ZRYCHLENÍ ALGORITMU CHAOTICKÉ ŠIFRY PRO OBRAZY

Jiří Giesl
Inženýrská informatika, 2. ročník, prezenční forma studia
Školitel: prof. Ing. Karel Vlček, CSc.

Fakulta aplikované informatiky
Univerzita Tomáše Bati ve Zlíně
Nad Stráněmi 4511
760 05 Zlín
Česká republika
jgiesl@fai.utb.cz

Abstrakt. Chaotické systémy jsou velmi citlivé na počáteční podmínky a řídicí parametry. Tato vlastnost může být velmi vhodná pro kryptografické účely. Tato práce se zabývá návrhem šifry založené na chaotických mapách atraktoru Petera de Jonga. Statický obraz je převeden do vlnkové oblasti a poté jsou modifikovány příslušné vlnkové koeficienty. Hlavní účel vlnkové transformace je zredukovat výpočetní čas potřebný pro samotný proces šifrování a také dosáhnout vyšší nebo stejné úrovně bezpečnosti zašifrovaného obrazu.

Klíčová slova. šifrování obrazu, chaotické mapy, atraktor, vlnková transformace.

1 Úvod

Obraz je multimediální signál, který poskytuje nejvíce informací, protože přes 80% informace je získáno pozorováním. Z toho důvodu existuje také snaha o zabezpečení těchto informací proti neautorizovanému čtení. Mezi základní metody šifer obrazu patří permutace a modifikace pixelů. Tyto metody jsou natolik univerzální, že jsou otevřeny pro použití nejen v klasických šifrách, ale také v novějších algoritmech. Z toho důvodu je lze použít i pro algoritmy využívající teorii chaosu. Chaotické systémy jsou totiž velmi citlivé na počáteční podmínky a řídicí parametry. Dokonce minimální změna ve vstupních podmínkách takového systému může vést k jeho velkým změnám. Přitom také nelze přesně určit, jakým způsobem se bude chaotický systém chovat v delším časovém úseku. Toto všechno jsou vlastnosti, které jsou pro oblast kryptografie velmi velkou výhodou.

V posledních letech bylo vytvořeno mnoho šifer založených na chaosu. Některé z nich byly založeny na generaci šifrovacího klíče [1,2], pomocí kterého byla poté data upravena. Další algoritmy používaly dvou-dimenzionální mapy, protože obraz si lze představit jako 2D matici [3,4]. Mnoho z těchto šifer byly blokového charakteru; pouze několik z nich byly navrženy jako proudové šifry [5], které poskytují efektivní způsob pro aplikace v reálném čase.

V naší předchozí práci [6] jsme navrhli blokovou chaotickou šifru obrazu, při které zašifrované obrazy dosahovaly vysoké úrovně zabezpečení, ovšem tato bezpečnost byla na úkor výpočetního času. Pro aplikace v reálném čase je tedy tato šifra nepoužitelná. Naší snahou je tedy vytvořit takovou šifru, která by byla vhodná i pro některé náročné aplikace, jakým je například video-konference. Toho můžeme snadno dosáhnout šifrováním pouze nejdůležitějších informací v multimediálním signálu. Tato informace může být získána právě vlnkovou transformací. Pouze vybrané vlnkové koeficienty jsou poté šifrovány rozšířenou verzí chaotického systému Petera de Jonga. Ztráta informace daná výběrem vlnkových koeficientů by neměla být pro aplikace video-konference zásadní.

2 Metody

2.1 Chaos a atraktory

Teorie chaosu patří do oblasti nelineární dynamiky. Dynamické systémy mohou být považovány za chaotické, pokud nejsou předvídatelné ani opakovatelné a pokud malá odchylka v jejich vstupech způsobí odlišný vývoj jejich výstupů. Chování chaotických dynamických systémů zaujímá několik stavů, které se nazývají atraktory. Těchto atraktorů je několik typů – bod, křivka, různorodé tvary a komplikovaný útvar s fraktální strukturou, který je nazýván „podivný atraktor“ [8]. Fixní body tohoto „podivného atraktoru“ jsou lokálně nestabilní, ale globálně je celý systém stabilní. Tyto atraktory můžou být vytvořeny několika způsoby, např. kvadratickými (1) nebo trigonometrickými (2) mapami. Řídicí parametry a,b,c,d,e,f,g,h,i,j,k,l definují chování chaotického systému.

