UNIVERSITATEA "POLITEHNICA" DIN BUCUREȘTI

ȘCOALA DOCTORALĂ ETTI-B

Dezvoltarea de metode și tehnici criptografice folosind teoria haosului și statistica

Cryptographic methods and techniques using chaos theory and statistics

autor **ing. Corina MACOVEI**

REZUMAT

COMISIA TEZEI DE DOCTORAT

Președinte	**Prof. Dr. Ing. Gheorghe BREZEANU**	de la	**Universitatea "Politehnica" București**
Conducător	**Prof. Dr. Ing. Adriana VLAD**	de la	**Universitatea "Politehnica" București**
Referent	**Prof. Dr. Ing. Alexandru ȘERBĂNESCU**	de la	**Academia Tehnică Militară Bucureşti**
Referent	**Prof. Dr. Ing. Mihai CIUC**	de la	**Universitatea "Politehnica" București**
Referent	**Prof. Dr. Ing. Victor-Adrian GRIGORAȘ**	de la	**Universitatea Tehnică "Gheorghe Asachi" Iași**

București 2020

Cuprins

Capitolul 1

Contextul tezei

Lucrarea *Dezvoltarea de metode și tehnici criptografice folosind teoria haosului și statistica* tratează un subiect actual - comunicația privată - cu ajutorul teoriei haosului și statisticii.

Haosul determinist este un fenomen care la prima vedere pare aleator, însă acest comportament se poate determina exact dacă știm cu precizie infinită starea inițială a sistemului care îl generează. Pentru că precizia cunoscută a stării inițiale a sistemului generator nu poate fi infinită, putem spune că o predicție corectă a sistemelor haotice se poate face în anumite limite. Pe de altă parte, toate sistemele haotice sunt guvernate de legi de mișcare, de unde putem concluziona că există ordine în aparentul haos. Termenul de haos provine din dificultățile noastre de a detecta regularități în acest tip de dinamică. În ciuda determinismului său, acest sistem produce alegeri care ne surprind mintea. Iată, deci, de unde, denumirea de haos determinist.

Un exemplu practic de haos determinist este efectul fluturelui, descoperit de Edward Norton Lorenz, meteorolog, [1]. Acest fenomen, conform căruia bătăile de aripi ale unui fluture aici, poate să producă un uragan într-o alta parte a lumii, demonstrează o dependență mare a fenomenului față de condițiile inițiale. Meteorologul se ocupa și de predicția vremii. În cadrul unui experiment a întrerupt simularea efectuată pe computer, și a reluat-o dupa o pauză, cu 3 zecimale, în loc de 6 zecimale folosite anterior de mașina pe care lucra. Pentru a asigura continuitatea rezultatelor obţinute, Lorenz a reluat calculul ultimelor cateva zeci de puncte. A observat cu sur-

prindere că acestea nu mai coincideau cu cele calculate în simularea anterioară. Iată cum, o cunoaștere trunchiată a stării inițiale a sistemului generator poate conduce la divergența traiectoriilor inițial vecine.

Unul din cele mai cunoscute și mai simple sisteme haotice este funcția logistică, pe baza căreia se poate modela evoluția populației, așa cum arată biologul Robert May. Funcția logistică va servi pentru exemplificarea unor metodele şi tehnici dezvoltate de lucrarea noastră. Un alt exemplu interesant și foarte actual este chiar răspândirea virusului COVID-19 în toată lumea, acesta putând fi comparat cu efectul fluturelui, rapiditatea răspândirii lui găsind lumea nepregatită. Un studiu viitor deosebit de util pentru toată lumea ar fi să investigăm care este sistemul haotic pe care s-ar putea mapa răspândirea bolilor și pandemiilor globale. Lucrările lui Steven Strogatz şi a colaboratorilor săi sunt un bun punct de început al acestei cercetări viitoare.

Necesitatea criptării mesajelor s-a amplificat odată cu tendința digitalizării tuturor activităților din societate. Criptografia este o știință veche, primele consemnări datând din era împăratului Iulius Cezar. Totuși cercetarea și dezvoltarea de algoritmi criptografici a început relativ târziu, în 1970. Apoi acest domeniu s-a dezvoltat rapid. Principiul de bază al criptării este acela de a modifica mesajul inițial astfel încât acesta să poată fi descifrat doar de către destinatar. Acest lucru trebuie să conducă la un timp de decriptare foarte scurt pentru destinatar și un timp foarte lung pentru oricare altă entitate care ar atenta să descifreze mesajul. Primele forme de criptare au fost permutările și substituțiile. Performanțele computerelor și scăderea costurilor lor au facilitat dezvoltarea de algoritmi.

Haosul determinist este folosit ca generator de dezordine în algoritmii criptografici. Practic, ascundem mesajul într-un flux haotic de date. La recepție, pentru a extrage mesajul, este nevoie să cunoaștem valoarea parametrilor și a condițiilor inițiale ale sistemului haotic. Astfel, haosul determinist oferă un context favorabil pentru folosirea lui în aplicațiile criptografice.

Capitolul 2

Relevanţa funcţiei de autocorelaţie pentru distanţa de independenţă statistică

O proprietate a criptosistemelor performante este ca în urma analizei datelor produse de către criptosistemul respectiv să nu fie dezvăluită o relație existentă între eșantioanele analizate. Acestea trebuie să fie decorelate, varianta mai lejeră a independenței statistice, utilă în practică, unde nu se dispune, de multe ori, de suficientă informaţie. În acest sens, în Capitolul 2, am elaborat un test de medie asupra funcției de autocorelație, particularizat pe două dintre cele mai simple sisteme haotice folosite în criptografie: funcția cort și funcția logistică. Aceste rezultate au fost diseminate în două lucrări indexate în ISI Web of Science, în 2019 [2], respectiv 2020 [3].

Primul sistem investigat în această lucrare este funcţia cort, descrisă de (2.1), unde p este parametrul de control, iar x_0 condiţia iniţială. Momentul de timp discret este notat, aici, cu k.

$$x_{k+1} = \begin{cases} \frac{x_k}{p}, 0 \leq x_k \leq p \\ \frac{1-x_k}{1-p}, p \leq x_k \leq 1 \end{cases} \tag{2.1}$$

Fig. 2.1 prezintă două traiectorii ale funcţiei cort, pentru două condiţii iniţiale alese aleator în $(0, 1)$. Păstrând valoarea parametrului p constantă şi alegând $N = 10000$ de condiţii iniţiale x_{0j} dintr-o distribuţie uniform aleatoare în $(0, 1)$, am construit un proces aleator, j variază de la 1 la N. Cele două curbe din Fig 2.1 sunt două

dintre realizările particulare ale procesului aleator, date doar spre exemplificare.

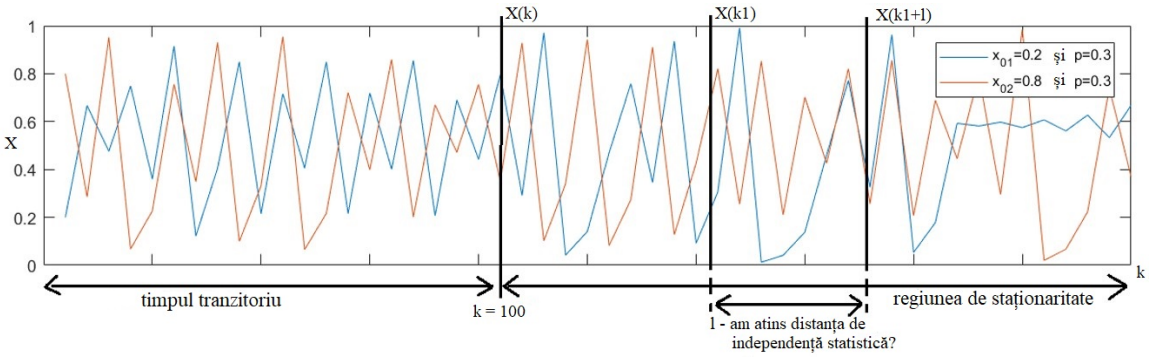

Fig. 2.1: Evoluția temporală a sistemului (2.1) pentru același parametru $p = 0.3$ și două condiții inițiale, $x_{01} = 0.2$ și $x_{02} = 0.8$.

Revenind la procesul aleator constituit din cele N curbe pentru N condiţii iniţiale diferite, pentru a-i investiga proprietăţile statistice avem nevoie să ne aflăm în regiunea de staţionaritate, iar procesul aleator să fie ergodic. Dacă se alege corect parametrul de control, şi sistemul este în regiunea de staţionaritate, procesul aleator generat de ele este ergodic.

Dat fiind că alegem condiţiile iniţiale dintr-o distribuţie uniformă în (0,1), eşantionând cele N curbe la iteraţia 1, vom avea o funcţie de densitate de probabilitate corespunzătoare acestui tip de distribuţie. Pe durata timpului tranzitoriu procesului aleator îi va varia funcţia de densitate de probabilitate de la o uniformă, către cea proprie procesului investigat. La momente succesive $k_1, k_1 + 1, \ldots$ această densitate de probabilitate va rămâne constantă, după ce la k_1 intră în regiunea de staţionaritate. Funcţia cort este un caz particular de semnal haotic, pentru care funcţia de densitate de probabilitate este uniformă, însă nu acesta va fi cazul celei de-a doua funcţii haotice folosite ca exemplu în acest capitol, funcţia logistică.

Ergodicitatea este o altă proprietate statistică relevantă pentru studiul nostru. Aceasta ne asigură că informaţia obţinută în urma analizei unei traiectorii temporale lungi, de zeci, sute de mii de iteraţii, va fi regăsită şi in studiul oricărei variabile obținută prin eşantionarea procesului aleator, odată aflaţi în regiunea de staţionaritate.

