.8%. Analizând Figura 3.2 se poate afirma că densitatea de probabilitate experimentală a noului sistem dinamic este similiară cu densitatea de probabilitate teoretică a funcției logistice.

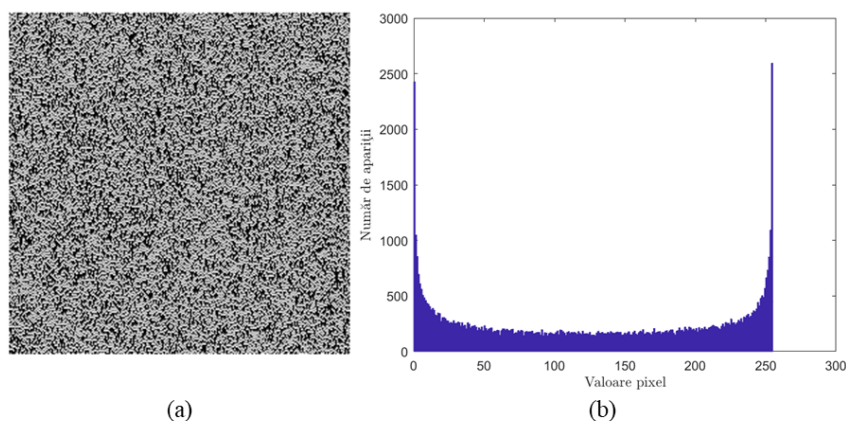


Figura 3.2 (a) Imaginea în punctul de observație 2 și (b) histograma corespunzătoare – scenariul de studiu

În concluzie, comportamentul statistic al noului sistem obținut prin incluziunea mesajului respectă legea de probabilitate de ordinul 1 a procesului aleator asociat funcției logistice. La acest fapt contribuie atât adăugarea comutatorului de decizie în schema de procesare, cât și o bună alegere a factorului de scalare.

3.3.3 Determinarea limitei superioare a magnitudinii factorului de scalare

Ne propunem să determinăm limitele magnitudinii factorului de scalare, F , astfel încât să permită funcționarea schemei în intervalul de definiție al funcției logistice și să nu modifice proprietățile statistice ale acesteia. Pentru un set de valori ale lui F , am aplicat o analiză Monte Carlo reluând testul Kolmogorov-Smirnov de 500 ori pentru fiecare valoare a lui F .

Tabelul 3.1 Analiza Monte Carlo rezultate test Kolmogorov-Smirnov (K-S) pentru dimensiuni diferite ale factorului de scalare

| F | 10^{-5} | 10^{-6} | 10^{-7} | 10^{-8} | 10^{-9} | 10^{-10} | 10^{-11} | 10^{-12} | 10^{-13} |
|-----|-----------|-----------|-----------|-----------|-----------|------------|------------|------------|------------|
| K-S | 0% | 26.4% | 91.2% | 94.6% | 95.2% | 96.4% | 94.6% | 94.8% | 95,8% |

Analizând rezultatele obținute în Tabelul 3.1, se poate afirma că limita superioară a factorului de scalare determinată experimental este 10^{-8} .

3.4 Analiza comportamentului statistic al sistemului dinamic în vederea unor aplicații criptografice

În schema din Figura 3.1 au fost introduse funcții de mixare aplicate intern pentru îmbunătățirea performanțelor criptării, rezultând o nouă schemă de criptare ilustrată în Figura 3.3.

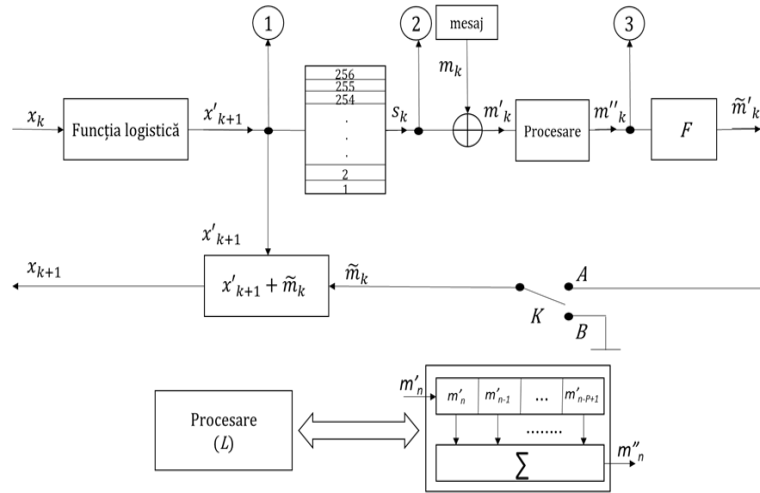


Figura 3.3 Schema de procesare cu transformări de mixare aplicate intern

Utilizarea funcției de mixare în această configurație are ca rezultat o accentuare a proprietăților de difuzie și confuzie prin folosirea doar a unei singure operații de mediere liniară [25]. Procentul de acceptare a ipotezei H_0 obținut a fost de 95.2%. În Figura 3.4 se observă că histograma imaginii din punctul de observație 2 urmează legea de probabilitate de ordinul 1 a funcției logistice. Inspectând vizual Figura 3.5 se poate afirma că performanțele schemei de criptare ce include funcții de mixare sunt vizibil îmbunătățite în comparație cu cele ale schemei de criptare ilustrate în Figura 3.1.

