Portál pre odborné publikovanie ISSN 1338-0087

Arnoľdovo zobrazenie, jeho vlastnosti a možné využitie

Oravec Jakub · Informačné technológie

04.04.2016

Tento článok je zameraný na predstavenie Arnoľdovho zobrazenia (Arnold's cat map), matematického predpisu, ktorý patrí medzi tzv. chaotické zobrazenia. Toto zobrazenie je možné využiť na preusporiadanie obrazových prvkov v štvorcových statických obrazoch. Článok sa ďalej zaoberá jeho periódou a spôsobmi jej výpočtu. Okrem toho článok popisuje vlastnosti Arnoľdovho zobrazenia, jeho známe modifikácie a použitia z oblasti steganografie. V prípade steganografického systému, ktorý využíva najmenej významnú bitovú rovinu (LSB), umožňuje Arnoľdovo zobrazenie ukrytie informácie z tohto extrahovaného obrazu aj pri extrakcii tejto roviny.

Úvod

Počas výskumu, ktorý sa týkal kryptografie v 80. rokoch minulého storočia sa objavili aj myšlienky využitia tzv. chaotických zobrazení [1, 2]. Tieto zobrazenia za svoj názov vďačia najmä citlivosti na vstupné parametre, ktoré ovplyvňujú hodnoty výstupných vzoriek. Chaotické zobrazenia v diskrétnej verzii vznikli väčšinou odvodením z im prislúchajúcich spojitých predpisov. V niektorých prípadoch boli vytvorené aj parametrizované (zovšeobecnené) verzie týchto zobrazení, čo je možné aj pri Arnoľdovom zobrazení [3].

V prípade spomenutých šifrovacích algoritmov boli, okrem chaotických zobrazení, navrhované rôzne ďalšie postupy, slúžiace na zvýšenie robustnosti voči ich prelomeniu. Aj keď sa môže zdať, že takéto šifry majú svoje výhody, môžme konštatovať, že doteraz (marec 2016) sa širšie neuplatnili. Iné použitie pre chaotické zobrazenia bolo objavené v období okolo roku 2010. Týka sa oblasti steganografie, vednej disciplíny, ktorá sa snaží ukryť skutočnosť o samotnom prenose tajnej informácie. Tento prenos sa realizuje prostredníctvom nevinne vyzerajúcich súborov, ktoré môžu byť pozmenené, vykazovať určité štatistické vlastnosti, alebo môžu byť vygenerované s cieľom preniesť tajnú informáciu [4].

Ku najjednoduchším steganografickým metódam sa dá zaradiť aj metóda LSB (Least Significant Bit, najmenej významná bitová rovina). Pri nej sa vybrané vzorky dát rozložia na jednotlivé bity, pričom tieto bity majú rozličný vplyv na výslednú amplitúdu vzorky. Bit, ktorý nesie najmenšie množstvo informácie sa označuje ako LSB. V niektorých prípadoch je možné tento bit nahradiť bitom tajnej informácie tak, že nevedomý pozorovateľ si túto zámenu neuvedomí. Avšak už jednoduchou extrakciou LSB sa dá určiť prítomnosť, alebo aj samotná tajná informácia [4]. Kvôli tejto nevýhode

je vhodné tajnú informáciu ešte pred vložením upraviť tak, aby jej obsah nebol zjavný. Niektoré riešenia využívajú šifrovacie algoritmy, avšak pre tieto účely je možné použiť aj chaotické zobrazenia.

Tento článok sa snaží v kapitole 1 predstaviť Arnoľdovo zobrazenie (AZ) a jeho vlastnosti, akými je jeho periodickosť a prítomnosť duchov, alebo miniatúr. Zovšeobecnená verzia AZ a úvahy o rozšírení AZ do troch rozmerov sú predstavené v kapitole 2. Ďalšia kapitola obsahuje zoznam známych použití AZ v oblasti steganografie. Posledná, štvrtá, kapitola zhŕňa vlastnosti AZ a steganografických systémov, ktoré používajú AZ a opisuje možnosti ďalšieho výskumu.