Odată în staţionaritate, ne putem pune problema independenţei statistice. Căutăm, deci, acea distanţă dintre momentele de timp k_1 şi k_{1+d} care să ne permită obţinerea a două variabile aleatoare independente statistic. Testele de corelaţie existente în literatură anterior lui 2006, precum cele ce folosesc coeficientul de corelație Spearman [4] sau gradul de corelație Pearson [5], rezolvau problema doar pentru variabile aleatoare Gaussiene, în acest caz decorelarea datelor implicând independenţa lor statistică. Dar procesele aleatoare generate de sistemele haotice nu respectă o distribuţie Gaussiană. Deci, decorelarea atestată de testele [4, 5] nu ar conduce la decizia implicită de independenţă statistică între cele două variabile aleatoare investigate.

Lucrarea [6] a rezolvat această situaţie prin aplicarea unor transformări de variabilă aleatoare asupra distribuţiilor empirice rezultate din variabilele aleatoare obţinute prin eşantionarea procesului aleator studiat la iteraţiile comparate, k_1 şi k_{1+d}. Testul din [6] (Badea-Vlad) este un test de independenţă statistică aplicabil pe orice lege de probabilitate, nu doar pe cele Gaussiene şi a fost folosit pentru a evalua sisteme în timp discret, precum funcţia cort sau sistemul tridimensional Rössler. Lucrarea [7] evaluează performanţa acestui test şi îl completează pentru situaţiile de interes, în 2016, automatizând decizia testului propus de [6], care era evaluată inițial vizual pentru a decide dacă, în urma transformărilor, cele două variabile aleatoare investigate sunt jointly-Gaussian, permiţând ca decizia de decorelare a datelor să fie echivalentă cu cea de independenţă statistică. Articolul [8] studiază independenţa statistică în contextul funcției cort (2.1). În [9, 10] discuţia se mută la funcţia logistică. Cercetarea din [10] ne răspunde la întrebarea "în ce măsură o mică variaţie a parametrului funcției logistice afectează studiul corespunzător procesului aleator generat?", răspuns esenţial pentru studiul nostru.

Răspunsul este, aşa cum intuiam, că procesul aleator este determinat de valoarea parametrului sistemului haotic, pentru funcţia logistică notat cu R din relaţia (2.2).

$$x_{k+1} = R \cdot x_k(1 - x_k) \tag{2.2}$$

Fig. 2.2 ne oferă o idee despre cât de diferite sunt traiectoriile funcţiei logistice în

dependență cu parametrul său. Întrebarea pe care ne-o punem este: cât de mult afectează studiul nostru o ușoară deviație a parametrului de control?

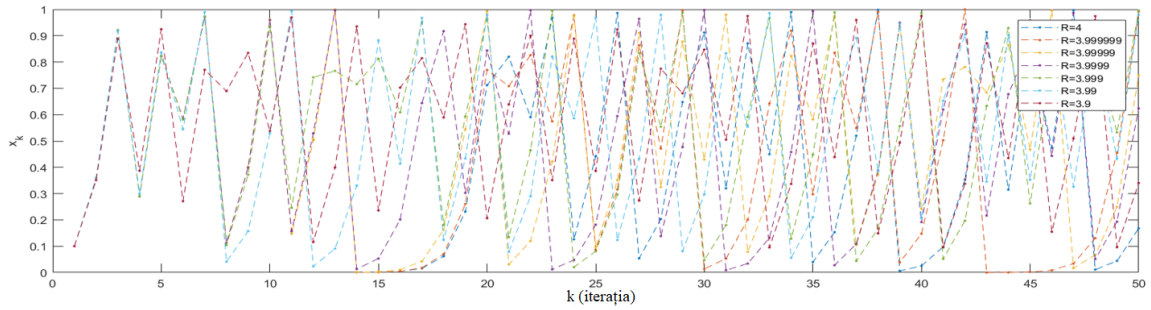

Fig. 2.2: Mai multe traiectorii ale funcției logistice pentru diferite valori ale lui $R = 4(1 - \epsilon)$ și aceeași condiție inițială $x_0 = 0.1$.

Funcția de autocorelație ne arată cât de corelat este un semnal cu o replică a sa aflată la un moment de timp ulterior. În studiul nostru este investigată autocorelația statistică. Variabilele aleatoare a caror autocorelaţie este studiată sunt obținute prin eșantionarea celor 10k de traiectorii anterior menționate, reprezentând procesul aleator dat de parametrul de control ales.

Scopul studiului este să determinăm de la ce distanță de eșantionare datele devin necorelate. În acest sens introducem funcția de autocorelație definită pentru procesul aleator X corespunzător funcției haotice, în relația (2.3) și funcția de autocorelație experimentală (2.4), unde $x_i(k_1)$ și $x_i(k_1 + l)$ sunt valorile iterațiilor k_1, respectiv $k_1 + l$ ale traiectoriei i, cu i variind de la 1 la N, N fiind numărul de traiectorii folosite pentru a simula procesul aleator. Este important să menționăm, k_1 trebuie ales după intervalul de timp corespunzător timpului tranzitoriu, deci, în regiunea de staţionaritate.

$$R_X(l) = E[X(k_1)X(k_2)] = E[X(k_1)X(k_1 + l)] \tag{2.3}$$

$$R_{exp,X}(l) = \frac{1}{N}\sum_{i=1}^{N} x_i(k_1)x_i(k_1 + l) \tag{2.4}$$

În acest capitol am făcut și o analogie între 2 sisteme cort cu domenii de definiție diferite, pe care le-am echivalat printr-o transformare de variabilă aleatoare, $Y =$

$2X$–1. Această echivalență duce la un calcul simplu al funcției de autocorelație, rezultatele obținute pe un sistem putând fi translatate și pentru celălalt sistem.

În stânga Fig. 2.3 sunt câte 3 funcții de autocorelație corespunzătoare funcției cort, calculate pentru mai mulți parametri de control. În acest caz, se observă că funcția de autocorelație tinde spre valoarea 0.25. În cazul funcţiei logistice, în dreapta Fig. 2.3 am reprezentat grafic funcții de autocorelație pentru diverse valori ale parametrului R, $R = 4$ și o vecinătate, 2 valori foarte apropiate de 4 ($R = 3.999999$ și $R = 3.9999$), (dreapta sus), precum și două valori mai depărtate ($R = 3.99$ și $R = 3.78$) (dreapta jos). La o primă vedere observăm că pentru $R = 4$ și l suficient de mare funcția de autocorelație tinde spre valoarea 0.25. Similar, pentru valori foarte apropiate de 4, este dificil de observat vizual o diferență. Pentru R mult diferit de valoarea de referință $R = 4$, funcția de autocorelație nu mai are o valoare medie de 0.25, ci este complet alta, aproximativ 0.28 pentru $R = 3.99$ și 0.41 pentru $R = 3.78$.

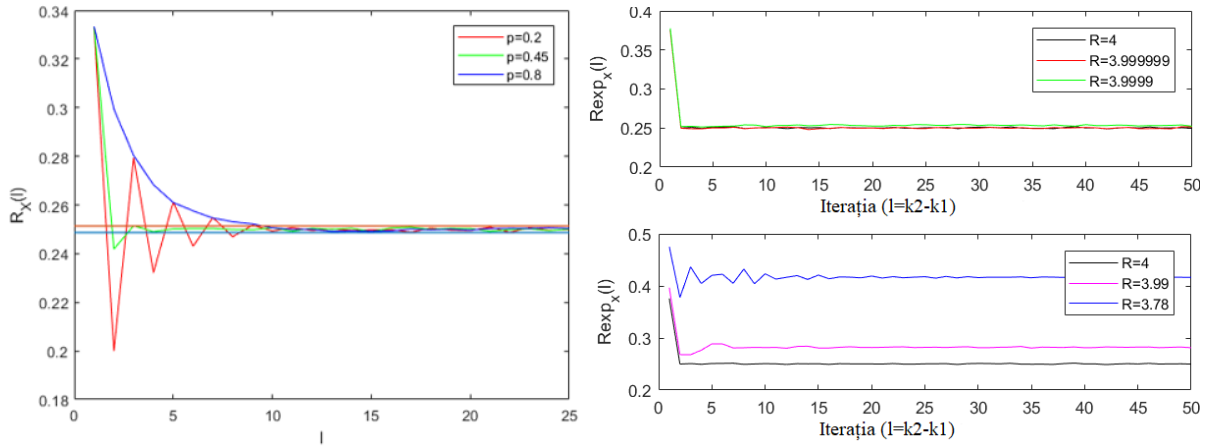

Fig. 2.3: Funcția de autocorelație experimentală asociată funcției cort (stânga) și funcției logistice (dreapta).

Valoarea funcţiei de autocorelaţie pentru parametrul $R = 4$ a fost determinată uşor, pentru această situaţie particulară distribuţia statistică a funcţiei logistice fiind cunoscută, media şi dispersia valorilor sale ne sunt la dispoziţie.

Relaţia (2.5) arată, deci, media variabilei aleatoare ξ, aflată în intervalul precizat, cu ε intervalul de incredere, corespunzător $\alpha/2$ quartilei caracteristice legii Gaussiene. $N = 10000$ reprezintă numărul de curbe considerate pentru studiu, iar σ corespunde

dispersiei valorilor v. a. ξ.

$$R_{exp,X}(l) \in [\mu_\xi - \varepsilon; \mu_\xi + \varepsilon]; \varepsilon = Z_{\alpha/2}\frac{\sigma_\xi}{\sqrt{N}} \tag{2.5}$$

Astfel, putem aplica testul statistic care ne va spune dacă ne aflăm în situația de decorelare a datelor investigate, cele doua variabile aleatoare la momentele k_1 şi k_1+d.

Testul are două ipoteze:

- H_0 - a fost atinsă valoarea aşteptată a funcţiei de autocorelaţie (distanța l poate corespunde independenței statistice între $X(k_1)$ și $X(k_2)$);
- H_1 - ne aflăm sub valoarea căutată a autocorelaţiei care ar putea asigura independenţa statistică ($X(k_1)$ și $X(k_2)$ nu sunt independente statistic).