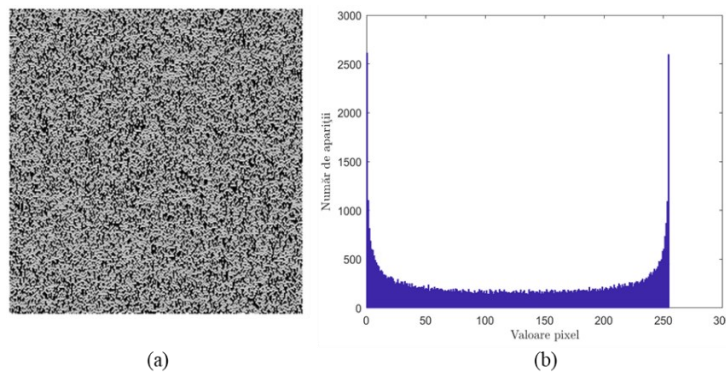


Figura 3.4 (a) Imaginea în punctul de observație 2 și (b) histograma corespunzătoare pentru schema îmbunătățită

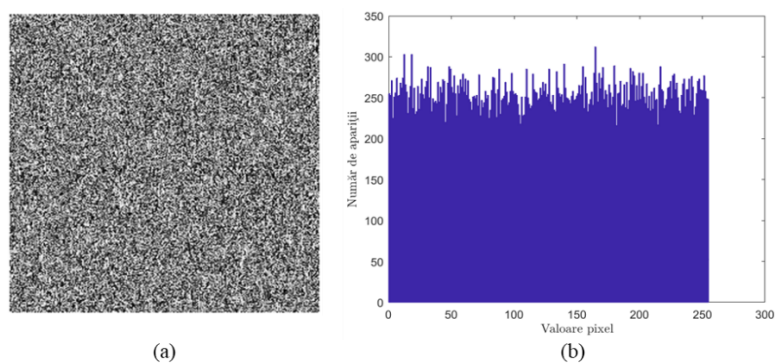


Figura 3.5 (a) Imaginea în punctul de observație 3 și (b) histograma corespunzătoare pentru schema îmbunătățită

Așadar, prin includerea funcțiilor de mixare și adăugarea comutatorului de decizie, schema de criptare propusă și analizată în acest capitol este una completă oferind rezultate optime din punct de vedere criptografic și, în același timp, păstrând proprietățile statistice ale sistemului dinamic.

3.5 Concluzii

În concluzie, principala contribuție a acestui studiu este de a propune un cadru de lucru și de analiză pentru buna funcționare a schemelor de criptare bazate pe haos ce folosesc tehnica incluziunii mesajului. Se pune în valoare și aplicabilitatea în criptografie a schemei de procesare propuse.

Capitolul 4

Studiu comparativ asupra criptării prin includerea mesajului în sisteme haotice precedată de transformări externe

4.1 Introducere

În acest capitol al tezei este prezentat un studiu comparativ asupra criptării imaginilor folosind includerea mesajului în sisteme haotice precedată de transformări externe. Cele două metode de transformări externe analizate sunt bazate pe transformata wavelet și transformări de mixare folosind operații de mediere liniară. Sistemele haotice folosite sunt funcția Hénon și funcția cort, utilizate și în capitolul 2.

4.2 Descrierea operațională a schemei de criptare cu transformări externe

Schema generică de criptare a mesajului este prezentată în Figura 4.1. Inițial imaginea de intrare este introdusă într-un bloc de pre-procesare obținându-se o nouă imagine numită în continuare imaginea pre-criptată. Sistemele haotice folosite sunt funcția Hénon și funcția cort. Modul de operare al schemei este descris în detaliu în *Secțiunea 3.2*. În continuare sunt detaliate cele două metode de pre-criptare. În Figura 4.2 este ilustrat modul de pre-procesare folosind transformata wavelet. Primul pas în pre-procesarea externă folosind transformata wavelet este descompunerea imaginii de test

în pachete wavelet pe 7 nivele folosind funcția wavelet Haar. Coeficienții pachetelor wavelet sunt permutați folosind o permutare generată aleator cu ajutorul funcției logistice. Imaginea pre-criptată este obținută în urma reconstrucției folosind pachetele wavelet permutate.