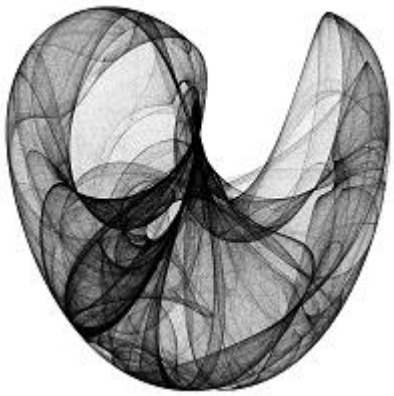
$$\begin{aligned} x_{n+1} &= a + b \cdot x_n + c \cdot x_n^{\,2} + d \cdot x_n y_n + e \cdot y_n + f \cdot y_n^{\,2} \\ y_{n+1} &= g + h \cdot x_n + i \cdot x_n^{\,2} + j \cdot x_n y_n + k \cdot y_n + l \cdot y_n^{\,2} \end{aligned} \tag{1}$$

$$\begin{aligned} x_{n+1} &= a \cdot \sin(b \cdot y_n) + c \cdot \cos(d \cdot x_n) \\ y_{n+1} &= e \cdot \sin(f \cdot y_n) + g \cdot \cos(h \cdot x_n) \end{aligned} \tag{2}$$

Nezbytnou podmínkou chaotického chování „podivného atraktoru“ je, aby Ljapunovský exponent aspoň jedné mapy byl kladný. Kladný exponent koresponduje s expanzí systému, záporný s jeho kontrakcí. Uvažujme $x_{n+1} = f(x)$. Ljapunovský exponent Λ je pak určen jako (3).

$$\Lambda = \lim_{n=>\infty} \left(\frac{1}{n} \cdot \sum_{i=0}^{n-1} \ln \left| f'(x_i) \right| \right) \tag{3}$$

Jeden z „podivných atraktorů“ s předdefinovanými řídicími parametry je zobrazen na Obrázku 1. Jedná se o atraktor vytvořený Peterem de Jongem a tento typ atraktoru je také používán v této práci pro šifrovací účely.

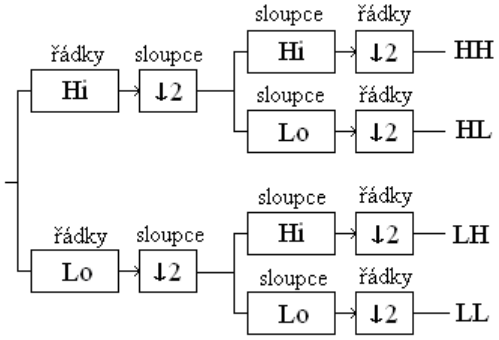


Obrázek 1: Příklad atraktoru Petera de Jonga.

2.2 Reprezentace obrazu ve vlnkové oblasti

Pro extrakci informace v různých měřítcích se používá tzv. multiresolution analýza, která se provádí pomocí vlnkové transformace. Obraz musí být zpracován bankou kvadraturně zrcadlových filtrů. Při dekompozici obrazu se vstupní signál (tedy matice obrazových dat) nechá projít bankou filtrů typu

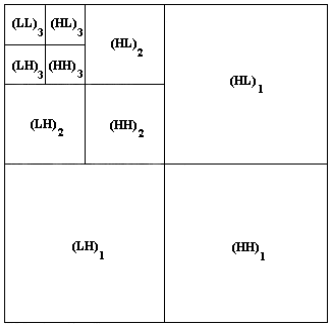
horní propust k analýze vyšších frekvencí a bankou filtrů typu dolní propust k analýze nižších frekvencí. Signál se tedy dělí na aproximaci (reprezentován nižšími frekvencemi zpracovaného signálu) a detailnější informaci (reprezentován vyššími frekvencemi zpracovaného signálu). Potom následuje podvzorkování, pomocí kterého se odstraní část vzorků v signálu.



Obrázek 2: Základní struktura dyadického rozkladu obrazu

Podle schématu tedy můžeme vidět, že se nejprve transformují všechny řádky obrazu (tedy pixely ve všech řádcích). Takto zanalyzovaná data se sloupcově podvzorkují a následně se transformují sloupce těchto dat. Po řádkovém podvzorkování je proveden dyadický rozklad (dekompozici) první úrovně a ve výsledku jsou k dispozici 4 sady koeficientů: LL – aproximace obrazu, LH – detaily obrazu v horizontálním směru, HL – detaily obrazu ve vertikálním směru, HH – detaily obrazu v diagonálním směru

Pro mnoho-úrovňovou dekompozici signálu se často používá nestandardní dyadický rozklad, u kterého se vždy rekurzivně analyzuje pouze aproximační část (LL pásmo) z předchozího kroku dekompozice. Na Obrázku 3 je schématicky zobrazena dekompozice obrazu třetí úrovně, která se často používá v oblasti zpracování statických obrazů.