Pentru a evidenția rezultatele obținute, am aplicat o analiză Monte Carlo pe un grup de funcții de autocorelație, analiză ce a pus în valoare și aspecte practice computaționale, precum precizia în calcul și degradarea traiectoriilor. Mai multe funcții de autocorelație au fost calculate pe grupuri de $N = 10^4$ sau $N = 10^5$ traiectorii ale funcțiilor cort și logistice. Au fost calculate 500 astfel de funcții de autocorelație și a fost analizat procentul de acceptare al testului de medie. Întrebarea noastră a fost: câte funcții de autocorelație se află în intervalul de acceptare al testului pentru un anumit l?

Pentru funcția cort rezultatele au arătat că pentru $l > 10 - 15$ iterații în aproape 95% din cazuri testul este trecut pentru orice parametru de control, iar în cazul funcției logistice s-a observat că pentru parametrul de control $R = 4$ (singurul parametru pentru care știm media și dispersia teoretică și putem calcula testul de medie), în aproape 95% din cazuri testul este trecut pentru $l > 5$, ca în Fig. 2.4 .

A fost studiată mai departe senzitivitatea la parametrul de control și modul în care aceasta se reflectă în testul de medie pentru valori ale parametrului R într-o vecinătate a lui 4 pentru funcția logistică. Am considerat același interval de acceptare, ca și pentru $R = 4$. În fiecare imagine din Fig. 2.5 sunt plotate 500 funcții de autocorelație pentru diverse valori ale parametrului de control. În figura stânga-sus, pentru R foarte apropiat de 4, un procent de 95% ale valorilor se află în intervalul

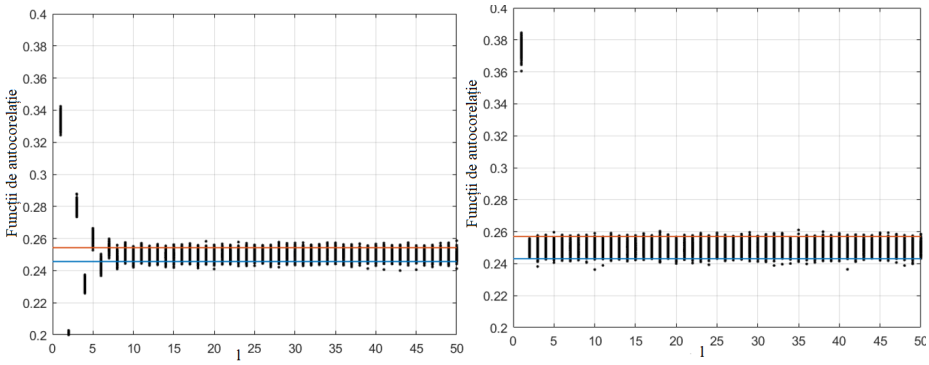

Fig. 2.4: Analiza Monte Carlo a testului de medie pe funcția de autocorelație $N = 10000$; $L = 500$, până la $l = k_2 – k_1 = 50$. Stânga: funcţia cort, $p = 0.2$. Dreapta: funcţia logistică, $R = 4$.

stabilit. În figura stânga-jos putem vedea că doar 68% din valori se află în intervalul dorit corespunzător lui $R = 4$. Dacă ne depărtăm de $R = 4$, funcția de autocorelație are o nouă valoare medie, cum putem vedea în figurile din dreapta. Astfel rezultatele din studiile anterioare sunt reconfirmate, deoarece pentru R foarte aproape de 4 legea de probabilitate pare că este aceeași ca pentru $R = 4$, iar când ne depărtăm avem o medie și o dispersie complet diferite față de cele pentru $R = 4$.

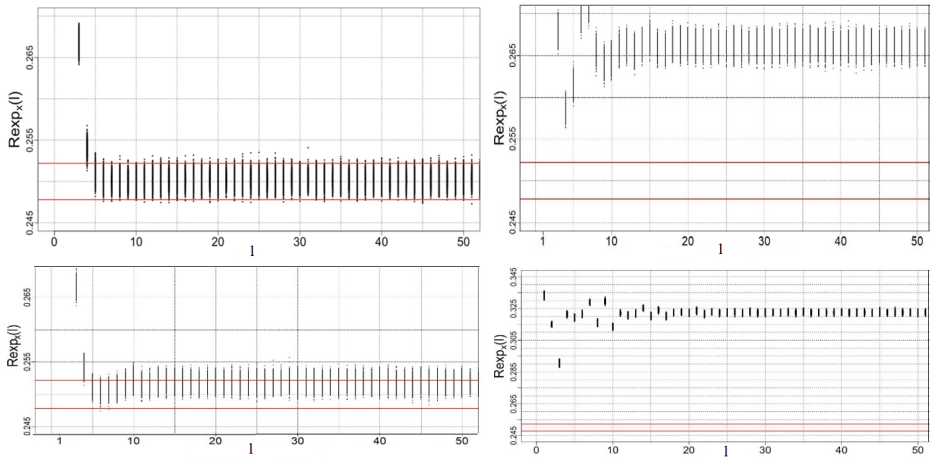

Fig. 2.5: $N = 10^5$ traiectorii diferite pentru funcția logistică, 500 funcții de autocorelație. Stânga: $R = 3.999999$ (sus), $R = 3.9999$ (jos) și dreapta: $R = 3.99$ (sus), $R = 3.78$ (jos).

În studiul nostru am observat că testul de medie este trecut pentru valori ale lui l mai mici decât cele obținute prin testul de independență statistică [6, 7]; acest lucru

p	Distanţa de independenţă statistică [6]	Distanţa de decorelare observată cu testul propus
0.25	25	8
0.45	15	4
0.55	15	3
0.75	35	7

Tabel 2.1: Relația dintre $R_X(l)$ și distanța de independență statistică pentru funcţia cort.

poate arăta că variabilele $X(k_1)$ și $X(k_2)$ sunt necorelate. Pentru funcția cort, în Tabelul 2.1 ultima coloană reprezintă distanța de decorelare observată în studiul de medie asupra funcției de autocorelație. Cea de-a doua coloană reprezintă distanța de independență statistică evaluată în articolele anterioare [6, 7]. Aceste valori depind de parametrul de control al sistemului haotic. Studiul a continuat cu o reevaluare a distanței minime de independență statistică pentru funcția cort și funcția logistică, rezultatele din literatură fiind reconfirmate.

Testul de medie este un instrument numeric important care masoară relația dintre evaluările de independență statistică și autocorelație. Dacă testul este trecut nu înseamnă neapărat că variabilele $X(k1)$ și $X(k2)$ sunt independente, ci necorelate. Indepedența statistică trebuie evaluată prin metode specifice. Deci testul de medie nu înlocuiește testul de independență statistică, dar este un suport al independenței statistice obținute. Pe de altă parte, dacă testul nu este trecut, clar nu avem indepedență statistică pentru distanța l la care a fost calculată funcția de autocorelație. Pentru funcţia cort putem aplica testul de medie pentru orice parametru de control, deoarece legea de probabilitate este uniformă pentru toate valorile parametrului de control. Pentru funcţia logistică, însă, studiul este mai complex: cunoaștem legea doar pentru parametrul de control $R = 4$; pentru această valoare putem calcula media și dispersia variabilei aleatoare x_i și putem aplica testul de medie în cazul variației cunoscute. Pentru valori $R \neq 4$, media teoretică și dispersia trebuie calculate prin proceduri specifice ce fac obiectul studiului viitor.

Capitolul 3

Generarea unui spațiu continuu de selecție a cheilor unui pRNG bazat pe haos

Capitolul 3 reia un studiu bazat pe sistemul tridimensional generalizat al lui Hénon, sistem discret în timp, rezultatele fiind diseminate într-o lucrare de revistă cotată $Q2$ [12] și într-o lucrare de conferință ISI Web of Science [11]. Un generator de numere pseudo-aleatoare reprezintă o tehnică de generare a unor secvențe ale căror elemente sunt independente. Generatorul de numere aleatoare de la care a plecat ideea acestui capitol a fost propus în lucrarea [13] şi implementat într-un FPGA (Field Programmable Gate Array) în articolul [14] de către aceiaşi autori. Un SAU EXCLUSIV între cei mai puţin semnificativi 8 biţi din reprezentările binare pe 64 de biţi ale celor trei stări ale sistemului conduce la obţinerea câte unor serii de octeţi aparent aleatori care, pentru parametrii a şi b adecvat aleşi, trec testele NIST (National Institute of Standards and Technology). Aceşti octeţi pot fi folosiţi, printre alte domenii de aplicabilitate a pRNG-urilor, pentru criptarea de text şi de imagine, acestea fiind reprezentate de asemenea pe 8 biţi, conform ASCII.

Sistemul menţionat are un comportament haotic sau hiperhaotic, aşa cum ne arată cercetarea din [15], doar pentru anumite valori ale parametrilor de bifurcație a și b.