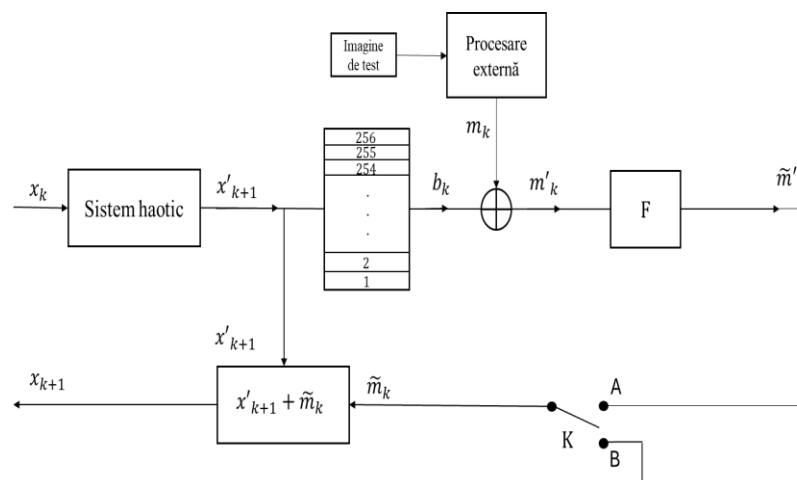


Figura 4.1 Schema generică de criptare

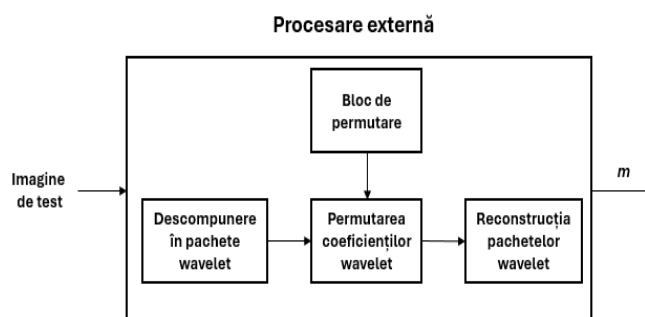


Figura 4.2 Procesare externă folosind transformata wavelet

Cea de-a doua metodă de pre-procesare folosind transformările de mixare este ilustrată în Figura 4.3. Imaginea de test este pre-criptată folosind funcția de mixare propusă de Shannon [17]. Descrierea funcțională a transformărilor de mixare este redată în Secțiunea 2.1.3.

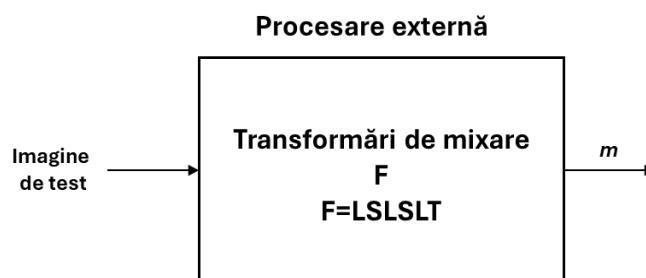


Figura 4.3 Procesare externă folosind transformări de mixare

4.3 Studiu comparativ asupra metodelor de criptare

4.3.1 Mod de lucru

Se evaluează rezultatele criptării folosind diferite configurații ale schemei generice. Ca imagini de test s-au folosit două imagini diferite de dimensiune 256x256 pixeli, cu entropie mică și cu entropie mare. Pentru funcția logistică utilizată la permutarea coeficienților wavelet am considerat parametrul de control $R = 4$.

4.3.2 Evaluarea schemei de criptare folosind funcția Hénon

Histogramele imaginilor criptate folosind sistemul Hénon și cele două metode de transformări externe sunt redată în Figura 4.4 și 4.5. Se poate observa că histogramele corespunzătoare configurației cu transformata wavelet nu sunt uniforme, în schimb când s-au folosit transformările de mixare, distribuția pixelilor este uniformă, indicând o performanță de criptare mai bună pentru această configurație.

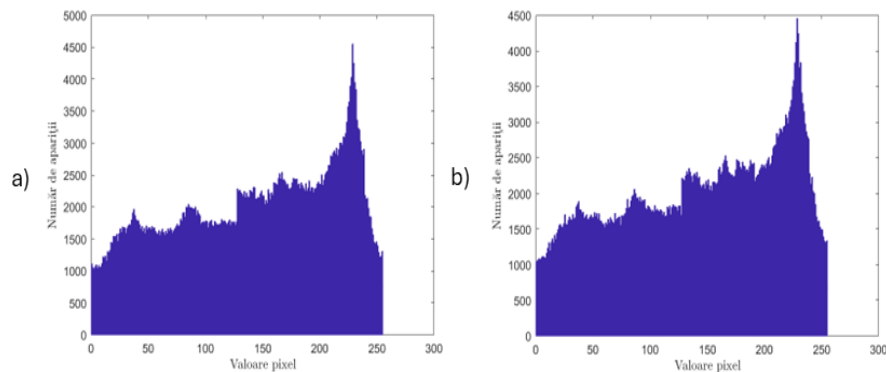


Figura 4.4 Histogramele corespunzătoare schemei cu transformata wavelet și funcția Hénon: a) imagine entropie mică; b) imagine entropie mare

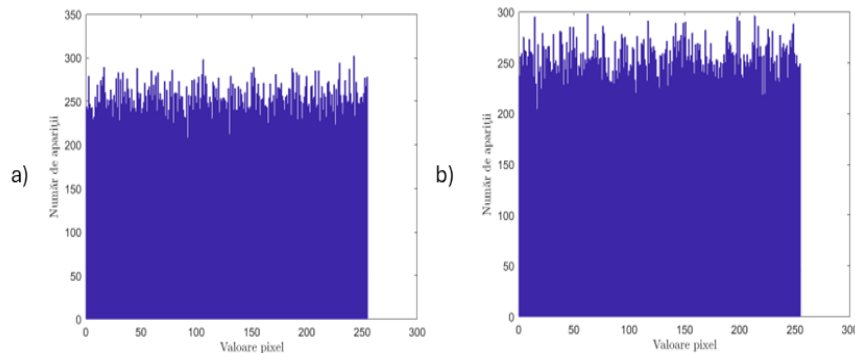


Figura 4.5 Histogramele corespunzătoare schemei cu transformări de mixare și funcția Hénon: a) imagine entropie mică; b) imagine entropie mare

4.3.3 Evaluarea schemei de criptare folosind funcția cort

Se evaluează performanța pentru configurația schemei cu funcția cort. În Figura 4.6 și 4.7 sunt redată histogrammele pentru schema de criptare în configurația cu transformata wavelet, respectiv pentru configurația cu transformările de mixare. Se poate afirma că în ambele configurații, distribuția pixelilor imaginilor criptate este uniformă.