Obrázek 3: Dyadický rozklad obrazu do 3. úrovně

2.3 Algoritmus šifrování obrazu

Uvažujme matici P, která obsahuje hodnoty pixelů $p_{i,j} \in P$ daného obrázku, kde $i \in (0,1,2,...W)$ a $j \in (0,1,2,...H)$, W a H určují šířku a výšku matice P (obrazu). Matice P je dyadicky rozložena a převedena do vlnkové oblasti. Výsledná matice C obsahuje vlnkové koeficienty $c_{i,j}$, které jsou vstupními daty pro šifrovací algoritmus.

Pro účely šifrování je zde použit atraktor Petera de Jonga. Tento typ chaotického systému je složen ze dvou map, které mohou být jednoduše použity pro permutaci koeficientů. Tato permutace ovšem není z hlediska bezpečnosti dostatečná, protože může být šifrovací proces jednoduše odhalen např. systémem ergodických fuzzy matic [7]. Z toho důvodu musí být do šifrování zakomponována i

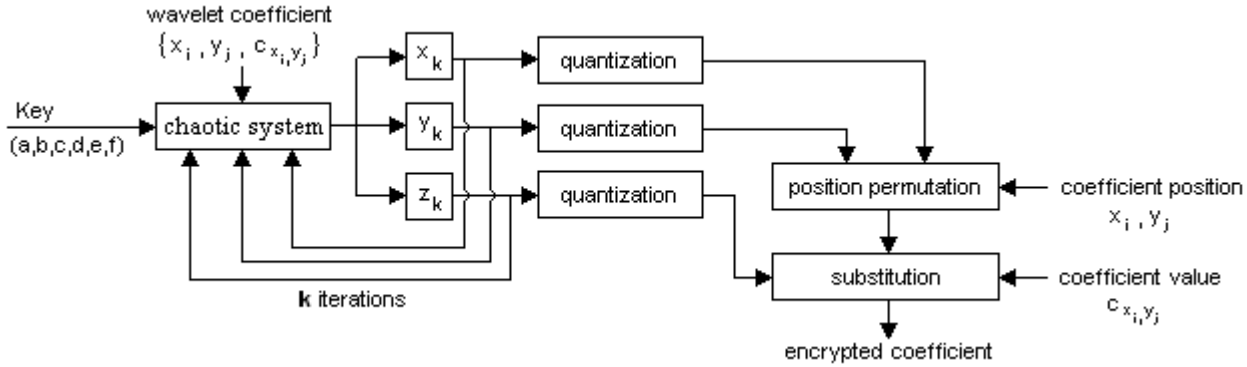
modifikace vlnkových koeficientů. Toto zlepšení spočívá v rozšíření chaotického systému v trojrozměrnou verzi (4). Třetí mapa může být použita pro účely modifikace.

$$\begin{aligned} x_{n+1} &= \sin(a \cdot y_n) - \cos(b \cdot x_n) \\ y_{n+1} &= \sin(c \cdot y_n) - \cos(d \cdot x_n) \\ z_{n+1} &= \sin(e \cdot z_n) - \cos(f \cdot y_n) \end{aligned} \tag{4}$$

Základní myšlenkou šifrování je zakryptovat každý vlnkový koeficient zvlášť. Řídicí parametry a, b, c, d, e, f chaotického systému (4) zde hrají roli šifrovacích klíčů. Definujme c_A jako vlnkový koeficient na souřadnicích (x_i, y_j). Pozice x_i, y_j a hodnota c_A jsou vloženy do (4) jako počáteční podmínky příslušné mapy. Výsledné hodnoty x_k, y_k a z_k jsou k dispozici po k-té iteraci chaotického systému. Druhý vlnkový koeficient c_B musí být poté nalezen na souřadnicích (x_k, y_k). Koeficient c_B je pak XORován s hodnotou z_k a tato upravená hodnota je prohozena s koeficientem c_A podle (5). Tímto způsobem získáme zašifrovaný koeficient.

$$c_A \leftrightarrow c_B \oplus z_k \tag{5}$$

Tento proces musí být proveden pro každý vlnkový koeficient v matici C a může být proveden m-krát pro zvýšení zabezpečení zašifrovaného obrazu. Obrázek 4 ukazuje jednoduchý nákres šifrovacího procesu.



