Deterministický chaos a jeho využití v kryptografii

Deterministic chaos and its applications in cryptography

Radek Kalabus

Bakalářská práce
2010

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2009/2010

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Radek KALABUS**
Osobní číslo:	**A07048**
Studijní program:	**B 3902 Inženýrská informatika**
Studijní obor:	**Informační a řídicí technologie**
Téma práce:	**Deterministický chaos a jeho využití v kryptografii**

Zásady pro vypracování:

1. **Vypracování literární rešerše na téma využití chaosu v kryptografii.**
2. **Analýza vlastností deterministického chaosu.**
3. **Návrh kryptografického systému pro statické obrazy.**
4. **Bezpečnostní analýza šifrovaných obrazů.**
5. **Srovnání metody s jinými kryptografickými systémy.**

Rozsah bakalářské práce:

Rozsah příloh:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **Delfs, H., Knebl, H. Introduction to Cryptography. Springer, Berlin, 2007, ISBN 978-3-540-49243-6**
2. **Peitgen, H. Chaos and Fractals: New Frontiers of Science. Springer, Berlin, 2004, ISBN 978-0-387-97903-8**
3. **Sengupta, A. Chaos, nonlinearity, complexity: the dynamical paradigm of nature, Springer, Berlin,**
4. **Sprott, J.C. Chaos and Time-Series Analysis, Oxford University Press, 2003, ISBN 978-0-198-50840-3**
5. **Sprott, J.C. Strange attractors: Creating Patterns in Chaos. M&T Books, 1993, ISBN 978-1-558-51298-6**
6. **Mao, Y., Chen, G. Chaos-Based Image Encryption. Springer, Berlin, 2003, ISBN 978-3-540-31756-2**
7. **Giesl, J., Vlcek, K. Image Encryption Based on Strange Attractor. ICGST-GVIP Journal, 2009, vol. 9, is. 2, pp. 19-26, ISSN 1687-398**
8. **Hossam, A., Hamdy, K., Osama, A. An Efficient Chaos-Based Feedback Stream Cipher (ECBFSC) for Image Encryption and Decryption. Informatica 31, 2007**
9. **Wong, K-W., Kwok, B.S-H., Law, W-S. A Fast Image Encryption Scheme based on Chaotic Standard Map. Physics Letters A. 2008, vol. 372, is. 15, pp. 2645-2652, ISSN 0375-9601**

Vedoucí bakalářské práce: **Ing. Jiří Giesl**
Ústav počítačových a komunikačních systémů

Datum zadání bakalářské práce: **5. března 2010**

Termín odevzdání bakalářské práce: **1. června 2010**

Ve Zlíně dne 5. března 2010

prof. Ing. Vladimír Vašek, CSc.
děkan

L.S.

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky

doc. Ing. Ivan Zelinka, Ph.D.
ředitel ústavu

ABSTRAKT

První část této práce se zaměřuje na vysvětlení základních pojmů teorie chaosu a jeho využití. Další část je zaměřena na jednodimenzionální mapy a kryptografii. V poslední části se zaměřuje na navržení a vytvoření kryptografického systému, který je pak zkoumán a srovnáván s jinými systémy.

Klíčová slova: Deterministický chaos, kryptografie, logistická mapa

ABSTRACT

The first part of this work is focused on explaining the basic concepts of chaos theory and its applications. Another section focuses on one-dimensional maps and cryptography. The last part focuses on the design and creation of cryptographic system, which is then examined and compared with other systems.

Keywords: Deterministic chaos, cryptography, logistic map

Rád bych zde poděkoval vedoucímu bakalářské práce Ing. Jiřímu Gieslovi, za odbornou pomoc a vedení v průběhu celé tvorby této práce. Také bych rád poděkoval mým rodičům za podporu v průběhu celého studia.

Prohlašuji, že

- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně …….

podpis diplomanta

OBSAH

ÚVOD

Důležitost kryptografie roste ze dne na den. S rozvíjením internetu a výpočetního výkonu počítačů se nedávno neprolomitelné šifry stávají zastaralé. Teorie chaosu proto slibuje velké využití a to nejen na tomto poli. Deterministický chaos není náhodné chování, jak by se mohlo zdát, ale je striktně předurčeno. Právě toho se dá s úspěchem využít v kryptografii, která se zabývá utajováním informací.

Ve druhé polovině dvacátého století se obsah pojmu chaos začíná měnit. Dříve se chaos používal jen ve smyslu zmatku a neuspořádanosti. V matematice chaos začal znamenat neperiodické deterministické chování, které je velmi citlivé na počáteční podmínky.

Kryptografie je už od starověku brána jako obor, který se zabývá utajováním informací. Moderní kryptografii můžeme datovat od sedmdesátých let dvacátého století a zabývá se i jinými službami než je utajování.

Tato práce vznikla proto, aby názorným příkladem předvedla symbiózu těchto dvou oborů. Praktická část je zaměřena na tvorbu programu, který dokáže zašifrovat a dešifrovat obrázek.

I. TEORETICKÁ ČÁST

1 DETERMINISTICKÝ CHAOS

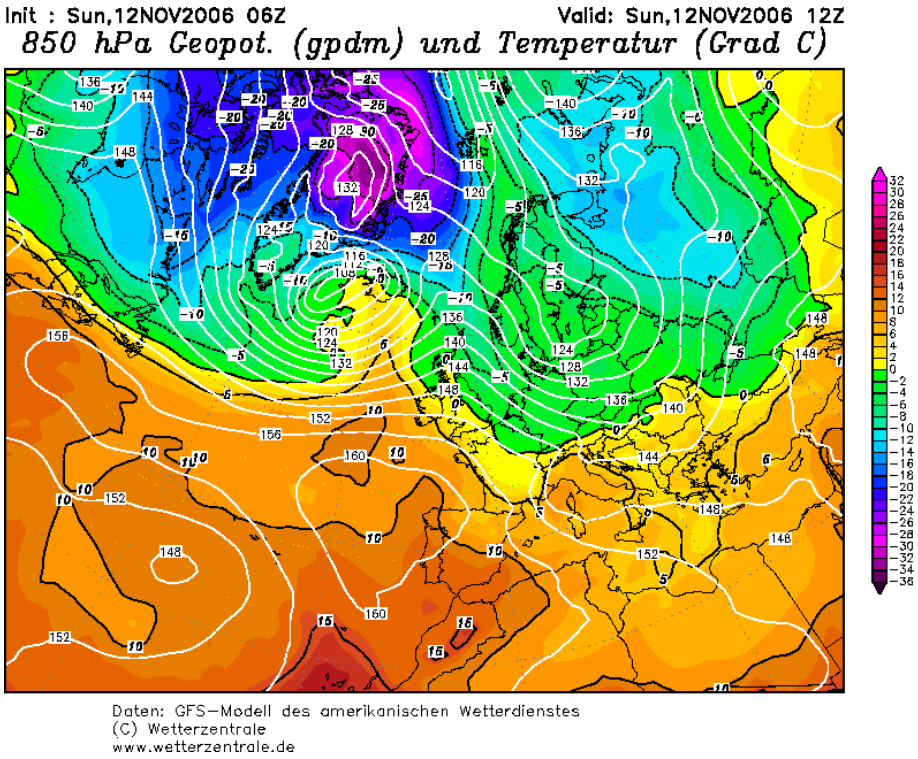
1.1 Co je to deterministický chaos

Mluvit o chaosu jako o součásti vědy se zdá na první pohled nepatřičné. Rozebereme si název deterministický chaos po jednotlivých slovech. Termín determinismus se používá tehdy, jestliže můžeme jednoznačně určit budoucnost systému. Pod pojmem chaos si vybavíme neuspořádanou strukturu nebo také náhodnou strukturu. Slovo chaos je známo už dlouhá staletí, když například staří Řekové věřili, že jejich bohové vznikli z chaosu. Příklady použití tohoto slova můžeme pozorovat i v ostatních mytologiích a náboženstvích a to je známka toho, že chaos zajímal lidi už v dobách dávno minulých. Determinismus a chaos si tedy odporují, ale jak je možné, že se používají tyto slova dohromady? Některé systémy, které se vyskytují v přírodě nebo jsou vytvořeny člověkem, se chovají tak, že prakticky nemůžeme určit jejich budoucnost, ale zároveň jsou tyto systémy naprosto deterministické. U těchto systémů jsou velmi důležité počáteční podmínky, protože i malá změna těchto podmínek může mít zásadní vliv na výstupy systému a jeho průběh. Tento jev se nazývá motýlí efekt a poprvé byl popsán E. N. Lorenzem 29. prosince 1979.

Deterministický chaos je i kontroverzní pojem. Pokud ho totiž budeme chápat ve smyslu lidského života, pak by vlastně všechny činy, které vykonáme, byly předurčeny a nebyl by prostor pro svobodnou vůli. Tímto se však zabývat nebudeme.

1.2 Výskyt chaosu

Chaos můžeme pozorovat ve svém každodenním životě. Mohou to být přírodní jevy nebo systémy vytvořené člověkem. Příkladem, na kterém je nejčastěji popisován motýlí efekt, je počasí. S předpověďmi se setkáváme každý den a jsou více či méně přesné. Počasí se dá předvídat na pár týdnů dopředu, ale nedá se předpovědět dlouhodobě. Existuje příliš mnoho faktorů, které ho mohou ovlivnit.



Obr. 1 Jeden z modelů počasí

Dalším příkladem může být horkovzdušný balón. Tento se nedá řídit směrově, je unášen větrem a člověk může kontrolovat pouze výšku. Nicméně pokud budeme znát přesné podmínky, můžeme vypočítat dráhu letu, protože se musí řídit fyzikálními zákony, které jsou deterministické.