Diagramele de bifurcaţie din Fig. 3.1 ne arată numărul de soluţii ale sistemului (3.1) cu parametrii $a \in (0, 2)$, $b \in [-0.3, 0.3], x, y, z \in (-2, 2)$, atunci când parametrul a este fixat, iar b baleiază intervalul $(-1, 1)$. Observăm că în cazul $a = 0.15$, în Fig. 3.1 (imaginea din stânga), pentru b în $(-0.7, 0.87)$ sistemul tridimensional al lui Hénon

converge la o singură valoare, fiind departe de comportamentul haotic caracterizat print-un număr foarte mare de soluţii, aşa cum o arată regiunea b în $(0.87, 1)$.

$$\begin{aligned} x_{k+1} &= a - y_k^2 - bz_k \\ y_{k+1} &= x_k \\ z_{k+1} &= y_k \end{aligned} \tag{3.1}$$

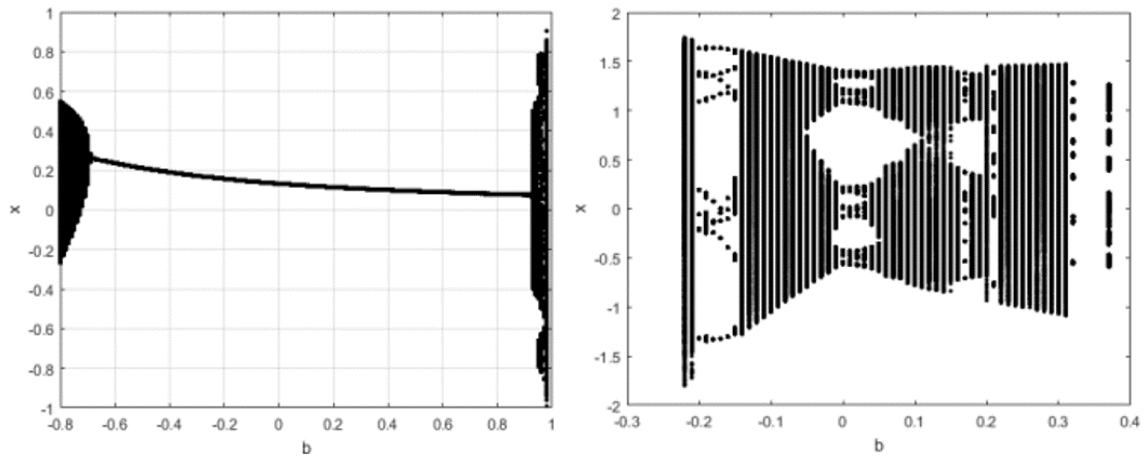

Fig. 3.1: Diagrame de bifurcație pentru parametrul a ținut fix la 0.15 (stânga), 1.4 (dreapta).

Pentru $a = 1.4$, situația este încă şi mai complexă, când b își schimbă succesiv valoarea, cu un pas de 10^{-2}, sistemul (3.1) alternează între comportament periodic, cu 8 soluţii, ca de exemplu pentru $b = -0.15$, 32 de soluţii cum e cazul pentru $b = 0.02$ sau acoperind întregul domeniu de amplitudine al lui x ca pentru $b = -0.19$. Acest tipar discontinuu pentru pseudo-aleatorism trebuie eliminat pentru a dobândi un pRNG cu proprietăţi statistice satisfăcătoare. Un studiu detaliat în acest sens este realizat în [16].

Contribuţia *Capitolului 3* este, în acest context, un algoritm de schimbare dinamică a valorilor parametrilor de bifurcație a şi b pentru a genera secvenţe pseudo-aleatoare care nu depind de valoarea inițială a acestora la execuţia pRNG-ului.

Într-un spaţiu tridimensional, spaţiul fazelor sau atractor, observăm în Fig. 3.2, pentru diferite perechi de parametri (a, b), funcţionarea sistemului Hénon în regim haotic (stânga), periodic(centru), sau chiar divergent către infinit (dreapta).

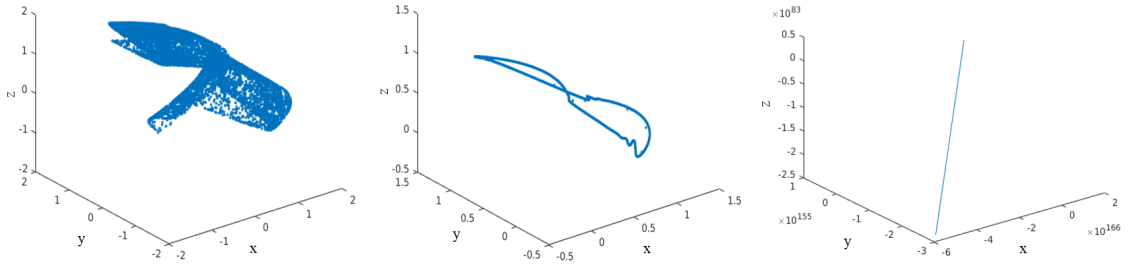

Fig. 3.2: Comportamentul sistemului Hénon 3-dimensional pentru diferite perechi (a,b).

Capitolul de faţă vine cu o îmbunătăţire a generatorului de numere pseudo-aleatoare din literatură [13], care folosea o pereche de parametri constanţi în evoluţia sistemului generalizat al lui Hénon producând, la fiecare iteraţie, valorile (x, y, z). Cel mai puţin semnificativi octeţi (LSB) ai acestora erau însumaţi modulo 2 fără transport (XOR-izaţi), aşa încât un byte pseudo-aleator era generat de sistem, la fiecare iteraţie. Schema bloc a acestuia este redată în Fig. 3.3. Varianta îmbunătăţită,

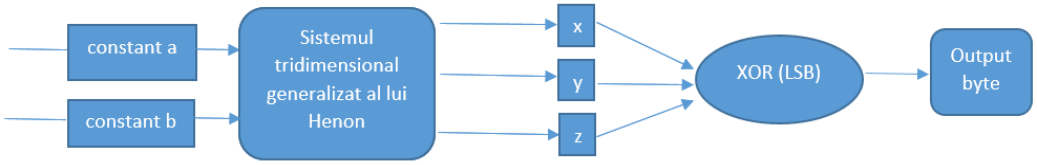

Fig. 3.3: Diagrama pRNG-ului propus în literatură.

prezentată în Fig. 3.4, face ca rezultatul criptării să nu mai fie dependent de alegerea parametrilor (a, b). Actualizatorul acestor parametri, notat cu e_1, va însuma valorile x, y şi z, la fiecare iteraţie, şi va actualiza valorile a și b, scalându-le în intervalele corespunzătoare, $(-2, 2)$ pentru a, respectiv $(-0.3, 0.3)$ pentru b, (3.2). Astfel, la fiecare iteraţie, avem de a face cu un comportament haotic, periodic sau divergent al sistemului tridimensional al lui Hénon, fără ca această alternanţă să altereze calitatea criptării imaginii. Pornind de la (a, b) anterior dat, trecem prin diferite regimuri la

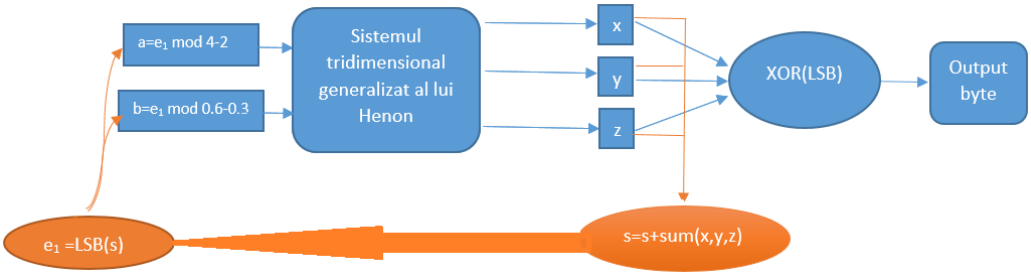

Fig. 3.4: Diagrama pRNG-ului propus în acest capitol.

iteraţiile ulterioare, ca în Fig. 3.2.

$$\begin{aligned} a &= e_1 mod 4 - 2 \\ b &= e_1 mod 0.6 - 0.3 \end{aligned} \tag{3.2}$$

Pentru imaginea stanga-sus din Fig. 3.5, utilizăm noul pRNG plecând cu perechea (a, b). Schimbând parametrii sistemului generalizat tridimensional al lui Hénon cu formulele prezentate, (ec. 3.2), alegerea unor parametri (a, b) care să corespundă unui comportament haotic devine o cerinţă opţională pentru buna funcţionare a pRNG-ului bazat pe acest sistem. Imaginea criptată nu o dezvăluie pe cea în clar, nici vizual, şi nici statistic, după cum se poate vedea în imaginea criptată dreapta-sus din Fig. 3.5 și histograma corespunzătoare.

În lucrarea [12] este diseminat un pas mai departe în cercetare, prin adăugarea unei a doua funcţii, în plus față de e_1, care poate actualiza parametrii (a, b) pe măsură ce imaginea în clar este criptată, bit cu bit. Aceasta este e_2 din ecuația 3.3. În studiul extins un aspect suplimentar este considerat: actualizarea parametrilor (a, b) nu mai este făcută la fiecare iteraţie, ci după un interval de actualizare.

$$\begin{aligned} e_1 &= e_1 + x_k + y_k + z_k \\ e_2 &= e_2 + sin((z_k - y_k)/2) \end{aligned} \tag{3.3}$$

În această extindere se testează mai multe sisteme. Se doreşte o configuraţie în care locul sistemului tridimensional al lui Hénon să poată fi ocupat de către oricare alt sistem capabil să manifeste şi comportament haotic.