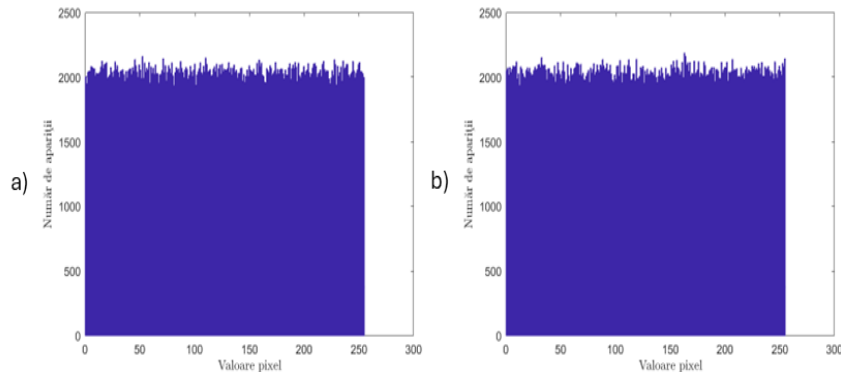


Figura 4.6 Histogrammele corespunzătoare schemei cu transformata wavelet și funcția cort: a) imagine entropie mică; b) imagine entropie mare

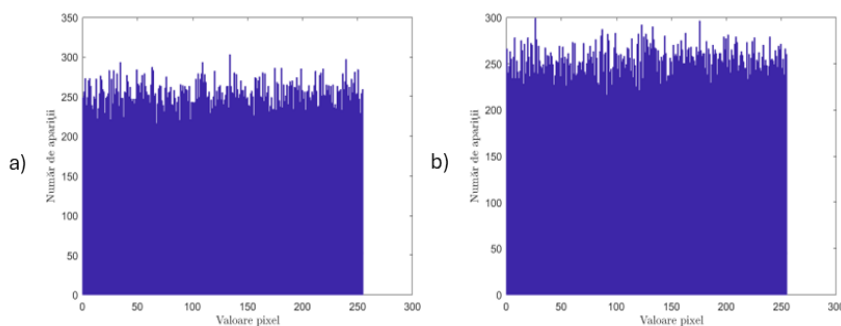


Figura 4.7 Histogrammele corespunzătoare schemei cu transformări de mixare și funcția cort: a) imagine entropie mică; b) imagine entropie mare

4.4 Concluzii

Criptarea este efectuată în două etape, asigurând astfel rezistență la atacurile criptografice. Folosind configurația schemei cu transformări wavelet, s-au obținut rezultate bune ale criptării doar pentru funcția cort. Pentru configurația cu transformări de mixare, s-au obținut rezultate bune pentru ambele sisteme dinamice considerate pentru incluziune. Așadar, performanța schemei de criptare în această configurație nu depinde de conținutul imaginii și nici de alegerea sistemului haotic.

Capitolul 5

Evaluarea pRNG-urilor bazate pe sisteme haotice folosind teste NIST, exponenți Lyapunov și diagrame de bifurcație

Acest capitol prezintă modalități de evaluare a pRNG-urilor bazate pe sisteme haotice folosind diverse instrumente precum: teste NIST, exponenți Lyapunov și diagrame de bifurcație. Rezultatele au fost prezentate la conferința „Romanian Cryptology Days Conference RCD-2019: Cryptography and Beyond, in a Connected World” și publicate ulterior într-un articol de revistă „Proceedings of the Romanian Academy”, Series A [20].

5.1 Introducere

Cercetarea a pornit de la studiul din [14], unde autorii au evaluat aleatorismul unui pRNG bazat pe haos și au observat o corelație între rezultatele testelor NIST și metricile specifice teoriei haosului: exponenții Lyapunov și diagrama de bifurcație. Astfel, folosirea metricilor specifice haosului ar putea reprezenta o metodă facilă de evaluare a pRNG-urilor bazate pe haos și de identificare a unor spații de lucru (seed-uri) valide. Evaluarea posibilității utilizării practice a acestei metode reprezintă scopul capitolului curent. Pentru aceasta este aprofundat studiul din [14] și extins pentru alte pRNG-uri bazate pe haos din literatură.

5.2 Aprofundarea pRNG-ului bazat pe sistemul Hénon generalizat

În acest capitol, extindem intervalul de investigare din [14]. Parametrul de control b al sistemului Hénon 3D este fix $b = 0.1$, condițiile inițiale sunt $x_0 = y_0 = z_0 = 0$ și parametrul de control a variază în întreg domeniul de definiție $(0, 2)$, cu pasul 10^{-3} .