Obr. 2 Horkovzdušné balóny

Příkladem chaotického chování, které vytvořil člověk, je například loterie. Miliony lidí hádá každý den čísla, aby vyhráli. Když se na losování podíváme z pohledu deterministického chaosu, tak je jasné, že tato čísla nejsou náhodná. V bubnu, který se otáčí, je mnoho čísel a jsou vybírána strojově. Číslo, které je vybráno, ale není náhodné. V bubnu na ně působí mnoho sil jako odrazy, gravitace a rychlost. Pokud bychom všechny

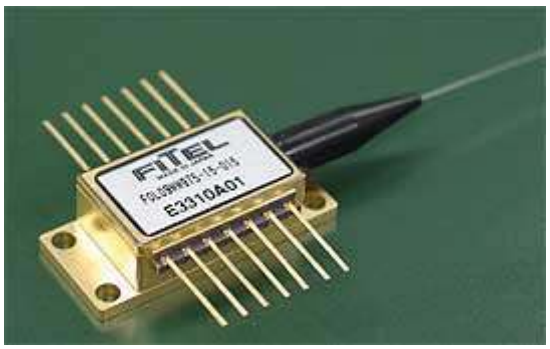
tyto síly znali, mohli bychom toto číslo určit. Je to ale extrémně složité a troufám si říct, že nemožné.

Obr. 3 Losovací zařízení

1.3 Aplikace chaosu

1.3.1 Fyzika

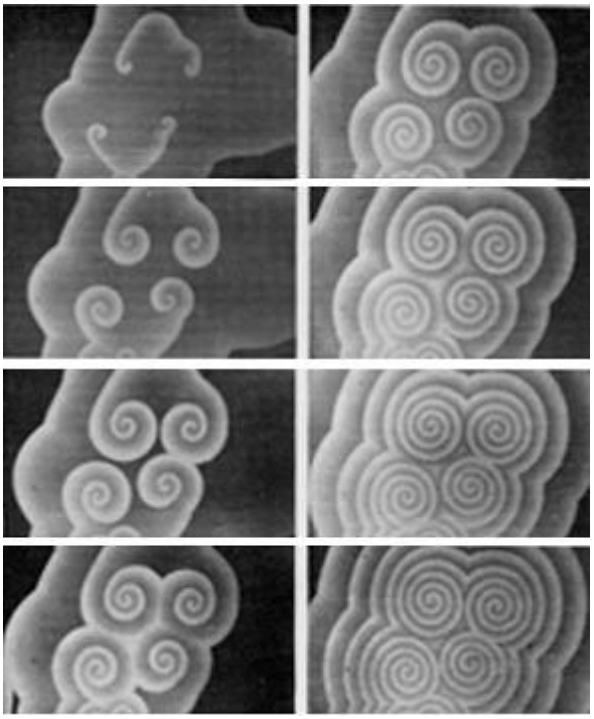
Deterministický chaos má široké uplatnění napříč všemi oblastmi. Jedno z prvních jeho použití je ve fyzice u multimodových laserů, kde bylo použitím řízení s otevřenou smyčkou dosaženo zdokonalení v síle radiačního záření. Dále se ve fyzice používá k řízení tření, turbulence a plazmatu.



Obr. 4 900nm Multimode Laser

1.3.2 Chemie

Zde se chaos používá u oscilací chemických reakcí. Jako příklady oscilací v chemických sloučeninách jsou nejčastěji uváděny zvláštní difuzní jevy nazývané Bělousovy-Žabotínského reakce. Jako první si jich všiml chemik a biofyzik Boris Bělousov, ale až Anatolu Žabotínskému se podařilo tento jev vysvětlit. Ve směsích schopných oscilačního chování probíhá souběžně několik reakcí, které jsou navzájem svázány komplikovaným řetězcem zpětných vazeb, který způsobuje zpomalení výsledné reakce a následnou změnu chování této směsi. Mezi chemickými reakcemi můžeme najít takové, při kterých třeba barva směsi pravidelně osciluje mezi několika stavy. Jiné chemické reakce zase velmi připomínají procesy v živých systémech. Kromě barevných oscilací se při reakci mohou vyskytovat i další pravidelné vzory, různé barvy mohou dokonce vytvářet zvláštní geometrické struktury, které jsou velmi podobné vzorům generovaným fraktální geometrií. [1]



Obr. 5 Chemické reakce

1.3.3 Lékařství

Život sám o sobě je známkou jakési nepravidelnosti. Živý tvor se musí neustále přizpůsobovat nově vznikajícím situacím a nemůže zůstávat stabilní. Stabilita v životě znamená smrt.

V lékařství se teorie chaosu vyskytuje hlavně při léčbě mozkových onemocnění a onemocnění srdce. Normální mozková aktivita je obvykle chaotická a mozková aktivita, která je v určitém pořádku, může být příčinnou nemocí jako je epilepsie. Těchto poznatků je možno využít při léčení chorob. Dále se dohaduje nad tím, že příliš mnoho periodicity v tlukotu srdce může indikovat nemoc. Při léčbě srdce se nyní třeba EKG zkoumá prostředky fraktálové geometrie.

1.3.4 Biologie

Chaotické chování můžeme nalézt například u pohybu hejna malých rybek. Pohyb každé jednotlivé rybky není nutné popisovat samostatně, protože každá rybka se řídí třemi jednoduchými lokálními pravidly: soudržností hejna, zařazením a oddělením.[2]

Dalším takovým příkladem může být kolonie bakterií. Každá část při zvětšení vypadá podobně jako celek. Kolonie baktérií je příkladem náhodného fraktálu.[2]

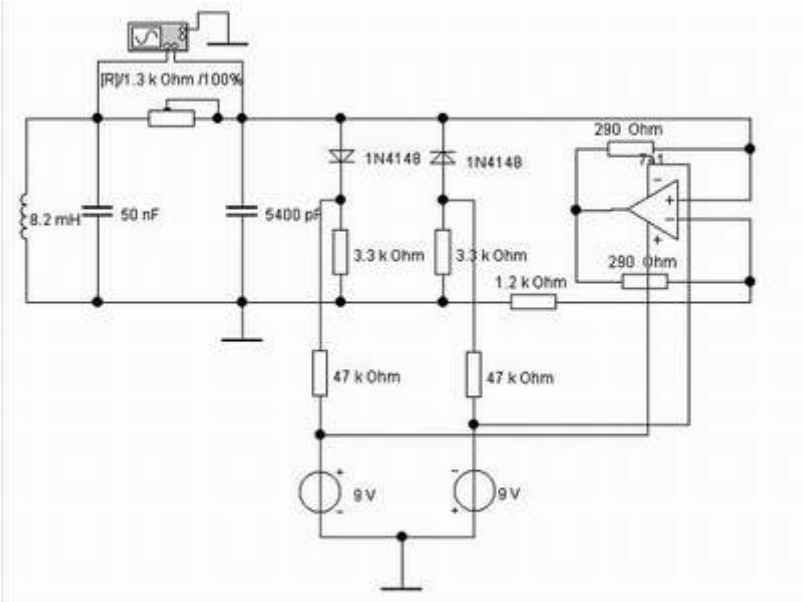
Dále se používá pro modelování biologických systémů jako je růst populace nebo epidemie.

1.3.5 Mechanické systémy

Jednoduché kyvadlo se skládá z malého těžkého předmětu, připevněného na konec lehké tyčky. Pro malé kmity (bez existence tření) se kyvadlo chová jako harmonický oscilátor. Perioda tohoto pohybu je úměrná druhé mocnině délky kyvadla. Pro velké kmity je pohyb kyvadla sice ještě periodický, ale již neplatí jednoduchý vztah. Pro velké kmity jsou rovnice pohybu kyvadla nelineární na rozdíl od lineárních rovnic pro malé oscilace. Protože rovnice pro velké kmity jsou nelineární, nelze pohyb kyvadla předpovídat. Dvojité kyvadlo se skládá ze dvou jednoduchých kyvadel, kdy jedno kyvadlo je připojeno na konec druhého kyvadla. Rovnice pohybu dvojitého kyvadla pro velké kmity jsou nelineární, ale pohyb je zcela nepravidelný a velmi citlivý vůči počátečním podmínkám. Tento druh chování je hlavním příznakem chaosu.[2]

1.3.6 Elektronické obvody

Často se s chaosem můžeme setkat v elektronických obvodech, kde ke vzniku chaosu stačí jen pár součástek. Příkladem může být Chuův obvod. Jedná se o dva rezonanční obvody s tím, že první z nich je klasický paralelní LC oscilátor a druhý je RC oscilátor s nelineárním odporem, mezi nimiž je vodivost G (G=1/R), což je řídicí parametr tohoto obvodu.



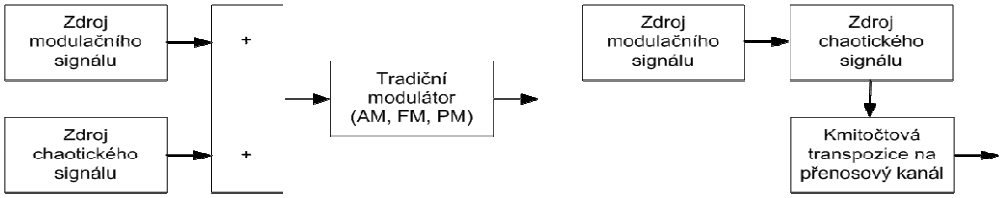
Obr. 6 Chuův obvod

1.3.7 Komunikační systémy

Zde se chaos využívá především ke skrytí signálu. Signál se namoduluje na chaotickou složku a přijímač ji odstraní. To má výhodu v tom, že když někdo zachytí tento signál, uvidí jen šumový, chaotický signál, ze kterého nebude moci přečíst informaci. Takové signály jsou neperiodické, amplitudově omezené, se spojitým spektrem, mohou být kmitočtové i velmi širokopásmové. Chaotické signály mají nízkou míru korelace, lze je využívat pro systémy s mnohonásobným přístupem. Vkládání informace do chaotických systémů můžeme několika způsoby.