Obrázek 4: Nákres šifrovacího procesu

3 Experimentální výsledky

Vlnka Daubechies 2.řádu byla použita pro dyadickou dekompozici obrazu a pouze submatice $C_0 \subset C$ s koeficienty $c_{m,n} \in C_0$, kde $m \in (0,1,2,...\frac{W}{4})$ a $n \in (0,1,2,...\frac{H}{4})$ je uvažována v následujících experimentech. Znamená to tedy, že pouze 1/16 všech koeficientů je šifrována. Přesto tato submatice obsahuje nejdůležitější koeficienty, které představují samotnou aproximaci a některé detaily zpracovávaného obrazu. Šifrovací proces je tedy zrychlen, pokud je zpracována pouze submatice C_0. Nicméně, použití pouze aproximace a zanedbání detailů má velký dopad na celkovou kvalitu rekonstruovaného obrazu. Tato ztráta informace je akceptovatelná pouze v některých aplikacích, jakým je například video konference.

Šifrovací proces popsaný výše byl odzkoušen na obrázku „Lena“ o velikosti 256x256 pixelů. Obrázek 5 ukazuje původní obrázek, distribuci jeho pixelů a vzorek vlnkové domény, která obsahuje

nejdůležitější koeficienty. Obrázek byl zašifrován pomocí klíčů (6). Tyto klíče jsou řídicími parametry chaotického systému.

$$\{a = 1.4, \mathrm{b} = -2.3, \mathrm{c} = -2.4, \mathrm{d} = -2.1, \mathrm{e} = 1.2, \mathrm{f} = 1.6\} \quad (6)$$

Zašifrovaný obrázek po rekonstrukci je ukázán na Obrázku 6. Distribuce pixelů není rovnoměrná, ale ve tvaru U, protože se bere v potaz pouze submatice C_0 a dochází zde ke ztrátě informace. Pokud bychom uvažovali celou matici C, která obsahuje všechny vlnkové koeficienty, distribuce by se velmi podobala rovnoměrnému rozložení. Rovnoměrnost je v tomto případě známka toho, že mezi původním a zašifrovaným obrazem neexistuje žádná statistická podobnost. Tvar U se objevuje u všech typů zašifrovaných obrazů. Můžeme tedy říci, tento U tvar nám dává z hlediska bezpečnosti stejnou statistickou informaci jako v případě rovnoměrného rozložení. Nejdůležitější vlnkové koeficienty jsou umístěny v nejnižším pásmu vlnkové oblasti (na prvních souřadnicích submatice C_0).

Zašifrovaný obraz byl poté dešifrován sadou klíčů (7). První řídicí parametr má minimální odchylku od prvního parametru v (6).

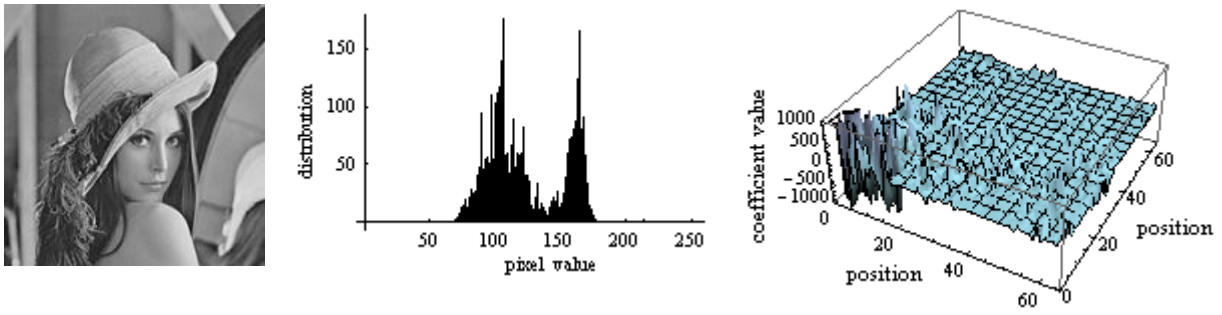
$$\{a = 1.40001, \mathrm{b} = -2.3, \mathrm{c} = -2.4, \mathrm{d} = -2.1, \mathrm{e} = 1.2, \mathrm{f} = 1.6\} \quad (7)$$

Obrázek 7 ukazuje, že i malá změna v sadě klíčů způsobí nečitelnost a nepředvídatelnost rekonstruovaného obrazu. V distribuci pixelů se opět objevuje tvar U a vlnkové koeficienty mají nyní různé hodnoty a jsou rozmístěny po celé vlnkové oblasti (submatice C_0 obsahuje různé hodnoty koeficientů na všech pozicích).