1. Arnoľdovo zobrazenie (Arnold's cat map)

Názov tohto zobrazenia pochádza od matematika Vladimíra Igoreviča Arnoľda, ktorý sa v rámci svojho doktorandského štúdia zameral aj na skúmanie teórie chaosu. V 60. rokoch minulého storočia realizoval experimenty so štvorcovým obrázkom mačky, ktorý zobrazoval do obrazu rovnakej veľkosti [5]. Toto zobrazenie jednotkového štvorca bolo neskôr pre potreby spracovania digitálneho obrazu diskretizované a jeho predpis sa dá uviesť ako (1):

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} (mod N) \tag{1}$$

kde (x', y') sú súradnice po zobrazení obrazového prvku so súradnicami (x, y), x, y, x', y' ε {0, 1, 2, …, N-2, N-1} a N je šírka, resp. výška štvorcového statického obrazu v obrazových prvkoch.

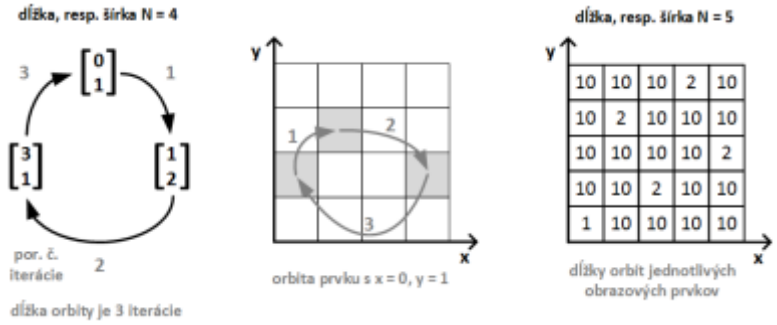
Dôsledky predpisu (1) sú zobrazené na Obr. 1. Môžme si všimnúť, že obraz sa po prvej iterácii AZ dá rozdeliť na štyri trojuholníky, ktoré vznikli „natiahnutím" (použitím operácie shearing) a následným preusporiadaním pôvodného obrazu. Každou ďalšou iteráciou (opakovaním) sa súradnice obrazových prvkov zmenia, a po určitom počte iterácií už výsledný obraz do istej miery pripomína zašumený obraz.

Obr. 1 Výstupné obrazy po rôznom počte iterácií AZ

Mohlo by sa zdať, že s rastúcim počtom iterácií AZ sa zmenšuje podobnosť pôvodného obrazu a obrazu získaného po iterácii AZ. Tento predpoklad však nie je správny, keďže AZ má vlastnosť tzv. periodicity. Pri vykonaní počtu iterácií, ktorý sa zhoduje s periódou AZ pre daný obraz sa opäť získa pôvodný obraz. Perióda AZ závisí od výšky, resp. šírky spracovávaného obrazu (v predpise 1 označené ako N). Jej výpočet je možný viacerými spôsobmi – zostrojením tzv. orbít a určením ich dĺžok, vypočítaním Pisanskej periódy pre zadané N, alebo použitím vzorcov [6, 7].

Orbitou pre obrazový prvok sa rozumie množina prvkov, do ktorých je tento prvok zobrazený, kým nie je zobrazený sám do seba (teda kým sa jeho súradnice nezhodujú s pôvodnými). Dĺžkou tejto orbity je potom počet potrebných iterácií AZ. Pri tomto spôsobe určenia periódy AZ je dôležité uvedomiť si, že dĺžky orbít jednotlivých obrazových prvkov môžu byť násobkami dĺžok orbít iných obrazových prvkov, a preto sa v tomto prípade perióda AZ rovná najväčšej dĺžke orbity. Za zaujímavosť môže byť považované, že obrazový prvok so súranicami x = 0, y = 0 má stále dĺžku orbity rovnú jednej.

Obr. 2 ilustruje príklad orbity a jej znázornenie pre jeden obrazový prvok a N = 4. Okrem toho poukazuje aj na rozličné dĺžky orbít všetkých obrazových prvkov pre N = 5.



Obr. 2 Príklad orbity, jej geometrické znázornenie a dĺžok orbít

Druhý spôsob na získanie periódy AZ využíva tzv. Pisanskú periódu. Ak pre prvky Fibonacciho postupnosti určíme čísla, ktoré sú s nimi kongruentné modulo N, získame postupnosť čísel, ktoré majú určitú periódu. Práve táto perióda sa označuje ako Pisanská. Keďže Fibonacciho postupnosť v „modernom“ ponímaní začína prvkami {0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, ...} tak po vykonaní operácie modulo N získavame súradnice na orbite prvku s x = 0 a y = 1. Príklad uvedieme pre N = 4: {0, 1, 1, 2, 3, 1, 0, 1, 1, 2, 3, 1, 0, ...}. Pretože pozícia obrazového prvku je určená dvojicou súradníc, periódou AZ nie je priamo Pisanská perióda, ale jej polovica. Jedinou výnimkou z tohto pravidla je prípad, kedy je N rovné dvom a perióda AZ je rovná hodnote Pisanskej periódy pre N = 2.