Rezultatele au arătat că pentru subintervalul $[0.786, 1.081]$, cel mai mare exponent Lyapunov (λ_1) este aproximativ 0 ceea ce implică un comportament stabil al sistemului dinamic. Pentru subintervalul $[1.4, 1.76]$, trei dintre valorile celui mai mare exponent Lyapunov (λ_1) sunt negative, prin urmare aceste valori ale parametrului a nu formează o pereche validă cu $b = 0.1$. Pe măsură ce micșorăm pasul de variație al parametrului a , la 10^{-4} , se observă un număr de 14 valori ale parametrului a care împreună cu $b = 0.1$, determină un comportament periodic al sistemului ($\lambda_1 < 0$). Când pasul de variație este scăzut mai mult, la 10^{-5} , numărul de perechi care nu generează haos este mai mare de o sută.

Suita de teste NIST este rulată pentru $b = 0.1$, $x_0 = y_0 = z_0 = 0$ și a variază în $[1.4, 1.76]$ cu pasul de 10^{-3} . Rezultatele sunt sumarizate în Tabelul 5.1. Numărul din paranteză indică numărul de teste picate pentru acea categorie particulară de teste.

Tabelul 5.1 Testele NIST picate pentru $b = 0.1$ și a variabil

| Teste NIST picate | $a \in [1.4, 1.76)$ |
|------------------------------------|---|
| Frequency | 1.404 |
| Block Frequency | 1.404, 1.427, 1.627, 1.655, 1.682 |
| CumulativeSums (2 teste) | 1.404 (2); 1.600, 1.655, 1.682 (1) |
| Runs, LongestRun, Rank, | 1.404, 1.655, 1.682 |
| OverlappingTemplate | 1.481, 1.655, 1.68, 1.726 |
| Universal | 1.404, 1.655, 1.682 |
| FFT | 1.404, 1.425, 1.505, 1.655, 1.682 |
| NonOverlappingTemplate (148 teste) | 1.408, 1.411, 1.413, 1.418, 1.421, 1.423, 1.435, 1.447, 1.448, 1.451, 1.458, 1.461, 1.462, 1.486, 1.487, 1.493, 1.498, 1.502, 1.506, 1.511, 1.512, 1.514, 1.520, 1.529, 1.539, 1.544, 1.558, 1.584, 1.585, 1.594, 1.596, 1.597, 1.607, 1.623, 1.628, 1.630, 1.638, 1.641, 1.650, 1.470, 1.465, 1.658, 1.668, 1.672, 1.673, 1.679, 1.687, 1.691, 1.702, 1.727, 1.728, 1.733, 1.748, 1.753, 1.759, 1.481, 1.726 (1); 1.428, 1.523, 1.560, 1.632, 1.655, 1.682, 1.708, 1.723, 1.731, 1.537 (3); 1.404 (118) |
| ApproximateEntropy | 1.404, 1.578, 1.655, 1.682 |
| Serial (2 teste) | 1.483, 1.701 (1); 1.404, 1.655, 1.682 (2) |
| LinearComplexity | 1.404, 1.655, 1.682 |
| Random Excursions | |

5.3 Extinderea studiului pentru alte pRNG-uri bazate pe haos din literatură

În această secțiune analiza este extinsă pentru alte trei pRNG-uri bazate pe haos din literatură [21], [22], [23] cu scopul de a verifica presupunerea făcută în [14]. Au fost selectați parametri de control care determină comportament haotic sau periodic și testele NIST au fost executate pentru aceste seed-uri. pRNG-urile utilizate sunt denumite în continuare GENERATORUL k , $k = \{1, 2, 3\}$.

Rezultatele experimentale sunt redate în Tabelul 5.2. Se poate observa că pentru GENERATOARELE 1 și 2 există un număr de teste picate chiar dacă comportamentul sistemului dinamic a fost haotic. În schimb pentru GENERATORUL 3 toate testele NIST au trecut atunci când parametrul de control determină un comportament haotic. Acest rezultat arată că buna funcționare a pRNG-urilor bazate pe haos nu este influențată doar de sistemul dinamic, dar și de arhitectura generatorului și de procesările efectuate.

Tabelul 5.2 Corespondență între rezultatele testelor NIST și parametrii de control ale pRNG-urilor pentru comportament haotic și periodic

| pRNG | Parametri | Comportament | Nr. teste NIST picate |
|-------------|----------------------|--------------|-----------------------|
| GENERATOR 1 | $R = 3.9999$ | haotic | 31 |
| | $R = 3.961$ | periodic | 157 |
| GENERATOR 2 | $R \in (3.6, 4)$ | haotic | 5 |
| | $R \in (3.3, 3.7)$ | periodic | 158 |
| GENERATOR 3 | $a = 1.656, b = 0.1$ | haotic | 0 |
| | $a = 1.404, b = 0.1$ | periodic | 121 |

Evaluăm performanțele GENERATOARELOR 1-3 în aplicații criptografice folosind o schemă de criptare de tip one-time pad (OTP) [24] ilustrată pe imagini. Pentru valorile parametrilor de control care determină comportament haotic s-a obținut o bună criptare a imaginilor, ceea ce indică un comportament pseudo-aleator al generatoarelor. Pe de altă parte, când utilizăm valori ale parametrilor de control care generează comportament periodic se observă că rezultatele criptării sunt slabe. Acest fapt arată lipsa comportamentului aleator al pRNG-urilor.