Když je obrázek dešifrován správnou sadou klíčů (6), získáme aproximaci původního obrazu. Ztráta informace je evidentní z Obrázku 8. Histogram reprezentující distribuci pixelů je trochu rozdílný oproti původnímu histogramu z Obrázku 5. Tato ztráta informace je dána zpracováním submatice C_0, která neobsahovala detaily původního obrazu. Nicméně, všechny vlnkové koeficienty submatice C_0 jsou stejné jako před samotným šifrovacím procesem.

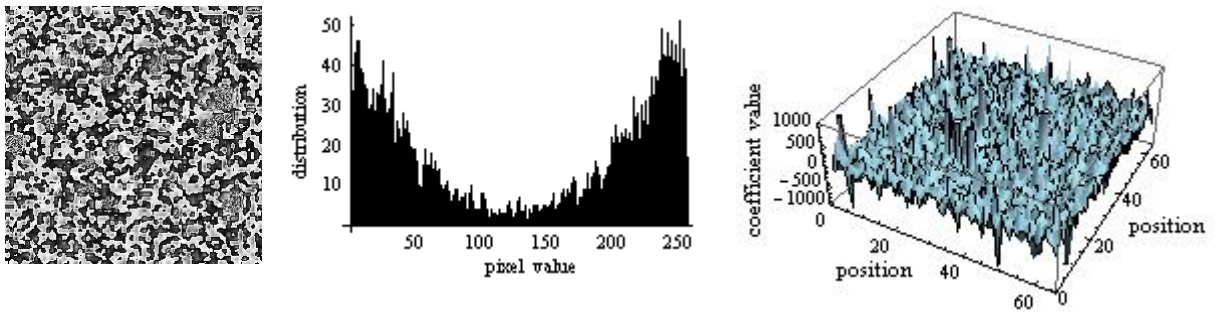
4 Výkonnost šifry

Jedním z hlavních úkolů naší práce bylo vytvořit takový šifrovací algoritmus, který by bylo možné využít pro aplikace v reálném čase. Algoritmus šifry byl napsán v jazyce C# a je nutné dodat, že kód nebyl optimalizován. Tabulka 1 zobrazuje čas v sekundách potřebný pro šifrování obrazu o velikosti 256x256 pixelů v závislosti na různě nastavených parametrech k a m. Úroveň zabezpečení zašifrovaného obrazu je přímo úměrná velikosti těchto dvou parametrů.



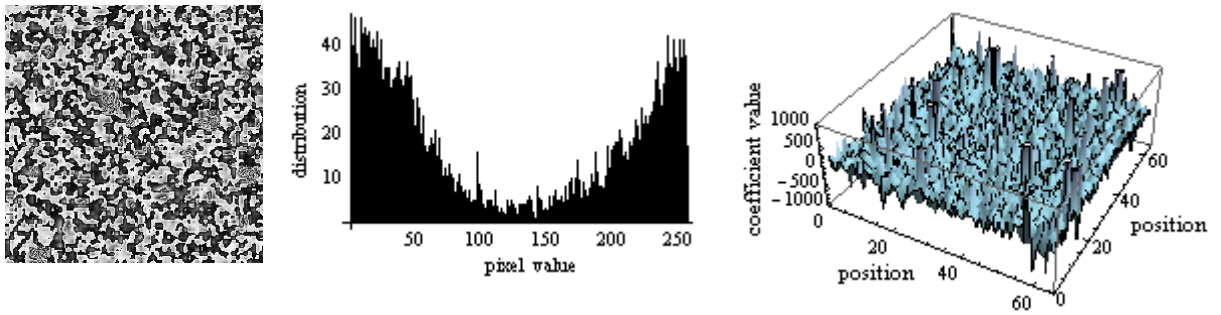
(a) (b) (c)

Obrázek 5: (a) původní obraz, (b) histogram původního obrazu, (c) vzorek vlnkové oblasti