U chaotického maskování je přenášený signál sloučen s chaotickým (zamaskován) a výsledný signál je přiveden do klasických tradičních modulátorů**.**

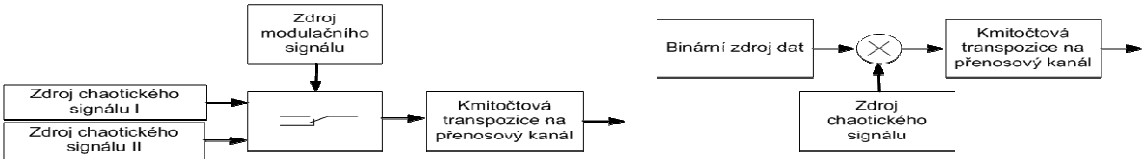
U přímé chaotické modulace je přenášený signál tvořen přímo jedním ze vstupů chaotického generátoru nebo moduluje jeden z jeho parametrů.



Obr. 7 Maskování a přímá modulace

Klíčování chaotických generátorů se nazývá metoda, kdy modulační signál slouží k přepínání různých chaotických generátorů.

Když je modulační binární signál násoben chaotickou sekvencí o vyšší čipové rychlosti (principiálně stejné jako DS-CDMA) tak se jedná o přímé rozprostření spektra chaotickou posloupností.



Obr. 8 Klíčování a rozprostření spektra

1.3.8 Informatika

Největší uplatnění má chaos v informatice a to v podobě fraktální geometrie a fraktálů v počítačové grafice. Fraktál je v podstatě nekonečně členitý útvar či geometrický objekt popisovaný nelineárními rovnicemi, který po rozdělení na menší části vykazuje tvarovou a funkční podobnost těchto jednotlivých částí s prvotním objektem. Tyto složité fraktální objekty jsou přibližně popisné pouze nelineárními rovnicemi, na rozdíl od jednoduchých pravidelných objektů, které popisuje klasická euklidovská geometrie. Základním principem v popisu fraktálu je takzvaná soběpodobnost (self similarity – invariance vůči změně měřítka), která vyjadřuje základní myšlenku, že objekt stále vypadá stejně a to ať se na něj díváme v jakémkoliv zvětšení.

Počítačová grafika se spolu s výkonem počítačů velmi rychle vyvíjí a tak je potřebné objevovat nové postupy modelování přírodních objektů, které jsou velmi složité.

2 JEDNO-DIMENZIONÁLNÍ MAPY

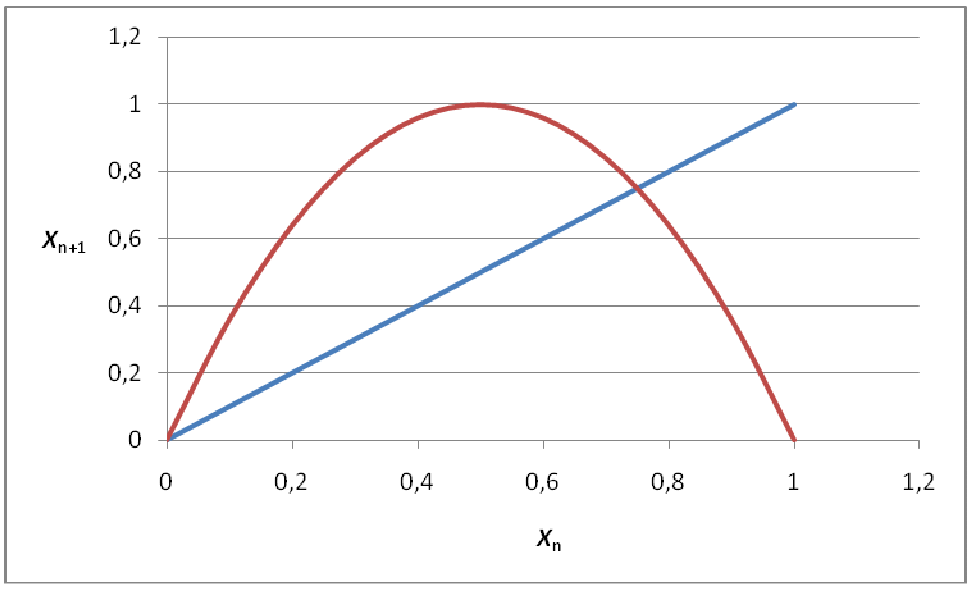
2.1 Logistická mapa

Kdykoliv narazíme na fenomén jako je chaos, který nastává při mnoha rozdílných příležitostech, je užitečné najít a studovat nejjednodušší systém kde se tento fenomén projevuje. Logistická mapa je nejjednodušší matematický chaotický systém. Obsahuje pouze jednu proměnnou a jeden řídící parametr. Přesné řešení je možné najít za použití algebry a může být graficky znázorněno. Obsahuje mnoho aspektů mnohem složitějších chaotických systémů, a proto slouží jako vzor.

Logistická rovnice (Rov. 1) se nejčastěji používá k modelování růstu populace. O parametru X přemýšlíme jako o velikosti populace od 0-1 a parametr A je mírou růstu populace. Rovnici můžeme demonstrovat na příkladu brouků, kteří každý rok nakladou vejce a pak zemřou. Příští rok se vejce vylíhnou a proces se opakuje. Jak se zvětšuje množství brouků, začne ubývat potrava a někteří zemřou dříve, než nakladou vejce. Toto řeší část rovnice $1 - X_n$, která redukuje růst populace, s tím jak se zvětšuje její velikost.

$$X_{n+1} = AX_n(1 - X_n) \tag{1}$$

Graf této rovnice se nazývá logistická křivka nebo logistická funkce a je to parabola jak je vidět na Obr. 9.

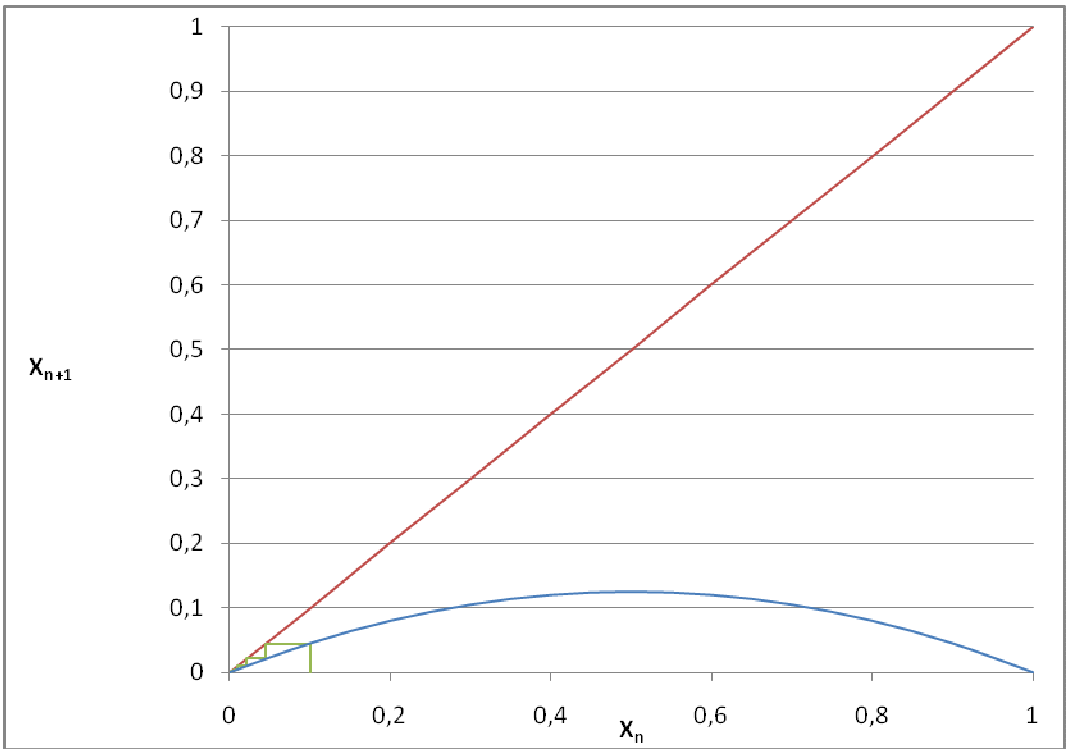


Obr. 9 Logistická mapa s A=4

Na obrázku je vidět také 45° křivka jejíž průsečíky s parabolou jsou hodnoty *X,* které se nemění v čase, takzvané pevné body. Je zajímavé sledovat chování logistické mapy v závislosti na její vstupní hodnotě, protože hlavní rysy jsou běžné pro mnoho chaotických systémů.

2.1.1 Případ 0<A<1

Parabola s A<1 může mít průsečík s 45° křivkou jen v jednom kladném bodě a tudíž má jen jeden fixní bod v 0. Všechny vstupní hodnoty z intervalu (0,1) jsou přitahovány do tohoto bodu jak je vidět na CobWeb diagramu který je na Obr. 10. CobWeb diagram bude popsán později.