5.4 Concluzii

În concluzie, chiar dacă metricile specifice haosului sunt ușor de implementat și oferă o indicație inițială cu privire la calitatea parametrilor selectați, ele nu înlocuiesc analiza pRNG-ului prin testele NIST. Cu toate acestea, rezultatele obținute au arătat că această abordare este promițătoare și poate oferi un cadru de lucru facil pentru extinderea spațiului de valori ale seed-urilor.

Capitolul 6

Concluzii

6.1 Concluzii și contribuțiile personale

Primul capitol al tezei cuprinde motivația și încadrarea tezei în domeniul de cercetare al criptografiei bazate pe haos. Sunt prezentate principalele caracteristici ale teoriei haosului evidențiind aplicabilitatea în criptografie în construcția de pRNG-uri și criptarea de imagini. Este ilustrată structura tezei și conținutul capitolelor.

Următoarele capitole din teză, 2, 3 și 4 au abordat aplicațiile sistemelor haotice în criptarea de imagini prin incluziunea mesajului. Capitolul 2 a evaluat aportul sistemelor dinamice în scheme de criptare cu incluziunea mesajului. Această contribuție a fost evidențiată în două etape: inițial, mesajul este doar inclus în dinamica sistemului și ulterior, mesajul este procesat și cu funcții criptografice de mixare. Atunci când se analizează doar contribuția individuală a sistemului dinamic, studiul a arătat că se obține o transformare vizuală a imaginii și că există diferențe între sistemele haotice folosite.

În cazul prelucrării mesajului cu funcții de mixare aplicate extern s-au obținut rezultate bune ale criptării pentru toate cele trei sisteme considerate atunci când s-a folosit o funcție de mixare extinsă. În cazul aplicării funcției de mixare intern schema de criptare este mai eficientă, deoarece s-au observat rezultate bune ale criptării pentru toate sistemele alese utilizând o funcție de mixare cu o singură operație de mediere liniară. Astfel, s-a obținut un rezultat care poate fi interesant din perspectiva obținerii unor funcții de mixare eficiente folosind participarea directă a sistemului dinamic în arhitectura acestor funcții.

Studiul transformărilor de mixare cu sisteme haotice este completat prin evaluarea criptării imaginilor pentru diferite valori ale parametrilor de control pentru funcția logistică și funcția Hénon. Prin includerea în schema de procesare a unei noi

operații de mediere liniară, înainte de operația de substituție, s-a obținut o funcție de mixare extinsă $F = LSL$, care oferă performanțe bune pentru diferite valori ale parametrilor de control. Astfel securitatea schemei de criptare este sporită prin creșterea spațiului cheilor.

În capitolul 3, principalul obiectiv urmărit a fost de a determina dacă incluziunea unui mesaj extern în evoluția sistemului dinamic afectează proprietățile statistice ale acestuia. Cercetarea contribuie teoretic la caracterizarea complexă a comportamentului statistic al sistemului dinamic considerând situațiile cu incluziunea mesajului. Pentru menținerea valorilor de ieșire ale sistemului în intervalul de definiție, a fost propusă utilizarea unui întrerupător de decizie în schema de procesare și a fost determinat un interval de alegere pentru factorul de scalare. Pentru evaluarea impactului includerii mesajului asupra proprietăților statistice ale sistemului s-a realizat o analiză Monte Carlo a testului Kolmogorov-Smirnov care a arătat că proprietățile statistice ale sistemului dinamic rămân neschimbate după incluziune. S-a arătat că proprietățile statistice sunt păstrate și în cazul în care se realizează o procesare suplimentară prin introducerea unei funcții criptografice de mixare asupra mesajului inclus. Așadar, principala contribuție a acestui studiu este de a propune un cadru de lucru și analiză statistică pentru a asigura funcționarea corectă a sistemelor dinamice în scheme de criptare bazate pe incluziunea mesajului în vederea criptării imaginilor.

În Capitolul 4 au fost aplicate conceptele propuse în capitolele anterioare, 2 și 3, în vederea construcției unei scheme de criptare bazate pe haos eficiente și sigure aplicată pe imagini. S-a efectuat un studiu comparativ între două modalități de pre-procesare externă și două sisteme dinamice diferite în scopul alegerii unei configurații optime pentru criptarea imaginii. Metodele de pre-procesare externă aplicate au fost bazate pe transformata wavelet, respectiv transformările de mixare. Sistemele dinamice utilizate au fost funcția Hénon și funcția cort. Criptarea este efectuată în două etape, asigurând astfel rezistență la atacurile criptografice. Rezultatele au arătat că pentru schema cu transformări wavelet s-au obținut rezultate bune ale criptării doar pentru funcția cort. Însă, în cazul configurațiilor cu transformări de mixare, s-au obținut rezultate bune pentru ambele sisteme dinamice considerate. Astfel utilizarea funcțiilor de mixare permite o construcție a schemei cu performanțe bune pentru diverse tipuri de imagini și sisteme dinamice diferite.

În Capitolul 5 au fost prezentate modalități de evaluare a pRNG-urilor bazate pe sisteme haotice folosind diverse instrumente precum: teste NIST, exponenți Lyapunov și diagrame de bifurcație. A fost extins un studiu anterior al echipei de lucru pentru un pRNG bazat pe Hénon map. Evaluarea corespondenței dintre testele NIST, exponenții Lyapunov și diagramele de bifurcație a fost realizată și pentru alte pRNG-uri bazate pe haos din literatură. Studiul a arătat că metricile specifice haosului sunt instrumente utile pentru evaluarea aleatorismului pRNG-urilor bazate pe haos și sunt ușor de implementat, care nu pot înlocui însă analiza statistică a pRNG-ului. Totuși, această abordare poate oferi un cadru de lucru facil pentru extinderea spațiului de valori ale seed-urilor pentru un pRNG.