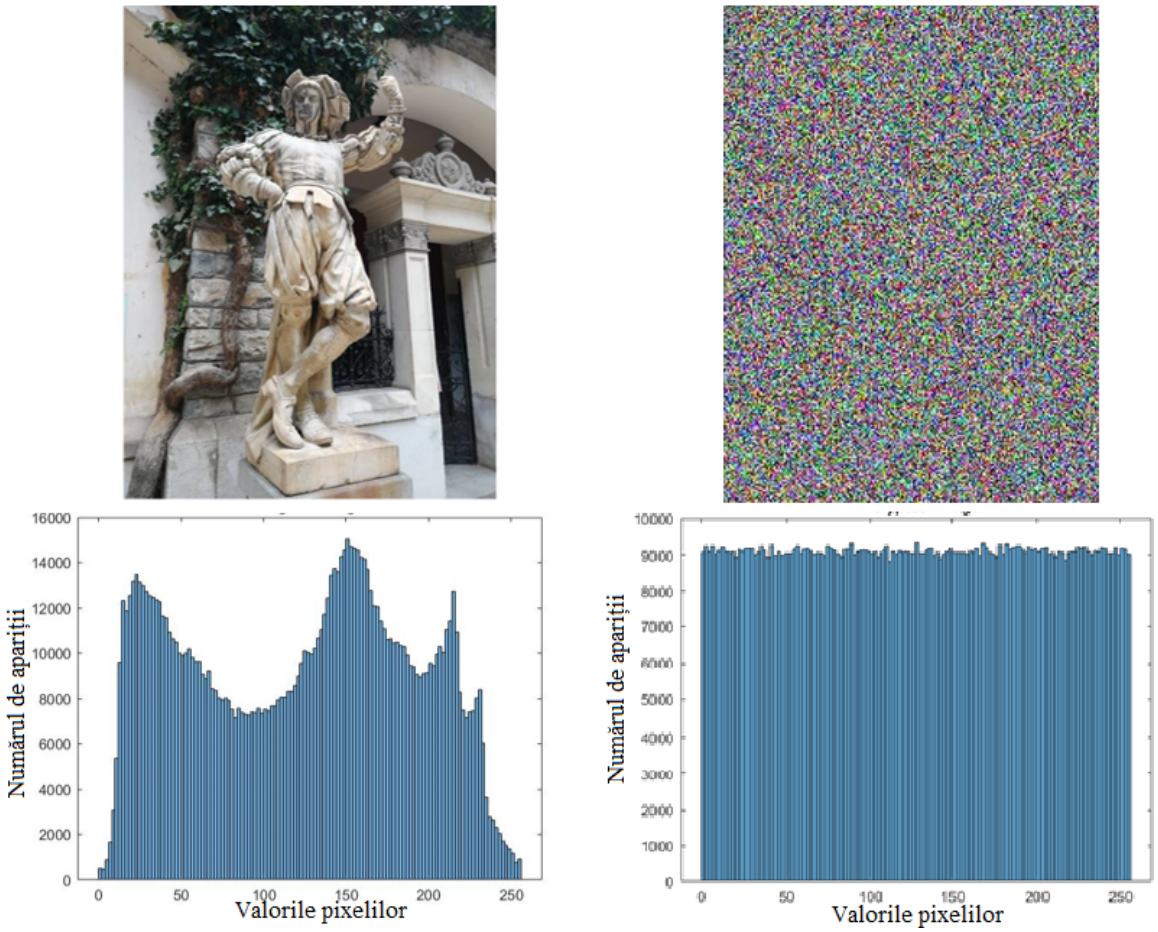

Fig. 3.5: Rezultatul criptării cu noul pRNG: imaginea originală (stânga-sus) și histograma corespunzătoare (stânga-jos), imaginea criptată (dreapta-sus) și histograma ei (dreapta-jos).

PRNG-ul rezultat este testat cu bateriile de test ale Institutului Naţional American de Standarde şi Tehnologii (NIST), dar şi cu Testul U01 [17]. Cu platforma de testare astfel formată au fost testate mai multe variante ale pRNG-ului propus de lucrarea de faţă, dar şi alte generatoare de numere pseudo-aleatoare din literatură, [18, 19], spre a servi pentru comparaţia performanţelor sale.

Capitolul 4

Criptanaliza matricei-cheie dintr-o comunicație secretă simetrică

Ideea *Capitolului 4* a pornit de la studiul unor lucrări din literatură [20, 21, 22]. În timpul participării la un workshop *Analyse du chaos et applications* în Cergy-Pontoise, Franța, am discutat câteva idei privind importanța analizei statistice în criptanaliză. Aceste discuţii au dus la cercetarea şi la diseminarea rezultatelor la o conferinţă ISI ATOM-n 2020 [23].

În acest capitol urmărim analiza statistică a unei scheme de criptare a datelor multimedia în general, în particular, aici, a unei imagini. Imaginea originală X este multiplicată cu o matrice ϕ conținând numere pseudo-aleatoare, cheia secretă. Rezultatul este stocat în matricea Y. Aceasta este schema de comunicație privată investigată, (4.1). Histogramele unei imagini criptate cu această metodă sunt prezentate în Fig. 4.1.

$$Y \;=\; \phi \cdot X \tag{4.1}$$

Urmărim să investigăm scenariul în care criptanalistul află matricea ϕ, vrând să extragă cheia secretă. Acest lucru este uşor, dacă atacatorul are la dispoziţie maşina de criptare. El criptează o imagine cunoscută, X'. Maşina îi dă la ieşire Y'. Cunoscând X', înmulţeşte 4.1, la dreapta, cu inversa matricei X' şi obţine, astfel, matricea cheie ϕ.

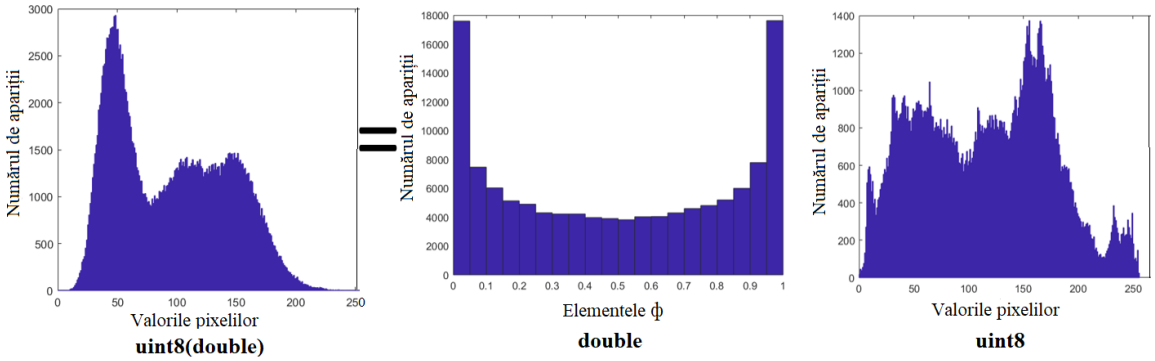

Fig. 4.1: Histrogramele corespunzătoare imaginii originale (dreapta), matricei ϕ (centru) și rezultatului criptării (stânga).

Se cunoaşte că matricea ϕ are drept elemente valori ale funcţiei logistice generate ca în Fig. 4.2, în scenariul investigat aici. Atacatorul încearcă, deci, având la dispoziţie matricea secretă, să afle date suplimentare despre parametrul de control R şi condiția initială care au generat-o. Este acest lucru posibil? Luăm în considerare

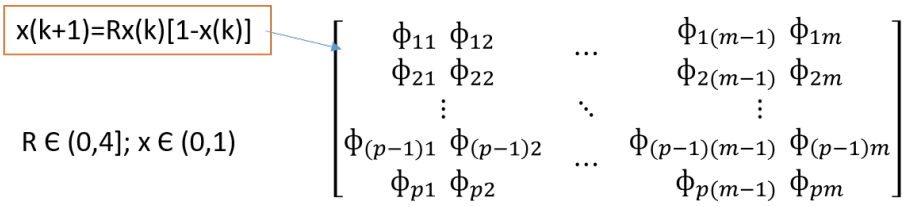

Fig. 4.2: Generarea matricei ϕ.

atât cazul în care matricea ϕ este generată cu funcția logistică luând toate iterațiile succesive, cât și cazul în care luăm iterațiile cu un anumit pas de eșantionare. Această strategie este inspirată din articolele din literatură ale echipei referitoare la distanța de independență statistică ilustrată în *Capitolul 2*, [6, 7].

Cele 2 scenarii sunt:

- Matricea ϕ, generată cu generatorul de numere pseudo-aleatoare - reprezentat de funcția logistică - este construită din iterațiile succesive ale funcției logistice;
- Distanța de eșantionare între iterațiile matricei ϕ considerate este distanța de independență statistică.

Pentru ambele cazuri considerăm timpul tranzitoriu de 250 de iterații, conform rezultatelor din literatură. Presupunem, deci, că suntem criptanalistul și am aflat matricea ϕ. Ne propunem să determinăm parametrul de control R. În acest scop folosim mai multe instrumente statistice: testul Smirnov (pentru a testa dacă două populații provin din aceeași distribuție), histograme (interpretarea vizuală a datelor), funcția de autocorelație (pentru a vedea influența parametrului de control asupra acesteia), precum și investigarea iterațiilor succesive.

Procesul aleator determinat de parametrul R fiind un proces ergodic, aşa cum discutam în *Cap. 2*, condiţia iniţială, x_0, este irelevantă, aici. Parametrul R folosit pentru a genera matricea ϕ poate fi recuperat aplicând testul Smirnov. Testul este trecut dacă îl aplicăm pe eșantioane extrase din matricea ϕ și eșantioane extrase din traiectoriile funcției logistice având același parametru R, chiar dacă se pleacă de la condiții inițiale diferite.

Histogramele arată clar că pentru parametru de control diferit, distribuția frecvențelor este diferită (pentru iterații succesive sau considerând distanța de independență), Fig. 4.3.

Funcția de autocorelație investigată în *Cap. 2* este de asemenea studiată în

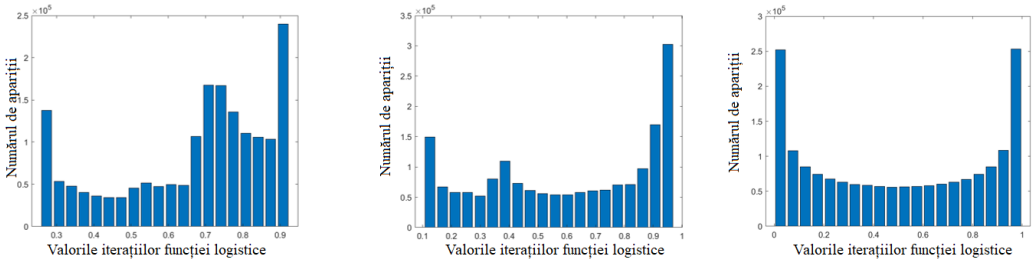

Fig. 4.3: Histograme ale funcției logistice pentru $x(0) = 0.4557$, $d = 1$ si $R = 3.7$ (stânga), $R = 3.89$ (centru), $R = 4$ (dreapta).

acest context. Concluzionăm că forma acesteia depinde de parametrul R. Analizând funcția de autocorelație pentru același R și plecând de la condiții inițiale diferite, funcția de autocorelație are aceeași formă. Dacă R este diferit, chiar și pentru aceleași condiții inițiale forma funcției de autocorelație diferă. Aceleași rezultate le avem și când luăm în considerare iterații succesive, și când luăm iterațiile cu o

anumită distanță. Procesul aleator este determinat doar de parametrul R, așa cum intuiam încă de la început și precum se vede în Fig. 4.4.