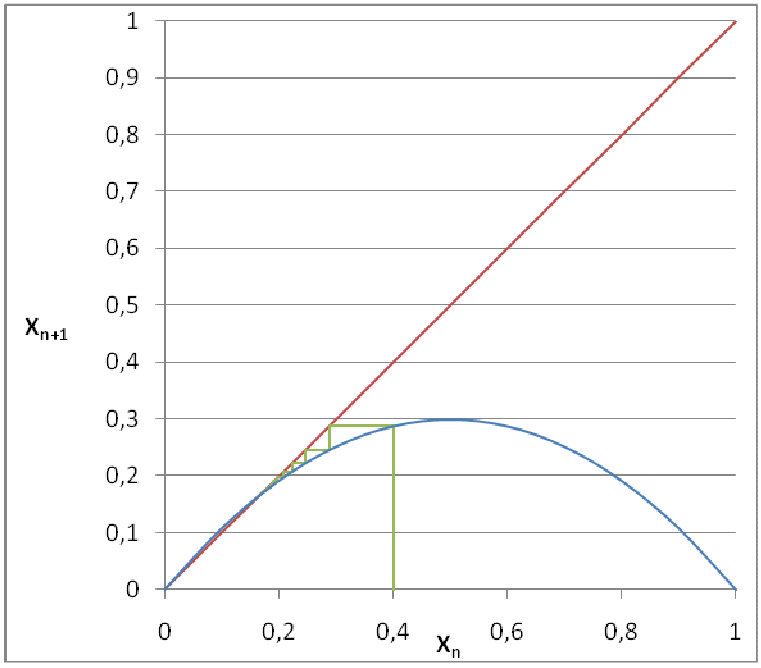
Obr. 10 CobWeb diagram pro A=0,5 a X_0=0,1

2.1.2 Případ 1<A<3

Logistická mapa s A>1 vytvoří nový atraktor v bodu

$$X^* = 1 - 1/A \tag{2}$$

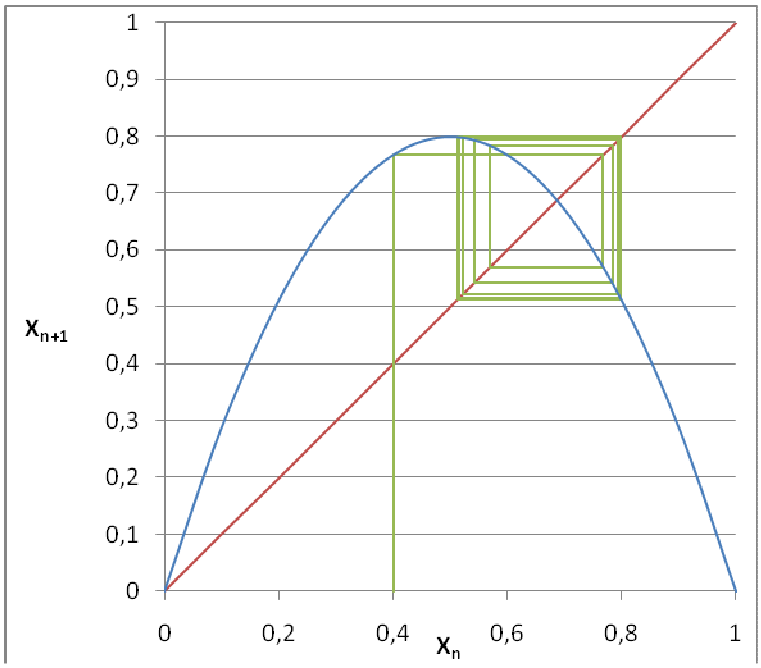
Všechny vstupní hodnoty budou přitahovány k tomuto bodu a nakonec se v něm ustálí, jak je vidět na Obr. 11. Tomuto stavu se říká period-1 cycle nebo také 1-cycle.



Obr. 11 CobWeb diagram pro A=1,2 a X_0=0,4

2.1.3 Případ 3<A<3,44948

V tomto případě se vytvoří stálý bod podle rovnice (2), ale místo toho aby se v něm hodnota X po několika iteracích ustálila, tak se od něj vzdaluje, až se ustálí na dvou hodnotách, mezi kterými osciluje. Toto je příklad 2-cycle.



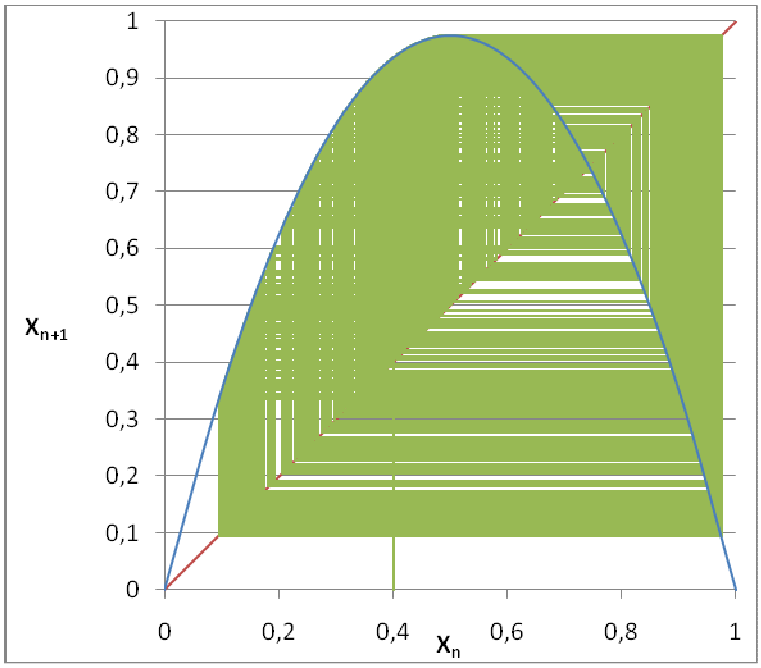
Obr. 12 CobWeb diagram pro A=3,2 a X_0=0,4

2.1.4 Případ 3,44948<A<3,56994

Pro tyto hodnoty platí stejná pravidla jako pro předchozí případ s tím rozdílem, že čím větší je A, tím se periody zdvojují. Pro hodnotu A=3,449490 je to 4-cycle a tak dále. Jak se periody zdvojují, postupně se přibližují až do akumulačního bodu. V tomto bodě se perioda stává nekonečná a počet hodnot X je také nekonečný.

2.1.5 Případ 3,56994<A≤4

Když je A zvětšeno za akumulační bod, nastává chaos. Už nejdou vidět žádné oscilace a malou změnou v počáteční hodnotě dostaneme mnoho rozdílných výsledků.



Obr. 13 CobWeb diagram pro A=3,9 a X_0=0,4

2.1.6 Případ A>4

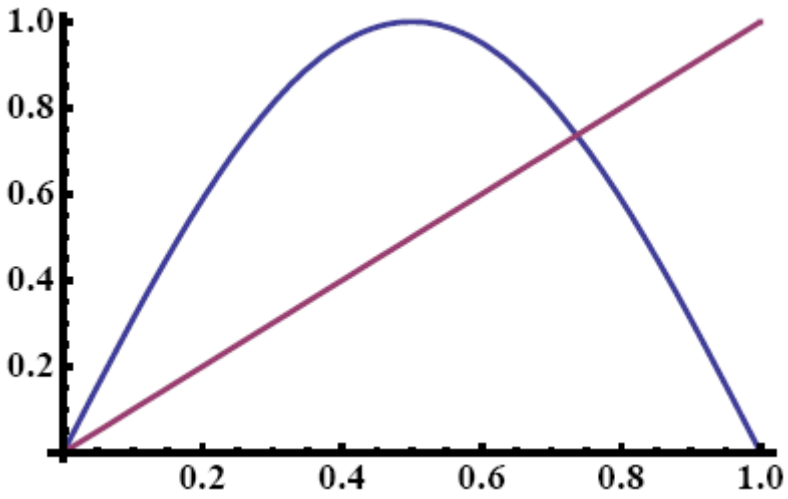
V tomto případě vrchol paraboly přesáhne hodnotu 1, tedy většina počátečních hodnot má iterace, které překročí jedničku.

2.2 Sinová mapa

Sinová mapa se řídí podle vztahu:

$$X_{n+1} = A \sin \pi X_n \tag{3}$$

Je velmi podobná logistické mapě a má skoro identický průběh. Navzdory podobnostem má však odlišnosti. Její Lyapunovský exponent je o půl procenta menší, bifurkace se objevují dříve a mezery mezi periodickými okny jsou menší než u logistické mapy.



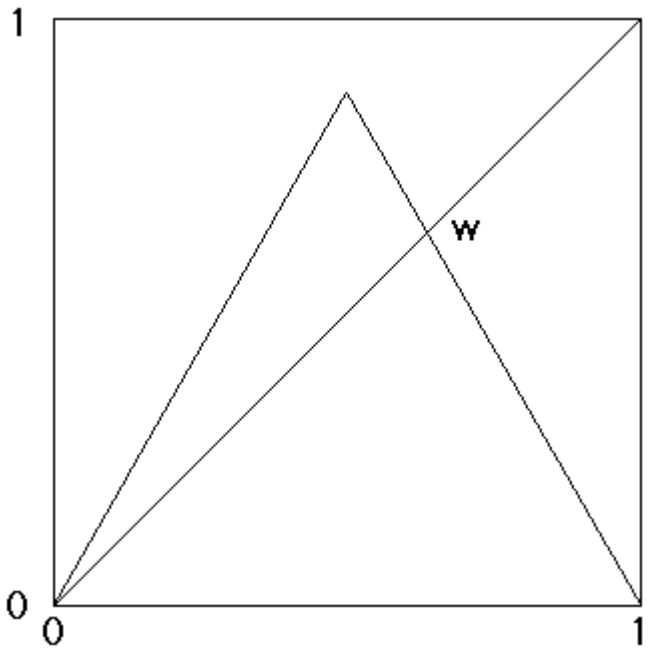
Obr. 14 Sinová mapa

2.3 Tent mapa

Jednodušší než logistická mapa je tent mapa. Pojmenovaná je tak proto, že svým tvarem připomíná stan. Její rovnice je:

$$X_{n+1} = A\min(X_n, 1 - X_n) \tag{4}$$

Je po částech lineární, protože její graf se skládá ze dvou přímek, které se protínají v bodě X_n=0,5.