6.2 Listă de publicații

Articole de revistă:

- O. Datcu, A.E. Lupu (Blaj), T. Blaj, R. Hobincu, *NIST tests, Lyapunov exponents and bifurcation diagrams when evaluating chaos based PRNGs*, Special Issue of Proceedings of the Romanian Academy, Series A, The Publishing House Of The Romanian Academy, Vol 21, Issue 1, pp. 29-36, March 2020, **WOS: 000519765700004**
- C. Macovei, A.E. Lupu (Blaj), M. Răducanu, *Enhanced cryptographic algorithm based on chaotic map and wavelet packets*, U.P.B. Sci. Bull., Series C Vol. 82, Iss. 4, 2020, ISSN 2286-3540, **WOS: 000596151000010**
- A.E. Lupu (Blaj), A.Vlad, *A Closer Look at the Statistical Behavior of a Chaotic System with Message Inclusion for Cryptographic Applications*, *Electronics*. 2024; 13(12):2270. <https://doi.org/10.3390/electronics13122270>, **WOS:001255765900001**

Articole de conferință:

- A.E. Lupu (Blaj), T. Blaj, A. Vlad, *Cryptographic mixing transformations and message embedding in chaotic systems*, 2022 14th International Conference on Communications (COMM), Bucharest, Romania, 2022, pp. 1-5, doi: 10.1109/COMM54429.2022.9817169.
- A.E. Lupu (Blaj), *Revisiting Mixing Transformations and Chaotic Systems with a View to Cryptographic Applications*, 2024 International Symposium on Electronics and Telecommunications (ISETC), Timișoara, România, 2024, pp. 1-4, doi: 10.1109/ISETC63109.2024.10797432.

Bibliografie

- [1] L. Kocarev, *Chaos-based cryptography: a brief overview*, in IEEE Circuits and Systems Magazine, vol. 1, no. 3, pp. 6-21, 2001, doi: 10.1109/7384.963463
- [2] M.S. Baptista, *Cryptography with chaos*, Physics Letters A, Volume 240, Issues 1–2, 1998, Pages 50-54, ISSN 0375-9601, [https://doi.org/10.1016/S0375-9601\(98\)00086-3](https://doi.org/10.1016/S0375-9601(98)00086-3).
- [3] Lawnik, M., Moysis, L., & Volos, C. (2022). *Chaos-Based Cryptography: Text Encryption Using Image Algorithms*. Electronics, 11(19), 3156. <https://doi.org/10.3390/electronics11193156>
- [4] Hu, H., Liu, L., & Ding, N. (2013). *Pseudorandom sequence generator based on the Chen chaotic system*. in Computer Physics Communications, 184(3), 765-768.
- [5] Mohammed M. Al-Mhadawi, Ekhlās Abbas Albahrani, Sadeq H. Lafta, *Efficient and secure chaotic PRNG for color image encryption*, Microprocessors and Microsystems, Volume 101, 2023, 104911, ISSN 0141-9331, <https://doi.org/10.1016/j.micpro.2023.104911>.
- [6] O. Datcu, C. Macovei, R. Hobincu, *Chaos Based Cryptographic Pseudo-Random Number Generator Template with Dynamic State Change*. Applied Sciences. 2020; 10(2):451. <https://doi.org/10.3390/app10020451>
- [7] C. Zhu, S. Li, Q. Lu, *Pseudo-random Number Sequence Generator Based on Chaotic Logistic-Tent System*, 2019 IEEE 2nd International Conference on Automation, Electronics and Electrical Engineering (AUTEEE), Shenyang, China, 2019, pp. 547-551, doi: 10.1109/AUTEEE48671.2019.9033389
- [8] B. Zhang, L. Liu, *Chaos-Based Image Encryption: Review, Application, and Challenges*, Mathematics. 2023; 11(11):2585. <https://doi.org/10.3390/math11112585>
- [9] Safwan El Assad, Mousa Farajallah, *A new chaos-based image encryption system*, Signal Processing: Image Communication 41 (2016): 144-157. <https://doi.org/10.1016/j.image.2015.10.004>
- [10] Y. Pourasad, R. Ranjbarzadeh, A. Mardani, *A New Algorithm for Digital Image Encryption Based on Chaos Theory*, Entropy. 2021; 23(3):341. <https://doi.org/10.3390/e23030341>
- [11] Liu, Wenhao; Sun, Kehui; Zhu, Congxu. *A fast image encryption algorithm based on chaotic map*. Optics and Lasers in Engineering, 2016, 84: 26-36.
- [12] Steven H. Strogatz, *Nonlinear Dynamics and Chaos*, Publisher: Addison-Wesley 1994