Investigând iterațiile matricei ϕ, pentru a recupera parametrul R, pentru cazul

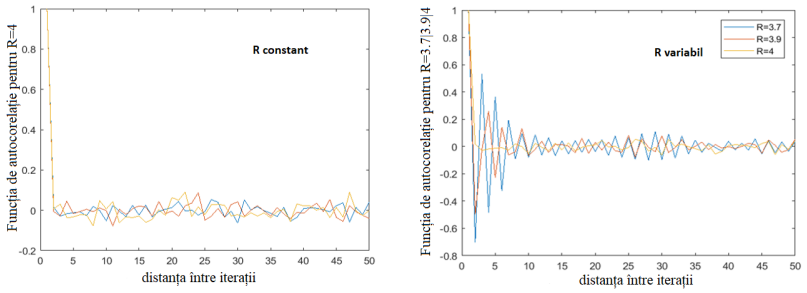

Fig. 4.4: Funcția de autocorelație pentru $R = 4$ constant (stânga) și R variabil (dreapta).

în care am considerat iterații succesive, dar și pentru cazul în care valorile sunt eșantionate conform distanței de indepedență, rezultatele arată că: dacă avem acces la iterații succesive putem găsi parametrul R cu o eroare relativă de ordinul 10^{-9} ca în Tabelul 4.1, în timp ce dacă știm iterațiile funcției logistice cu o anumită distanță între eșantioane, R-ul recuperat este foarte diferit de cel original cum putem vedea în Tabelul 4.2. Astfel, rezultă că avem nevoie de cel puțin două iterații succesive extrase din funcția logistică pentru a afla parametrul R.

R	3.999029407218239	4
$\hat{R}$	3.999029407100511	4.000000000137501
[($\hat{R}$ - R)/R] [%]	**2.94391433550104e-9**	**3.437525e-9**

Tabel 4.1: Erori relative între R estimat și R original, $d = 1$.

R	3.999029407218239	4
$\hat{R}$	3.052585858468511	0.227703495214937
[($\hat{R}$ - R)/R] [%]	**23.66683143268213**	**94.30741261962658**

Tabel 4.2: Erori relative între R estimat și R original, $d > 1$.

Capitolul 5

Algoritmi criptografici cu pachete wavelet și sisteme haotice

În acest capitol sunt prezentate îmbunătățiri ale unor algoritmi criptografici din literatură folosind pachete wavelet și funcții haotice. Pachetele wavelet le-am folosit în faza de pre-procesare a algoritmului, în timp ce funcțiile haotice sunt utilizate pentru împrăștierea pixelilor în toată plaja de valori posibile. Rezultatele sunt diseminate într-un articol de revistă [24], precum și două lucrări de conferință indexate în ISI Web of Science, [23] și [25].

În Fig. 5.1 este prezentată transformata wavelet discretă 2D, implementată folosind filtre digitale și decimatoare. Pe un nivel de descompunere avem un coeficient de aproximare (A_{j+1}) și 3 coeficienți detaliu (H_{j+1}, V_{j+1}, D_{j+1}). Am folosit transformata Haar în simularile noastre deoarece aceasta s-a mapat pe necesitățile algoritmului, permițând reconstrucția semnalului, în cazul nostru a imaginii, fără a introduce efecte de margine.

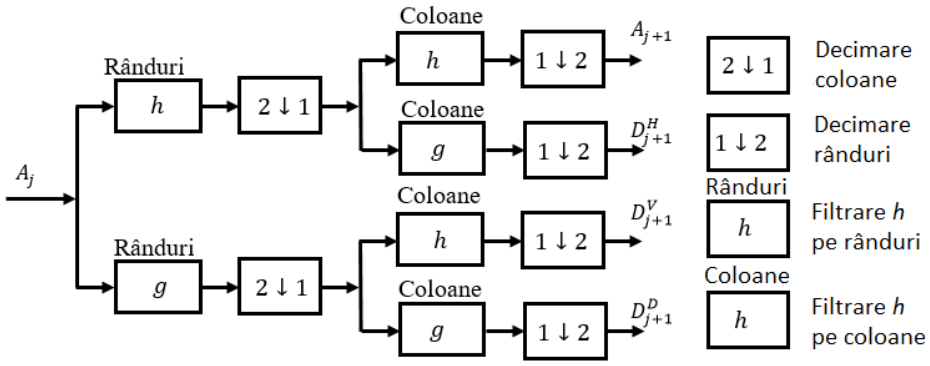

Fig. 5.1: Transformata wavelet discretă 2D.

În lucrarea [24] se prezintă o îmbunătățire a unui algoritm din literatură, [26], folosind pachete wavelet și sistemul haotic cort. Permutarea pachetelor wavelet s-a folosit pentru a înlocui simpla permutare a pixelilor existentă în algoritm, iar funcția cort înlocuiește sistemul Hénon și este utilizată pentru distribuția sa uniformă care ajută la împrăștierea pixelilor în toată plaja de valori posibile. Schema algoritmului este prezentată în Fig. 5.2.

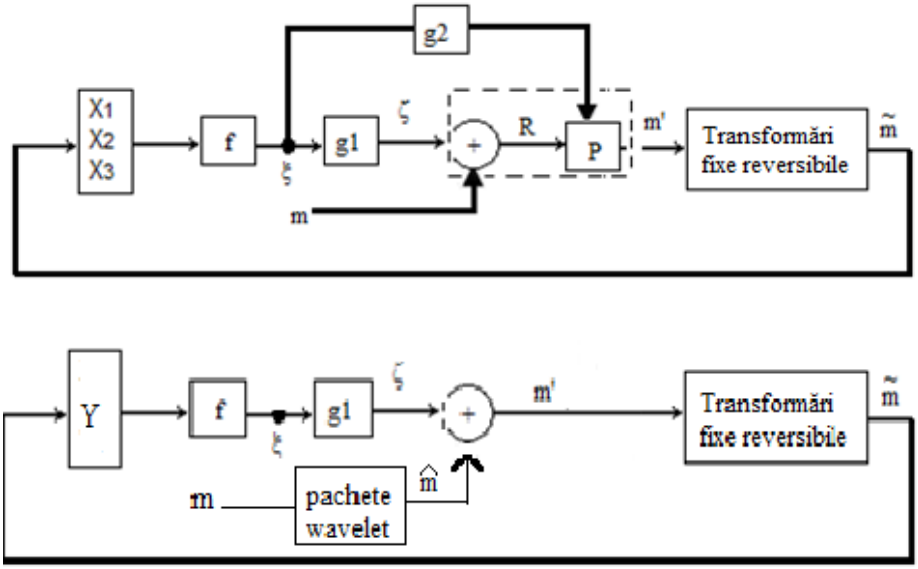

Fig. 5.2: Schema de criptare originală (sus) și cea îmbunătățită (jos).

Semnificația schemei este următoarea:

- $[Y]$ reprezintă funcția cort. Pentru parametrul de control p' și condiția inițială $y(0)$ aleasă aleatoriu, rezultă o realizare particulară a procesului aleatoriu.
- f corespunde unei transformări de variabilă aleatoare care conduce la o variabilă random discretă $\xi = f(sin(y))$, cu $\xi \in 1, 2, ..., 10$.
- g_1 alocă variabilei aleatoare ξ un număr întreg în intervalul $[0, 255]$, $g_1(\xi) = \zeta$.
- m este imaginea originală.
- permutarea $P = g_2(\xi)$ din algoritmul anterior este înlocuită de descompunerea imaginii ce se dorește a fi criptată cu pachete wavelet folosind transformata Haar și permutarea acestor pachete cu funcția logistică, ec. 2.2.
- $\widehat{m}$ este reprezentarea ASCII pe 8 biți a unui pixel din imaginea permutată cu pachete wavelet.

- m' este criptograma obținută după cifrare, fiind un byte rezultat din operația *bitxor* între $\widehat{m}$ și ζ.
- mesajul în binar rezultat este transformat în zecimal și scalat cu un factor ν; scalarea permite includerea mesajului în evoluția funcției cort fără afectarea dinamicii acesteia.
- $\widetilde{m}$ este mesajul scalat ce este adăugat în evoluția sistemului haotic cort.

A fost considerat un exemplu practic, o imagine, a carei histogramă ne-uniformă se poate observa în Fig. 5.3. După descompunerea cu pachete wavelet, amestecarea acestora și recompunere a rezultat o imagine, a cărei histogramă nu este uniformă, deci nu se poate vorbi încă de o criptare satisfăcătoare.

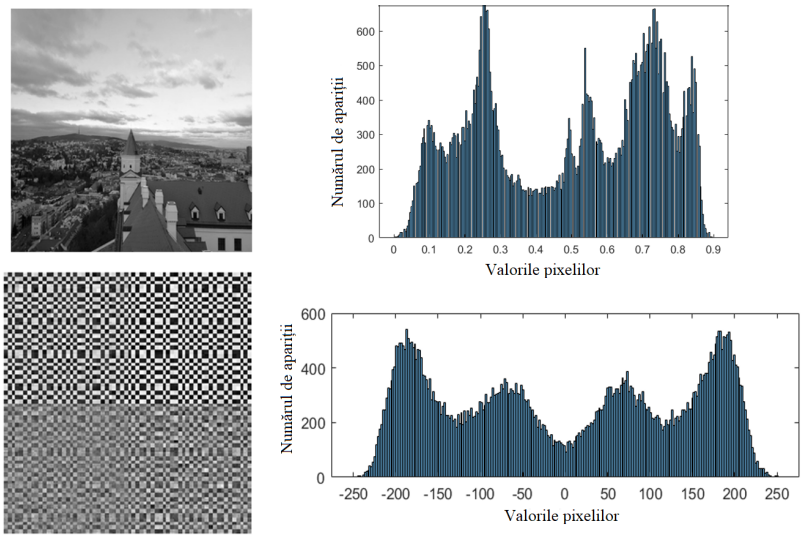

Fig. 5.3: Imaginea originală și histograma asociată (sus) & Imaginea criptată cu wavelet și histograma ei (jos).