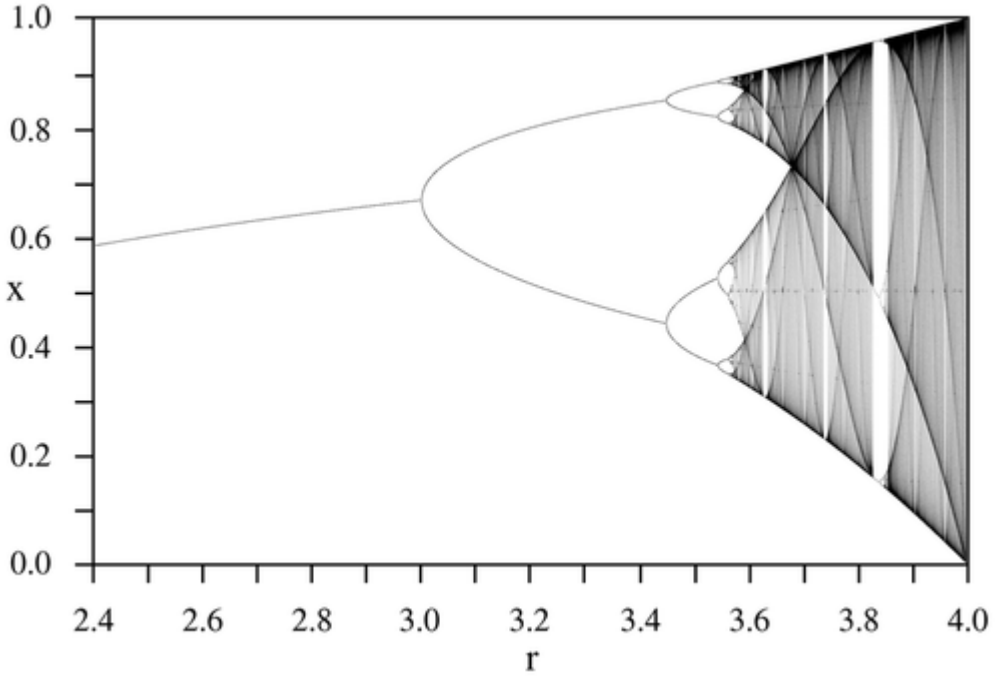
Obr. 15 Tent mapa

2.4 CobWeb diagram

Je to jednoduchý grafický způsob jak zkoumat změny parametru X, když se přibližuje k pevnému bodu. Způsob jeho vykreslení je jednoduchý. Začíná se v počáteční hodnotě X_0 na horizontální ose. Nakreslíme vertikální přímku k parabole a tím dostaneme X_1. Pak nakreslíme horizontální přímku k 45° přímce a znovu vertikální přímku k parabole. Tím získáme X_2. Toto můžeme opakovat, dokud potřebujeme.

2.5 Bifurkace

Bifurkace je označení pro bod zvratu na dějové linii, kdy v důsledku nerovnováhy negativních a pozitivních zpětných vazeb dojde k rozdělení původní trajektorie v několik nových struktur, které se navzájem liší. Bifurkační diagram je způsob, pomocí kterého můžeme znázornit chování logistické rovnice. Na bifurkačním diagramu pro logistickou rovnici Obr. 16 je dobře vidět její chování tak, jak je popsáno výše. Až do bodu r=3 je systém ustálen v jednom bodě a pak se situace změní a začne periodicky nabývat dvou hodnot.



Obr. 16 Bifurkační diagram

2.6 Lyapunovy exponenty

Dynamický systém s kladným Lyapunovým exponentem je chaotický a jeho hodnota udává, kdy je ztracena předvídatelnost. Systém má tolik Lyapunových exponentů kolik má rozměrů, ale nejdůležitější je obvykle ten největší. Lyapunův exponent si ukážeme na jednoduchém příkladu jednodimenzionální mapy jako je logistická mapa. Představme si dva blízké počáteční body v X_0 a $X_0+\Delta X_0$. Po jedné iteraci budou body odděleny podle rovnice (5).

$$\Delta X_1 = f(X_0 + \Delta X_0) - f(X_0) \cong \Delta X_0 f'(X_0)$$

Kde $f' = df / dX$. Teď definujeme Lokální Lyapunův exponent λ v X_0.

$$\lambda = \ln\left|\Delta X_1 / \Delta X_0\right| \cong \ln\left|f(X_0)\right| \tag{6}$$

Hodnota $\left|\Delta X_1 / \Delta X_0\right|$ je lokální Lyapunovo číslo. Absolutní hodnota zajišťuje, že logaritmus (Lyapunův exponent) je reálné číslo. Poznatky z toho, jak se lokální Lyapunovy exponenty od sebe liší, nám umožňuje identifikovat místa, kde jsou atraktory s dobrou a špatnou předvídatelností. K získání globálního Lyapunova exponentu (7) musíme pro rovnici (6) provést mnoho iterací.

$$\lambda = \lim_{N\to\infty} \frac{1}{N} \sum_{n=0}^{N-1} \ln\left|f'(X_N)\right| \tag{7}$$

Globální Lyapunův exponent určuje průměrnou exponenciální velikost separace mezi dvěma blízkými počátečními podmínkami. Pozitivní hodnota značí chaos a negativní hodnota značí, že systém má jeden fixní bod nebo periodický cyklus.

3 KRYPTOLOGIE

3.1 Kryptografický systém

Velký růst elektronické komunikace znamená, že otázky týkající se zabezpečení informací nabývají na významu. Zprávy vyměňované přes celosvětově přístupné sítě musí být udržovány důvěryhodné a chráněné proti manipulaci. Elektronické obchodování vyžaduje digitální podpisy a zabezpečené platební protokoly. Moderní kryptografie přináší řešení pro všechny tyto problémy.

Kryptografie je věda o zachovávání tajemství tajemstvími. [4]

Kryptografie má mnoho bezpečnostních cílů jako jsou důvěrnost dat, integrita dat, autentizace entit, nepopiratelnost a řízení přístupu. Kryptografický systém je matematická metoda, zajišťující některou informačně bezpečnostní službu. Šifrovací algoritmus je znám a jeho proces závisí na parametru, kterému se říká klíč. Po zašifrování zprávy se tato zpráva stává neinterpretovatelná pro člověka, který nezná metodu a klíč, pomocí něhož byla zašifrována. Obnovení zprávy do původní podoby se říká dešifrování. Šifrovací algoritmy byly vytvořeny proto, aby byl obsah zpráv přístupný pouze tomu, komu je určen. Z hlediska použití klíče ke zpracování otevřeného textu rozeznáváme dva základní druhy šifer a to blokové šifry a proudové šifry. Blokové šifry šifrují najednou bloky (řetězce) znaků a používají stejnou šifrovací funkci e_k kde k je šifrovací klíč. Naopak proudové šifry šifrují každý znak abecedy otevřeného textu zvlášť a z klíče k vygenerují posloupnost klíčů a poté šifrují jednotlivé znaky otevřeného textu za pomoci různých šifrovacích transformací. Mezi nejčastěji používané proudové šifry patří RC4, FISH, Helix, SEAL nebo WAKE. Mezi blokové šifry patří algoritmy DES, AES, IDEA a další [7,8,9].

Kryptografický systém se může hodnotit podle jeho rezistence proti neoprávněnému dešifrování. Dešifrování se věnuje kryptoanalýza a jedná se vlastně o proces transformace šifrované informace do původního tvaru srozumitelného pro kohokoliv. Kryptoanalytické metody (typy útoků na šifru) můžeme rozdělit do čtyř skupin podle přístupu k informacím. Nejobtížnější metoda je Ciphertext Only Attack, kde není znám plaintext. K výsledku lze dospět na základě rozborů pravidelností v textu šifry. Útok, kdy je znám původní text a jeho šifra, se nazývá Known Plaintext Attack. Rozborem lze odvodit klíč a šifrovací algoritmus. Chosen Plaintext Attack se nazývá metoda, kdy jsi lze zvolit vstupní text a získat jeho šifru. Vhodným výběrem tohoto textu mohou být objevena slabá místa

šifrovače. U metody Chosen Ciphertext si útočník může zvolit různé segmenty zašifrované zprávy a následně získat příslušné segmenty původní zprávy[10].

O kryptografickém systému můžeme říct, že je bezpečný, jestliže jeho prolomení je s použitím nejefektivnějších známých útoků natolik složité, že převyšuje výpočetní možnosti a zdroje protivníka. Musíme ale brát v úvahu rychlý vývoj techniky, kdy dnes bezpečná šifra může být prolomena za několik let.