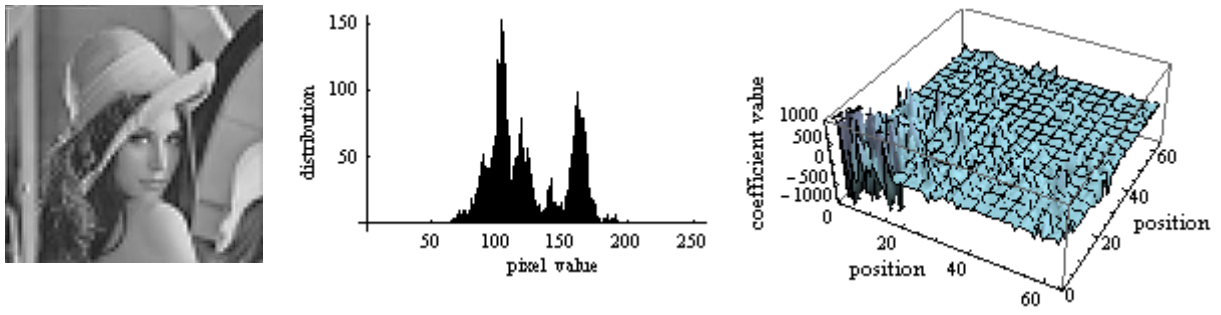
(a) (b) (c)

Obrázek 6: (a) zašifrovaný obraz, (b) histogram zašifrovaného obrazu, (c) vzorek vlnkové oblasti



(a) (b) (c)

Obrázek 7: (a) nesprávně dešifrovaný obraz, (b) histogram nesprávně dešifrovaného obrazu, (c) vzorek vlnkové oblasti



(a) (b) (c)

Obrázek 8: (a) dešifrovaný obraz, (b) histogram dešifrovaného obrazu, (c) vzorek vlnkové oblasti

Tabulka 1: Rychlost šifry

Iterace k / Cykly m	**1**	**5**	**10**	**25**
1	0.031	0.062	0.078	0.109
5	0.062	0.093	0.125	0.250
10	0.078	0.140	0.203	0.421
25	0.078	0.265	0.468	1.125

Vzhledem k naší předchozí práci [6] je potřebný čas na šifrování snížen 22-krát. To znamená, že maximální rychlost šifry je 2064kB/s na procesoru 1.50-GHz AMD Athlon. Pro optimální zabezpečení zašifrovaného obrazu je nutné nastavit parametry k a m na hodnotu 5. Rychlost zpracování se poté sníží na 688kB/s. Můžeme tedy vytvořit zabezpečenou video konferenci o rychlosti 10.75 FPS. Předpokládáme, že pokud provedeme optimalizaci kódu, je možné dosáhnout rychlosti 15 FPS, což je pro potřeby video konference již naprosto dostačující.

5 Závěr

Navržený šifrovací algoritmus pro statické obrazy využívá vlnkovou transformaci pro extrakci důležité informace z obrazu. Po převedení obrazu do vlnkové oblasti jsou vybrány pouze některé vlnkové koeficienty, které jsou následně zašifrovány chaotickým systémem Petera de Jonga. Souřadnice a hodnoty každého koeficientu jsou považovány za počáteční podmínky příslušné mapy. Iterací těchto map lze získat nové souřadnice a nové hodnoty koeficientů. Výpočetní čas byl výrazně snížen právě díky výběru důležitých vlnkových koeficientů. Přitom bezpečnost zašifrovaného obrazu stále zůstává dostatečná. Nicméně, při zanedbání koeficientů, reprezentujících detaily obrazu, dochází při rekonstrukci ke ztrátě informace. Tento šifrovací algoritmus lze tedy použít v některých real-time procesech, jako je video konference, kde požadavky na kvalitu jsou druhořadé.

Poděkování

Rád bych poděkoval na tomto místě svému školiteli prof. Vlčkovi za jeho vřelý přístup v mém dosavadním doktorském studiu a také mému kolegovi Ing. Běhalovi za odborné diskuze ohledně teorie chaosu a dynamických systémů.

Literatura

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

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

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

[4] Zhai, Y., Lin, S., Zhang, Q. Improving Image Encryption Using Multi-chaotic Map, Workshop on Power Electronics and Intelligent Transportationi System, 2008.

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

[6] Giesl, J., Vlcek, K., Image Encryption Based on Strange Attractor, ICGST-GVIP Journal. 2009, vol. 9, is. 2, pp. 19-26. ISSN 1687-398.

[7] Zhao., X-y., Chen, G., Zhang, D., Wang, X-h., Dong, G-c. Decryption of pure-position permutation algorithms. JZUS, Hangzhou, 2004.

[8] Sprott, J.C. Chaos and Time-Series Analysis, Oxford University Press, 2003, ISBN 978-0-19-850840-3.