După includerea imaginii, astfel amestecată cu pachete wavelet, în evoluția funcției haotice cort, așa cum am descris în algoritmul prezentat, a rezultat o imagine perfect criptată, a cărei histogramă uniformă se poate vedea în Fig. 5.4. Se observă clar îmbunătățirea adusă în comparație cu histograma imaginii criptate cu algoritmul de referință [26]; în plus entropia imaginii criptate este aproape de valoarea maximă 8, iar diagrama de dispersie arată că pixelii sunt impaștiați în toată plaja de valori posibile.

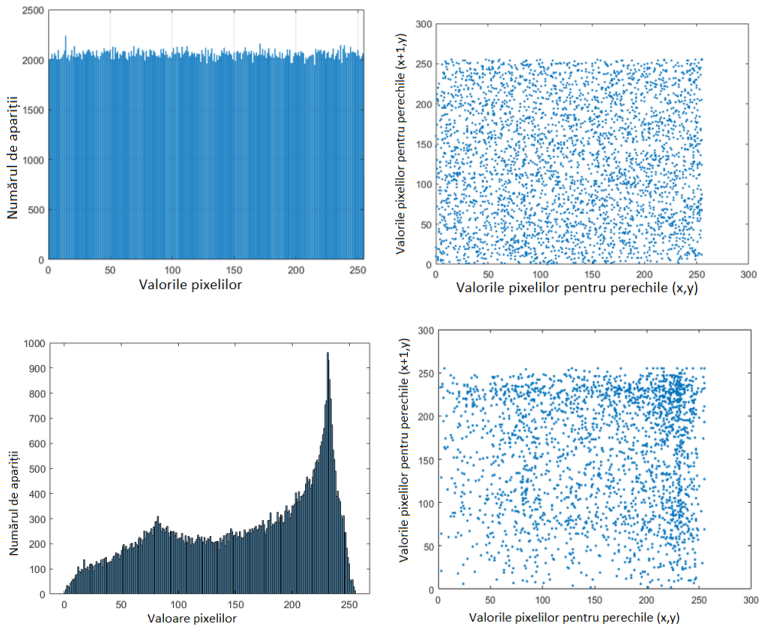

Fig. 5.4: Histograma și corelația imaginii criptate cu algoritmul propus (sus) vs. histograma și corelația imaginii criptate cu algoritmul original (jos), [26].

Luând în considerare vulnerabilitățile algoritmului de criptare din Capitolul 4 - algoritm în care o matrice generată cu funcția haotică logistică se înmulțește cu mesajul în clar - s-a propus în acest capitol o îmbunătățire prin adăugarea de noi pași, și anume descompunerea cu pachete wavelet, permutarea cu funcția logisică și utilizarea sistemului haotic 3D Arnold. Acești pași suplimentari încetinesc eforturile atacatorului de a sparge cifrul. Mai departe s-a dorit îmbunătățirea algoritmului. Astfel, s-a înlocuit permutarea pachetelor wavelet cu funcția logistică din algoritmul de criptare cu permutarea folosind funcția haotică Baker. De asemenea, generarea matricei ϕ nu s-a mai făcut cu funcția logistică, ci cu funcția cort. S-au testat astfel, comparativ, mai multe sisteme haotice.

Capitolul 6

Concluzii, perspective și contribuții originale

6.1 Concluzii și perspective

Capitolul 1 încadrează teza în domeniul căreia îi aparţine, cel al metodelor statistice aplicate în domeniul semnalelor haotice cu perspectiva folosirii lor în criptografie și, mai larg, în domeniul comunicațiilor.

Capitolul 2 prezintă prima contribuţie a tezei, un test de medie pe funcția de autocorelație, test ce susține distanța de independență statistică corespunzătoare sistemelor haotice, studiată în articolele anterioare ale echipei. Întrucât nu am găsit în literatură lucrări pe această temă, considerăm că este un studiu original din punct de vedere teoretic și experimental. Studiul este particularizat pe două sisteme haotice în timp discret, funcţia cort şi funcţia logistică. Este studiată şi senzitivitatea funcţiei logistice la schimbarea valorii parametrului de control și efectul asupra testului de medie. Această variație a valorii parametrului afectează rezulatele testului de medie și este într-o conexiune strânsă cu distanța de independență statistică. Este confirmată intuiţia că decorelarea apare mai repede decât independența statistică. Am lucrat cu precizie dublă și extinsă, folosind o librărie pentru precizie aritmetică arbitrară, concluzionând că precizia folosită în calcule nu determină schimbări majore în rezultatele testului propus deoarece distanța de independență, cât și cea de decorelare sunt mai mici decât distanța la care traiectoriile încep să fie alterate, caracterul pseudo-aleator degradându-se.

Capitolul 3 propune un algoritm care sa crească performanţa unui generator de numere pseudo-aleatoare bazat pe sistemul haotic tridimensional generalizat al lui Hénon, în timp discret. Algoritmul schimbă dinamic valoarea parametrilor de bifurcație a și b. Studiul a fost extins printr-un şablon de generatoare de numere aleatoare, configurabil pentru diverse sisteme haotice și diverși parametri. Ca perspectivă ne propunem să demonstrăm că generatorul este performant din punct de vedere criptografic și își poate găsi aplicabilitatea în lumea reală.

Capitolul 4 analizează din punctul de vedere al criptanalistului o schemă de criptare exemplificată pe imagini. Concentrarea este pe determinarea parametrului de control R din matricea, cheia secretă de criptare, generată cu funcţia logistică. Mai multe metode statistice sunt aplicate în acest sens: testul Smirnov, histograme, funcția de autocorelație, precum și analiza valorilor iterațiilor vecine. O perspectivă, neinvestigată, încă, este schimbarea dinamică, la fiecare k iteratii, a valorii parametrului R corespunzător matricei ϕ.

Capitolul 5 investighează beneficiile aduse de pachetele wavelet în faza de preprocesare a schemei de criptare și utilizarea acestora împreună cu sistemele haotice. Un algoritm din literatură este îmbunătățit cu ajutorul pachetelor wavelet și al sistemului haotic reprezentat de funcţia cort. De asemenea, schemei de criptare din Capitolul 4 îi sunt adăugați noi pași pentru a crește robustețea algoritmului.

Capitolul 6 prezintă concluziile, perspectivele și curiozitatea autorului de a studia evoluția sistemelor dinamice în timp continuu, [27], [28].

Rezultatele obţinute în urma cercetării din lucrarea de faţă au continuat lucrările echipei din care fac parte, şi reprezintă ele însele direcţii de cercetare viitoare.

6.2 Diseminarea activității de cercetare

6.2.1 Articole de revistă

1. Octaviana Datcu, **Corina Macovei**, Radu Hobincu, *"Chaos Based Cryptographic Pseudo-Random Number Generator Template with Dynamic State*

Change," Appl. Sci. 2020, https://doi.org/10.3390/app10020451, Published: 8 January 2020, https://www.mdpi.com/2076-3417/10/2/451, Applied Sciences-Basel, Vol. 10, Issue: 2, Article Number: 451, DOI: 10.3390/app10020451, JAN 2020, MDPI, ST Alban-Anlage 66, CH-4052 Basel, Switzerland, WOS 000522540400027, Impact Factor: 2.474, **Q2**.

2. **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

6.2.2 Articole de conferință

3. **Corina Macovei**, Alezandru Văduva, Adriana Vlad și Marta Zamfir, *"A mean test on the autocorrelation function of a chaotic signal aiming to support the statistical independence sampling distance,"* 2019 International Symposium on Signals, Circuits and Systems (ISSCS), Iasi, Romania, 2019, pp. 1-4, doi: 10.1109/ISSCS.2019.8801778, WOS:000503459500050

4. Radu Hobincu, Octaviana Datcu și **Corina Macovei**, *"Entropy global control for a chaos based pRNG,"* 2019 42nd International Conference on Telecommunications and Signal Processing (TSP), Budapest, Hungary, 2019, pp. 432-435. doi: 10.1109/TSP.2019.8768818. WOS:000493442800094

5. Octaviana Datcu, Radu Hobincu, **Corina Macovei**, *"Singular Value Decomposition to Determine the Dynamics of a Chaotic Regime Oscillator,"* 2019 International Semiconductor Conference, CAS Proceedings, Sinaia, Romania, October 2019, pp. 119-122, WOS:000514295300024, **Julkaisu conference 1**, https://www.imt.ro/cas/, https://www.tsv.fi/julkaisufoorumi/haku.php?nimeke=&konferenssilyh=CAS&issn=&tyyppi=kaikki&kieli=&maa=&wos=&scopus=&nappi=Search.

6. Octaviana Datcu, Radu Hobincu, **Corina Macovei**, *"Genetic Algorithms for high-Order sliding-Mode Observers,"* 2019 International Semiconduc-

tor Conference, Sinaia, CAS Proceedings, Romania, October 2019, pp. 305-308, WOS:000514295300064, **Julkaisu conference 1**, `https://www.imt.ro/cas/`, `https://www.tsv.fi/julkaisufoorumi/haku.php?nimeke=&konferenssilyh=CAS&issn=&tyyppi=kaikki&kieli=&maa=&wos=&scopus=&nappi=Search`.