3.2 Šifrování obrazu

Šifrování obrazu je odlišné od šifrování textu. I když můžeme použít tradiční kryptosystémy k šifrování obrazu tak, není to dobrá volba ze dvou důvodů. Zaprvé, velikost obrazu je téměř vždy mnohem větší než velikost textu, proto tradiční kryptosystémy potřebují více času k zašifrování dat. Další problém je, že dešifrovaný text musí být vždy stejný jako originální text. Nicméně tento požadavek u obrazu není vždy nutný. K vzhledem k lidskému vnímání je dešifrovaný obraz, který obsahuje malé množství zkreslení, obvykle akceptovatelný.

3.3 Deterministický chaos v kryptografii

Využití deterministického chaosu v kryptografii je velmi výhodné, protože oba tyto systémy jsou si podobné. Chaotické a kryptografické systémy mají několik stejných vlastností: oba systémy jsou citlivé na počáteční podmínky a parametry; oba vykazují náhodné chování; kryptografické systémy pracují s daty na základě rund šifrovacího algoritmu a chaotické systémy rozptylují data přes celý prostor na základě iterací.

Chaotické systémy	**Kryptografické systémy**
Množina reálných čísel	Množina celých čísel
Iterace	Rundy
Parametry	Klíče
Citlivost na počáteční podmínky	Difúze

Tab. 1 Podobnosti a rozdíly mezi chaotickými a kryptografickými systémy

Rozdílné jsou pouze v tom, že kryptografické systémy provádí své operace na množině celých čísel, zatímco chaotické systémy pracují s reálnými čísly. Jeden z dalších rozdílů mezi těmito systémy se týká otázky bezpečnosti zašifrovaných dat. Klasický

kryptografický systém, jakým je například algoritmus RSA, má svoji bezpečnost založenou na skutečnosti, že je velmi obtížné rozložit velmi velké číslo na součin prvočísel. Z čísla $n = p \times q$ je tedy v rozumném čase prakticky nemožné zjistit činitele p a q protože není znám žádný algoritmus faktorizace, který by pracoval v polynomiálním čase vůči velikosti binárního zápisu čísla n [20]. Něco podobného u chaotických systémů neexistuje. Chybí tedy důkaz o bezpečnosti nebo jeho nedostatku u šifer založených na deterministickém chaosu.

II. PRAKTICKÁ ČÁST

4 NÁVRH KRYPTOGRAFICKÉHO SYSTÉMU

Cílem praktické části této práce je navržení jednoduchého kryptografického systému a jeho realizování v programovacím jazyce. Program umí načíst obrázek, vygenerovat dva klíče a s jejich pomocí obrázek zašifrovat i dešifrovat. Dále může průběžné výsledky ukládat.

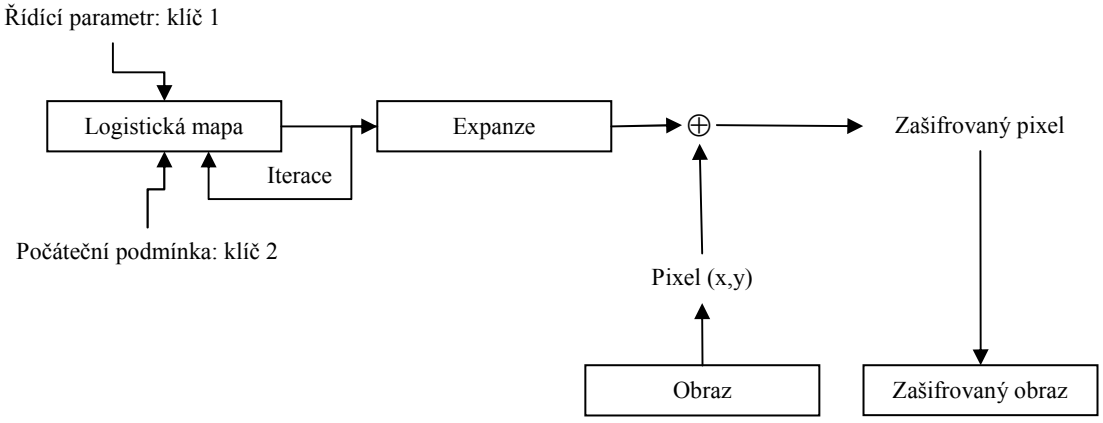
Kryptografický systém bude pracovat na základě logistické mapy. Základní myšlenkou šifrování je modifikovat každý pixel zvlášť a tak řídící parametr A a počáteční podmínka v logistické mapě zde hrají roli šifrovacích klíčů. Mějme obrázek o velikosti $W \times H$ pixelů, kde W je šířka a H je výška. Základním chaotickým systémem je zde logistická mapa.

$$X_{n+1} = AX_n(1 - X_n) \tag{8}$$

Počáteční podmínka logistické mapy X_0 a řídící parametr A zde hrají roli šifrovacích klíčů. Logistická mapa na základě náhodně generovaných klíčů chaoticky vygeneruje hodnotu z intervalu (0,1). Tato hodnota se procesem, který nazýváme expanze, převede do rozsahu (0,256). Celý proces šifrování lze zapsat jako

$$C_n = \exp and(X_n) \oplus P_n \tag{9}$$

Kde expand je funkce pro expanzi výstupu logistické mapy, P_n je n-tý pixel v obraze a C_n je příslušný zašifrovaný pixel, $n \in (0, W \times H - 1)$. Je nutné říct, že každý pixel je interpretován pomocí souřadnic (x, y) a na každý jednotlivý pixel je aplikována operace XOR s hodnotou kterou jsme dostali po expanzi. Tímto způsobem získáme zašifrovaný pixel. Tento proces je proveden pro každý pixel. Blokové schéma je uvedeno na obr. 17.



Obr. 17 Blokové schéma systému

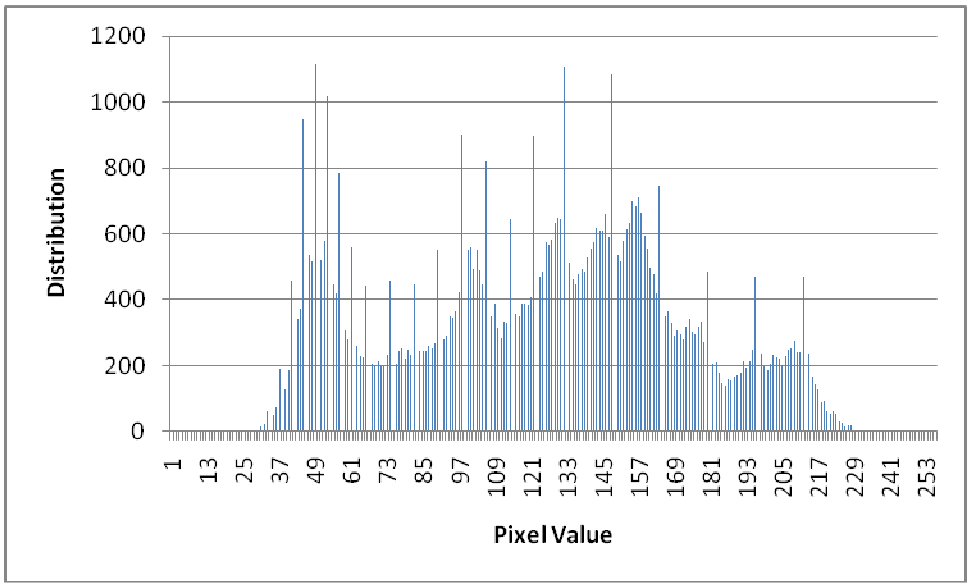
5 ANALÝZA BEZPEČNOSTI

Každý algoritmus pro šifrování by měl splňovat bezpečnostní podmínky zmíněné v [12,13]. Tato kapitola analyzuje zabezpečení zašifrovaných obrazů.

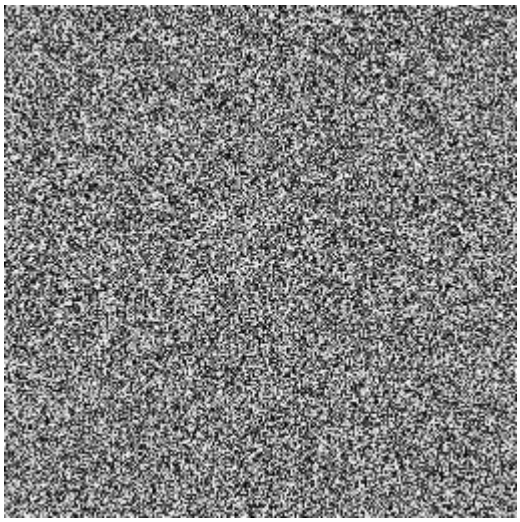
5.1 Distribuce pixelů

Navržený šifrovací algoritmus byl experimentálně vyzkoušen na obrázku „Lena“ o velikosti 256x256 pixelů. Obr. 19 zobrazuje původní obraz a obr. 20 jeho histogram, který reprezentuje distribuci pixelů v tomto obraze. Obr. 21 ukazuje již zašifrovaný obraz a obr. 22 jeho histogram. Je vidět, že šifrovací proces zajistil, že zašifrovaný obraz je zašuměný a nečitelný. Histogram znázorňuje, že rozložení pixelů je téměř rovnoměrné. Z rovnoměrné distribuce pixelů můžeme usoudit, že zašifrovaný obraz neobsahuje žádnou statistickou podobnost k původnímu obrazu. Tento aspekt je důkazem rezistence šifry proti útoku typu known-plaintext.