- [13] Alan Wolf, Jack B. Swift, Harry L. Swinney, John A. Vastano, *Determining Lyapunov exponents from a time series*, Physica D: Nonlinear Phenomena, Volume 16, Issue 3, 1985, Pages 285-317, ISSN 0167-2789, [https://doi.org/10.1016/0167-2789\(85\)90011-9](https://doi.org/10.1016/0167-2789(85)90011-9).
- [14] O. Datcu, R. Hobincu, *NIST tests versus bifurcation diagrams and Lyapunov exponents when evaluating chaos-based pRNGs*, Proceedings of ITISE 2018, Granada, Spain, pp. 1640-1649
- [15] O. Datcu, J.P. Barbot, A. Vlad, *New enciphering algorithm based on chaotic Generalized Hénon map*, CHAOS THEORY, Modeling, Simulation and Applications, 2011, 143-150
- [16] Corina Macovei, Adina-Elena Lupu (Blaj), Mircea Răducanu, *Enhanced cryptographic algorithm based on chaotic map and wavelet packets*, U.P.B. Sci. Bull., Series C Vol. 82, Iss. 4, 2020, ISSN 2286-3540
- [17] C. E. Shannon, *Communication theory of secrecy systems*, Bell System Technical Journal, vol. 28, no. 4, pp. 656–715, 1949
- [18] Alvarez, G.; Amigo, J.M.; Arroyo, D.; Li, S. *Lessons learnt from the cryptanalysis of chaos-based ciphers. In Chaos-Based Cryptography: Theory, Algorithms and Applications*; Kocarev, L., Lian, S., Eds.; Springer: Berlin/Heidelberg, Germany, 2011; Volume 354, pp. 257–295.
- [19] Zhu, F.; Wang, F.; Ye, L. *Artificial switched chaotic system used as transmitter in chaos-based secure communication*. J. Frankl. Inst. 2020, 357, 10997–11020
- [20] O. Datcu, A.E. Lupu (Blaj), T. Blaj, R. Hobincu, *NIST tests, Lyapunov exponents and bifurcation diagrams when evaluating chaos based PRNGS*, Special Issue of Proceedings of the Romanian Academy, Series A, The Publishing House Of The Romanian Academy, Vol 21, Issue 1, pp. 29-36, March 2020.
- [21] Patidar, Vinod & Sud, K.K. & Pareek, Narendra. (2009). *A Pseudo Random Bit Generator Based on Chaotic Logistic Map and its Statistical Testing*. Informatica. 33. 441-452.
- [22] Hamdi, M., Rhouma, R., & Belghith, S. (2015). *A Very Efficient Pseudo-Random Number Generator Based On Chaotic Maps and S-Box Tables*. World Academy of Science, Engineering and Technology, International Journal of Computer, Electrical, Automation, Control and Information Engineering, 9, 481-485.
- [23] D. Sava, A. Vlad, R. Tataru, *A new type of keystream generator based on chaotic maps: Illustration on a Hénon generalized map*, 2014 10th International Conference on Communications (COMM), Bucharest, Romania, 2014, pp. 1-6, doi: 10.1109/ICComm.2014.6866726.
- [24] Lugrin, T. (2023). *One-Time Pad*. In: Mulder, V., Mermoud, A., Lenders, V., Tellenbach, B. (eds) Trends in Data Protection and Encryption Technologies . Springer, Cham. https://doi.org/10.1007/978-3-031-33386-6_1

- [25] A. E. Lupu (Blaj), T. Blaj, A. Vlad, *Cryptographic mixing transformations and message embedding in chaotic systems*, 2022 14th International Conference on Communications (COMM), Bucharest, Romania, 2022, pp. 1-5, doi: 10.1109/COMM54429.2022.9817169.
- [26] A. E. Lupu (Blaj), *Revisiting Mixing Transformations and Chaotic Systems with a View to Cryptographic Applications*, 2024 International Symposium on Electronics and Telecommunications (ISETC), Timisoara, Romania, 2024, pp. 1-4, doi: 10.1109/ISETC63109.2024.10797432.
- [27] L. Kocarev, *Chaos-based cryptography: a brief overview*, in IEEE Circuits and Systems Magazine, vol. 1, no. 3, pp. 6-21, 2001, doi: 10.1109/7384.963463
- [28] Adriana Vlad, Mihai Mitrea, *Cryptographic mixing transformations for image applications*, Proc. SPIE 3405, ROMOPTO '97: Fifth Conference on optics, (2 July 1998)
- [29] A.E. Lupu (Blaj), A.Vlad, *A Closer Look at the Statistical Behavior of a Chaotic System with Message Inclusion for Cryptographic Applications*, Electronics. 2024; 13(12):2270. <https://doi.org/10.3390/electronics13122270>
- [30] Walpole, R.E.; Myers, R.H.; Myers, S.L.; Ye, K. *Probability & Statistics for Engineers & Scientists, Global Edition, 9th ed.*; Pearson Education Limited: Essex, UK, 2016; pp. 316–319.
- [31] D. A. Miller, G. Grassi, *A discrete generalized hyperchaotic Henon map circuit*, Proceedings of the 44th IEEE 2001 Midwest Symposium on Circuits and Systems. MWSCAS 2001 (Cat. No.01CH37257), 2001, pp. 328-331 vol.1, doi: 10.1109/MWSCAS.2001.986179.
- [32] A. Luca, A. Ilyas, A. Vlad, *Generating random binary sequences using tent map*, ISSCS 2011 - International Symposium on Signals, Circuits and Systems, 2011, pp. 1-4, doi: 10.1109/ISSCS.2011.5978664