7. **Corina Macovei**, Alexandru Văduva, Adriana Vlad și Bogdan Badea, *"The autocorrelation function of the logistic map chaotic signal in relation with the statistical independence issue"*, 13th International Conference on Communications (COMM), Bucuresti, Romania, June 2020, pp. 25-30, IEEE, doi: 10.1109/COMM48946.2020.9142000

8. **Corina Macovei**, Adina-Elena Lupu, Mircea Răducanu și Octaviana Datcu , *"Key extraction in a chaos-based image cipher and wavelet packets"*, ATOM-N 2020, The 10th edition of the International Conference "Advanced Topics in Optoelectronics, Microelectronics and Nanotechnologies," 20 - 23 August 2020, Constanta, Romania, **EXCELLENT PAPER AWARD**

9. **Corina Macovei**, Mircea Răducanu și Octaviana Datcu, *"Image encryption algorithm using wavelet packets and multiple chaotic maps"*, International Symposium on Electronics and Telecommunications (ISETC), IEEE, November 2020

6.2.3 Rapoarte de cercetare

10. **Corina Macovei**, *"Analiza independenței statistice între mulțimi de date experimentale extrase din funcția cort și sistemul dinamic haotic Hénon."* (Iunie 2015)

11. **Corina Macovei**, *"Model de aplicație de securitate ce urmărește profilul utilizatorului din punctul de vedere al protecției informațiilor personale."* (Decembrie 2015)

12. **Corina Macovei**, *"Studiu statistic privind utilizarea secvențelor binare generate de funcția cort în aplicații criptografice. Ilustrare pe imagini."* (Iunie 2016)

13. **Corina Macovei**, *"Studiu asupra funcției de autocorelație statistică asociată semnalului haotic tent map în relație cu distanța de independență statistică."* (Decembrie 2016)

14. **Corina Macovei**, *"Simulări cu diverse perechi de parametri de control ai sistemului dinamic Hénon în vederea testării unui algoritm de generare de numere pseudo aleatoare."* (Iunie 2017)

6.2.4 Școală de vară, simpozion, stagiu, workshop

15. *"Security and Privacy in Digital Life 2015"*, Summer School Privacy, Security and Trust, June 29th - July 10th 2015, Trento, Italy

16. **Corina Macovei**, Adriana Vlad și Marta Zamfir, *"On the autocorrelation function of the skew tent map chaotic signal in relation with the statistical independence sampling distance,"* Annual Symposium of Doctoral School ETTI-B, SADETTI, 2018, Bucharest, Romania

17. Stagiu la Applications École Nationale Supérieure de l'Électronique et de ses Applications (ENSEA), Cergy, France, 24 May -14 June 2019

18. **Corina Macovei**, Adina-Elena Blaj, Octaviana Datcu, Radu Hobincu, *"Cryptanalysis of a compressive sensing communication scheme,"* Workshop "Analyse du chaos et applications," Applications École Nationale Supérieure de l'Électronique et de ses Applications (ENSEA), Cergy, France, December 2019

Bibliography

[1] The butterfly effect and the maths of chaos, Maths careers and The Institute of mathematics and its applications, online on 30th of June 2020 at https://www.mathscareers.org.uk/article/the-butterfly-effect-and-the-maths-of-chaos/

[2] C. Macovei, A. Văduva, A. Vlad and M. Zamfir, "A mean test on the autocorrelation function of a chaotic signal aiming to support the statistical independence sampling distance," in International Symposium on Signals, Circuits and Systems (ISSCS2019), Iaşi, 2019, pp. 1-4, IEEE.

[3] C. Macovei, A. Văduva, A. Vlad and B. Badea, "The autocorrelation function of the logistic map chaotic signal in relation with the statistical independence issue," In 2020 13th International Conference on Communications (COMM) (pp. 25-30). IEEE.

[4] A. Leontitsis (2020). Spearman Rank Correlation, `https://www.mathworks.com/matlabcentral/fileexchange/4374-spearman-rank-correlation`, MATLAB Central File Exchange. Retrieved July 8, 2020.

[5] Correlation coefficients, Mathworks, online at `https://www.mathworks.com/help/matlab/ref/corrcoef.html` on 8 July 2020.

[6] B. Badea and A. Vlad, "Revealing statistical independence of two experimental data sets: an improvement on Spearman's algorithm," in International Conference on Computational Science and Its Applications, pp. 1166-1176, Springer, Berlin, Heidelberg.

[7] A. Văduva, A. Vlad and B. Badea, "Evaluating the performance of a test-method for statistical independence decision in the context of chaotic signals," In 2016 International Conference on Communications (COMM), pp. 417-422, IEEE, Bucharest, Romania

[8] A. Luca, A. Vlad, B. Badea and M. Frunzete, "A study on statistical independence in the tent map," In 2009 International Symposium on Signals, Circuits and Systems (pp. 1-4). IEEE.

[9] A.Vlad, A. Luca and M. Frunzete, "Computational measurements of the transient time and of the sampling distance that enables statistical independence in the logistic map," in O. Gervasi et al. (eds) Computational Science and Its Applications – ICCSA 2009, Lecture Notes in Computer Science, vol 5593, pp. 703-718, Springer, 2009.

[10] O. Hodea and A. Vlad, "Logistic map sensitivity to control parameter and its implications in the statistical behaviour," In International Symposium on Signals, Circuits and Systems ISSCS2013, pp. 1-4, IEEE, Iasi, Romania

[11] R. Hobincu, O. Datcu and C. Macovei, (2019, July). "Entropy global control for a chaos based pRNG," In 2019 42nd International Conference on Telecommunications and Signal Processing (TSP), pp. 432-435, IEEE, Budapest, Hungary

[12] O. Datcu, C. Macovei and R. Hobincu, (2020). "Chaos Based Cryptographic Pseudo-Random Number Generator Template with Dynamic State Change," Applied Sciences, 10(2), 451, doi: 10.3390/app10020451

[13] R. Hobincu, O. Datcu, "A novel Chaos Based PRNG Targeting Secret Communication," 12th International Conference on Communications (COMM),pp. 459-462, Bucharest, Romania, 2018, WOS: 000449526000086.

[14] R. Hobincu, O. Datcu, "FPGA Implementation of a Chaos Based PRNG Targeting Secret Communication," 13th Symposium on Electronics and

Telecommunications (ISETC 2018), pp. 1-4, Timişoara, Romania, WOS: 000463031500052.

[15] D.A. Miller, G. Grassi, "A discrete generalized hyperchaotic Hénon map circuit," Proceedings of the 44th IEEE 2001 Midwest Symposium on Circuits and Systems, Dayton, OH, 2001, 328-331, Vol. 1.

[16] R. Hobincu, O. Datcu, "NIST tests versus bifurcation diagrams and Lyapunov exponents when evaluating chaos-based pRNGs," (ITISE 2018) International Conference on Time Series and Forecasting Proceedings of Papers, Granada, Spain, ISBN: 978-84-17293-57-4.

[17] A. Suciu, R.A. Toma, K. Marton, "Parallel implementation of the TestU01 statistical test suite," In Proceedings of the 2012 IEEE 8th International Conference on Intelligent Computer Communication and Processing, Cluj-Napoca, Romania, 30 August–1 September 2012; pp. 317–322.

[18] M. Matsumoto, T. Nishimura, "Mersenne twister: A 623-dimensionally equidistributed uniform pseudo-random number generator." ACM Trans. Model. Comput. Simul. (TOMACS) 1998, 8, 3–30.

[19] D. J. Bernstein, "ChaCha, A Variant of Salsa20." Workshop Record of SASC 2008: The State of the Art of Stream Ciphers. Available online: https://cr.yp.to/chacha/chacha-20080120.pdf (accessed on 25 November 2020).

[20] L. Yu, J.-P. Barbot, G. Zheng and H. Sun, (2010). "Compressive sensing with chaotic sequence". IEEE Signal Processing Letters, 17(8), 731-734.

[21] L. Yu, J.-P. Barbot, G. Zheng and H. Sun, (2010, July). "Toeplitz-structured chaotic sensing matrix for compressive sensing". In 2010 7th International Symposium on Communication Systems, Networks and Digital Signal Processing (CSNDSP 2010) (pp. 229-233). IEEE.

[22] M. Frunzete, L. Yu, J.-P. Barbot and A. Vlad, (2011, September). "Compressive sensing matrix designed by tent map, for secure data transmission". In Signal

Processing Algorithms, Architectures, Arrangements, and Applications SPA 2011 (pp. 1-6). IEEE.

[23] C. Macovei, A. Lupu, M. Răducanu and O. Datcu, "Key extraction in a chaos-based image cipher with wavelet packets," ATOM-N 2020, The 10th edition of the International Conference "Advanced Topics in Optoelectronics, Microelectronics and Nanotechnologies," 20 - 23 August 2020, Constanta, Romania.

[24] C. Macovei, A. Lupu and 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

[25] C. Macovei, M. Răducanu and O. Datcu, "Image encryption algorithm using wavelet packets and multiple chaotic maps," International Symposium on Electronics and Telecommunications (ISETC), IEEE, Timisoara, Romania, November 2020.

[26] O. Datcu, J.-P. Barbot, A. Vlad, "New enciphering algorithm based on Chaotic Generalized Henon Map", in Modeling, Simulation and Applications Selected Papers from the 3rd Chaotic Modeling and Simulation International Conference CHAOS2010) edited by Christos H. Skiadas, Ioannis Dimotikalis & Charilaos Skiadas, World Scientific, Singapore, 2011, ISBN: 978-981-4350-33-4

[27] O. Datcu, R. Hobincu, C. Macovei, "Singular Value Decomposition to Determine the Dynamics of a Chaotic Regime Oscillator," 2019 International Semiconductor Conference, Sinaia, Romania, October 2019, pp. 119-122, WOS:000514295300024, JULKAISU conference 1.

[28] O. Datcu, R. Hobincu, C. Macovei, "Genetic Algorithms for high-Order sliding-Mode Observers," In 2019 International Semiconductor Conference, Sinaia, Romania, October 2019, pp. 305-308, WOS:000514295300064, JULKAISU conference 1.