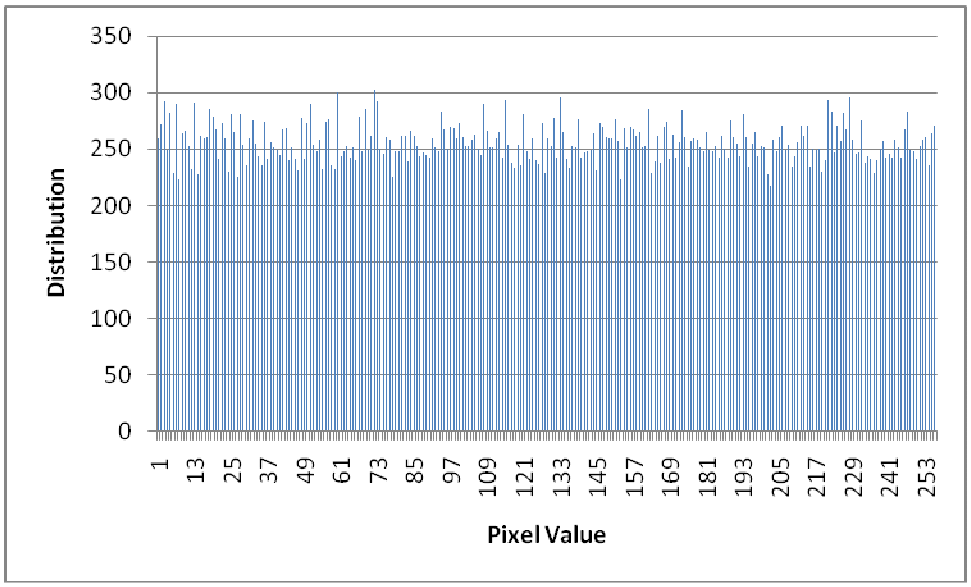
Obr. 18 Původní obrázek „Lena“



Obr. 19 Histogram původního obrázku „Lena“



Obr. 20 Zašifrovaný obraz



Obr. 21 Histogram zašifrovaného obrazu

5.2 Informační entropie

Dosažení nečitelnosti a nepředvídatelnosti jsou hlavními činnostmi šifrování obrazu. Toto může být ukázáno pomocí informační entropie. Entropii můžeme pochopit také jako míru neurčitosti systému.

Entropie *H* zdroje zpráv *S* může být vyjádřena jako (8)

$$H(S) = \sum_{i=1}^{N} P(s_i) \cdot \log \frac{1}{P(s_i)} \tag{1}$$

kde $P_{(S_i)}$ reprezentuje pravděpodobnost symbolu s_i a log je binárním logaritmem o základu 2.

Pokud budou všechny hodnoty pixelů distribuovány rovnoměrně, pak bude entropie obrazu maximální. Při šifrování požadujeme, aby hodnota entropie byla co největší. Tab. 2 zobrazuje hodnoty entropie původních obrazů a jejich zašifrovaných forem. Tyto hodnoty jsou velmi blízké maximální hodnotě entropie. Dokonce i obraz obsahující pouze pixely černé barvy, který má nulovou entropii, dosahoval po šifrovacím procesu k maximální hodnotě entropie.

Obraz	Entropie původního obrazu	Entropie zašifrovaného obrazu
Šedá škála	8	7,996
Černá barva	0	7,996
Lena	7,201	7,997

Tab. 2 Tabulka entropie

5.3 Křížová korelace obrázků a přilehlých pixelů

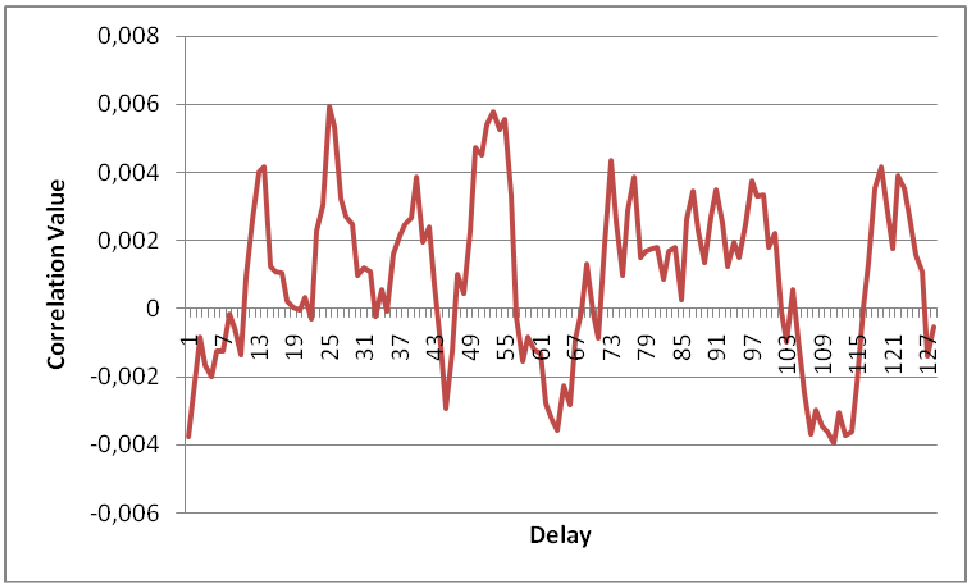
Křížová korelace je standardní metoda pro odhad, do jaké míry jsou dvě série korelované. Uvažujme dvě série x_i a y_i kde $i = 1,2,.....N$ a $E_{(x)}$ a $E_{(y)}$ jsou prostředkem k příslušné sérii podle (9).

$$E(x) = \frac{1}{N} \cdot \sum_{i=1}^{N} x_i \tag{9}$$

Křížová korelace r ve zpoždění d je definována jako

$$r(d) = \frac{\sum_i (x_i - E(x)) \cdot (y_{i-d} - E(y))}{\sqrt{\sum_i (x_i - E(x))^2} \cdot \sqrt{\sum_i (y_{i-d} - E(y))^2}} \tag{10}$$

Křížová korelace může být také použita jako měřítko podobnosti dvou obrazů. Na obr. 23 vidíme křížové korelace původního obrázku a zašifrovaného obrázku. Je zřejmé, že hodnota korelace nepřesahuje hodnotu 0,006. To znamená velmi malou korelaci a velmi malou podobnost obrázků a jejich pixelů.



Obr. 22 Křížové korelace původního obrázku a zašifrovaného obrázku

Jedním z požadavků na účinný proces šifrování obrazů je generování šifrovaných obrazů s nízkou hodnotu korelace sousedních pixelů. Korelace mezi dvěma horizontálně, vertikálně a diagonálně sousedními pixely původního obrazu a zašifrovaného obrazu byla analyzována. Pro každý vybraný pár sousedních pixelů původního obrazu byl proveden výpočet koeficientu korelace podle rovnice (10). Stejně se postupovalo u zašifrovaného obrazu. Tyto korelační koeficienty v různých směrech sousedních pixelů jsou uvedeny v tabulce 3.

Směry sousedních pixelů	Původní obraz	Zašifrovaný obraz
Horizontální	0,942906678295296	-0,00311647985137356
Vertikální	0,971151483222909	0,00377788674457351
Diagonální	0,920257791832602	0,00169137957980492

Tab. 3 Korelační koeficienty originálního a zašifrovaného obrazu

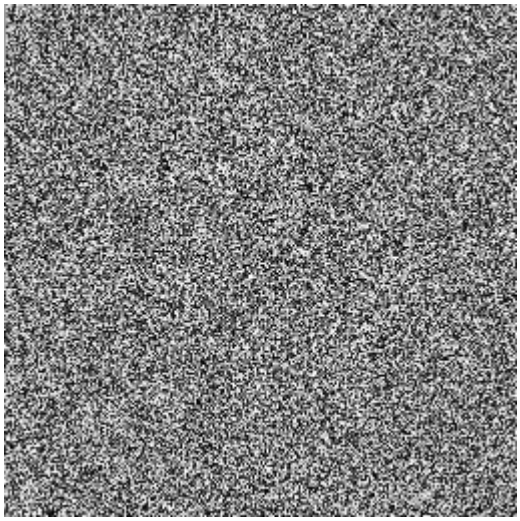
5.4 Citlivost klíčů

Snažíme se dosáhnout toho, aby minimální změna v klíči měla za následek zcela odlišný výsledek. Pro náš program náhodně generujeme dva klíče. Pro experiment použijeme dvě sady klíčů:

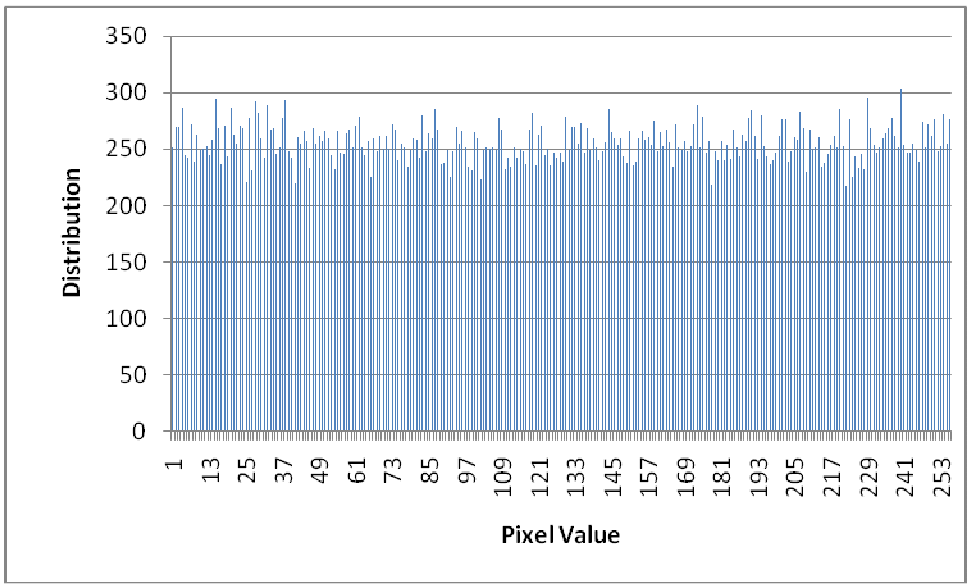
$$a = 0{,}28579554859818\,,\ b = 3{,}99545673159671 \tag{11}$$

$$a = 0{,}28579554859817\,,\ b = 3{,}99545673159671 \tag{12}$$

Sady klíčů (11) a (12) se od sebe liší jen velmi minimálně. Test citlivosti klíčů je založen na šifrování obrazu pomocí sady klíčů (11) a poté na dešifrování obrazu pomocí sady (12). Na obr. 23 vidíme obraz dešifrovaný špatnou sadou klíčů a na obr. 25 vidíme jeho distribuci pitelů. Jak je vidět obrázek nemůže být dešifrován ani při minimální změně klíčů.



Obr. 23 Obrázek dešifrovaný špatnou sadou klíčů



Obr. 24 Distribuce pixelů špatně dešifrovaného obrázku

5.5 Prostor klíčů

Kryptografický systém musí být rezistentní vůči útoku hrubou silou. To zajišťuje velký prostor klíčů, který udává kolik kombinací klíčů může daný systém mít. Maximální přesnost běžného PC procesoru je 16 desetinných míst. Počet všech kombinací jednoho klíče je tedy 10^{16}, což odpovídá přibližně prostoru klíčů o velikosti 2^{53}. V navržené šifře jsou 2 klíče. Prostor klíčů je tedy rozsáhlý 2^{106}.

6 SROVNÁNÍ S JINÝMI CHAOTICKÝMI SYSTÉMY

V této části bude představeno a srovnáno několik chaotických kryptografických systémů. V [11] jsou představeny dva druhy metod založených na vícedimenzionálních mapách. Použitím diskretizované chaotické mapy jsou pixely v obrazu přehozeny po několika operacích. Mezi každými dvěma koly je proveden difuzní proces který velmi změní distribuci pixelů. V [14] jsou představeny tři logistické mapy, které jsou použity jako proudový generátor klíčů a tento okruh vylepší lineární složitost klíčového proudu. Další studie jsou zmíněny v [15], kde se používá hyper chaotický system pro zmatení vztahu mezi původním a zašifrovaným obrazem. V [16] je představen Lorenzův systém pro generování klíčů a S-Box algebraické operace jsou popsány v [17, 18].

Pro první srovnání navrženého systému s ostatními systémy použijeme tabulku korelačních koeficientů Tab. 4. S navrženým systémem porovnáme systémy navržené v [10, 15, 19].

Směry sousedních pixelů	**Původní obraz**	**Zašifrovaný obraz**	**Zašifrovaný obraz podle [10]**	**Zašifrovaný obraz podle [15]**	**Zašifrovaný obraz podle [19]**
Horizontální	0,942906	-0,003116	0.005776	-0.014200	0.030800
Vertikální	0,971151	0,003777	0.028434	-0.007400	0.030400
Diagonální	0,920257	0,001691	0.020662	-0.018300	0.031700

Tab. 4 Srovnání korelačních koeficientů

Lze vidět, že všechny systémy můžou efektivně dekorelovat sousední pixely v obrázku. Korelační koeficienty jsou nejmenší u navrženého systému.

Dále porovnáme prostory klíčů pro různé systémy Tab. 5. Z tabulky je zřejmé, že navržený systém má nejmenší prostor klíčů a tak je z porovnávaných systémů nejnáchylnější vůči útoku hrubou silou.

Systém	**Prostor klíčů**
Navržený	2^{106}
[10]	2^{128}
[14]	2^{158}
[15]	2^{232}

Tab. 5 Prostory klíčů

ZÁVĚR

Cílem této práce bylo stručně popsat deterministický chaos, kryptografii a navrhnout a realizovat kryptografický systém. Navržená metoda pro kryptografický systém je založena na logistické mapě, což je jednodimenzionální chaotická mapa. Algoritmus šifrování pracuje na základě chaoticky vygenerované hodnotě logistickou mapou, která se následně expanduje do rozsahu 0-256 a tato hodnota se aplikuje pomocí operace XOR na každý pixel obrazu. Pro analýzu bezpečnosti navržené metody byly vytvořeny soubory s daty histogramů a soubory s daty křížové korelace. Výsledky analýzy bezpečnosti jsou uvedeny v příslušné kapitole.

Výstupem této práce je funkční program v programovacím jazyce C#, který realizuje navrženou metodu a ukládá soubory s daty.

Deterministický chaos se v posledních letech velmi rozvíjí a má velký potenciál pro využití napříč celým spektrem vědy.

ZÁVĚR V ANGLIČTINĚ

The aim of this study was to briefly describe the deterministic chaos, cryptography, and to propose and to implement a cryptographic system. The proposed method for the cryptographic system is based on the logistic map, which is one dimension chaotic map. The encryption algorithm works on the basis of value generated by chaotic logistic map, which in turn expands the range of 0-256 and this value is applied to each pixel using the XOR operation. For the security analysis of the proposed method were created files with data of histograms and cross-correlations. The results of security analysis are given in security analysis chapter.

The outcome of this work is a functional program in C #, which implements the proposed method and stores the data files.

In recent years, the deterministic chaos has highly developed and has great potential for use across the entire spectrum of science.

SEZNAM POUŽITÉ LITERATURY

[1] *Johny Long Step* [online]. 17.11.2008. Oscilace v chemických reakcích. Dostupné z WWW: <http://jlswbs.wordpress.com/2008/11/17/oscilace-v-chemickych-reakcich/>.

[2] *Johny Long Step* [online]. 2.4.2008. Příklady komplexity. Dostupné z WWW: <http://jlswbs.wordpress.com/2008/04/02/priklady-komplexity/>.

[3] Tišňovský, Pavel. *Root.cz* [online]. 16.11.2005. Fraktály v počítačové grafice. Dostupné z WWW: <http://www.root.cz/clanky/fraktaly-v-pocitacove-grafice-iv/>.

[4] Delf, Hans; Knebl, Helmut. *Introduction to cryptography : principles and applications* [online]. 2nd edition. Berlin : Springer, 2007. Dostupné z WWW: <http://www.springerlink.com/content/gm2886/?p=7d653593e3e247faa59f202fe838cf57π=1332>.

[5] Lian, S., Sun, J., Wang, Z. (2005) Security analysis of a chaos-based image encryption algorithm, Physica A, vol. 351, is. 2-4, pp. 645-661, ISSN 0378-4371

[6] Kelber, K., Schwartz, W. (2005) General Design Rules for Chaos-Based Encryption Systems, Proceedings of the NOLTA 2005, Bruges, Belgium, 2005

[7] Meneyes AJ; van Oorschot PC, Vanstone SA (1996) Handbook of Applied

Cryptography. CRC Press, Boca Raton, FL

[8] Stallings W (1999) Cryptography and Network Security: Principles and Practice.

Prentice-Hall, Upper Saddle River, NJ

[9] Stinson DR (2002) Cryprography: Theory and Practice (2nd. edn.) Chapman and

Hall/CRC, Boca Raton, FL

[10] Mao, Y., Chen, G. Chaos-Based Image Encryption. Springer-Verlag, Berlin, 2003

[11] Fridrich J (1998) Symmetric Ciphers based on two-dimensional chaotic maps. Int J

Bifurcation and Chaos 8(6): 1259-1284

[12] Lian, S., Sun, J., Wang, Z. Security analysis of a chaos-based image encryption

Algorithm. ScienceDirect, 2005.

[13] Kelber, K., Schwartz, W. General Design Rules for Chaos-Based Encryption Systems.

NOLTA 2005, Bruges, 2005.

[14] Fu, Ch., Zhang, Z., Chen, Z., Wang, X. An Improved Chaos-Based Image Encryption Scheme. ICCS 2007, Springer-Verlag, Berlin, 2007.

[15] Gao, T., Chen, Z. A new image encryption algorithm based on hyper-chaos. ScienceDirect, 2007.

[16] Fu, Ch., Zhang, Z., Cao, Y. An Improved Image Encryption Algorithm Based on Chaotic Maps. ICNC 2007.

[17] He, X., Zhu, Q., Gu, P. A New Chaos-Based Encryption Method for Color Image. Springer-Verlag, Berlin, 2006.

[18] Asim, M., Jeoti, V. Hybrid Chaotic Image Encryption Scheme based on S-box and Ciphertext Feedback. ICIAS 2007.

[19] Hossam, A., Hamdy, K., Osama, A. An Efficient Chaos-Based Feedback Stream Cipher (ECBFSC) for Image Encryption and Decryption. Informatica 31, 2007.

[20] Podoba, T., Giesl, J., Vlcek, K., GPU Benchmarks Based on Strange Attractors. CISSE SCSS 2009, International Conference on Systems, Computing Sciences and Software Engineering, University of Bridgeport, USA.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

EKG	Elektrokardiogram.
DS-CDMA	Dirty Sequence Code Division Multiple Access.
RC4	Rivest Cipher 4.
FISH	FIbonacci SHrinking.
SEAL	Software-Optimized Encryption Algorithm.
WAKE	Word Auto Key Encryption.
DES	Data Encryption Standard.
AES	Advanced Encryption Standard.
IDEA	International Data Encryption Algorithm.

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

P1: Přenosné médium CD-ROM

PŘÍLOHA P I: PŘENOSNÉ MÉDIUM CD-ROM

Přenosné médium obsahuje bakalářskou práci ve formátu pdf a program vytvořený v jazyce C#.