Výpočet periódy AZ vzorcami je založený na overení platnosti množiny podmienok pre zadané N. V niektorých prípadoch je však nutné určiť, či je N prvočíslo, alebo zložené číslo. Tento krok môže byť pri väčších číslach výpočtovo náročnejším, ako využitie vyššie spomínaných metód. Ak sa ukáže, že N je zložené číslo, je potrebné rozložiť ho na súčin jeho deliteľov. Algoritmus ďalšími krokmi postupne vylučuje niektoré z deliteľov, ich násobky a podiely, až kým nenájde jeden z deliteľov, ktorý spĺňa množinu podmienok. Táto množina, ako aj celý algoritmus s príkladom použitia, sú uvedené v [7]. Za tento odstavec uvádzame v Tab. 1 príklad rôznych períód AZ pre rôzne N. Skratka op znamená obrazový prvok.

Tab. 1 Periódy AZ pri rôznych rozlíšeniach vstupného obrazu

N	perióda AZ	N	perióda AZ
120×120 op	60	128×128 op	96

121×121 op	55	129×129 op	44
122×122 op	30	130×130 op	210
123×123 op	20	131×131 op	65
124×124 op	15	132×132 op	60
125×125 op	250	133×133 op	72
126×126 op	24	134×134 op	204
127×127 op	128	135×135 op	180

Medzi ďalšie vlastnosti AZ patrí aj prítomnosť tzv. duchov, miniatúr, alebo otočenej verzie obrazu po určitom počte iterácií. Ako duchovia, alebo miniatúry sa označujú zmenšené verzie pôvodného obrazu, ktoré sa v obraze po aktuálnej iterácii vyskytujú viackrát. Existencia duchov, alebo miniatúr závisí od N zobrazovaného obrazu. Takáto situácia je ilustrovaná na Obr. 3, kde rozlíšenie zobrazovaného obrazu bolo 120×120 obrazových prvkov.

Obr. 3 Duchovia, alebo miniatúry pri použití AZ

Rotácia pôvodného obrazu závisí rovnako ako prítomnosť duchov od parametra N. Príklad otočeného obrazu pre N = 37 je na Obr. 4. Môžme si všimnúť, že prvý riadok a stĺpec obrazových prvkov nie je otočený rovnakým spôsobom ako zvyšok obrazu, ale ich obrazové prvky (okrem prvku s x = 0 a y = 0) sú otočené v rámci tohto riadka, resp. stĺpca. Ako už bolo spomenuté skôr, obrazový prvok so súradnicami x = 0 a y = 0 sa s použitím predpisu (1) zobrazí sám do seba.

Obr. 4 Výskyt otočeného obrazu po určitom počte iterácií AZ

2. Zovšeobecnené Arnoľdovo zobrazenie a rozšírenie do troch rozmerov

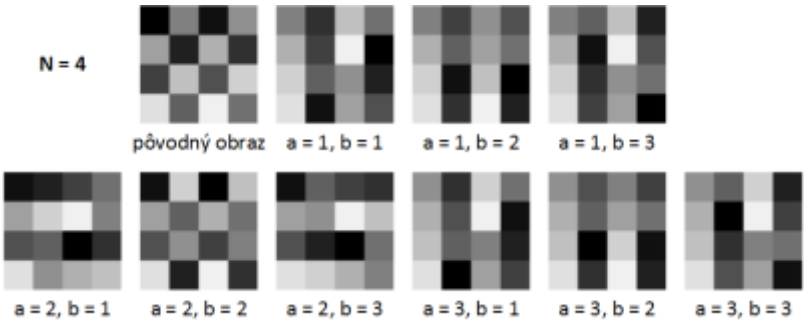
Arnoľdovo zobrazenie v podobe, ktorú sme si zatiaľ ukázali, predstavuje nástroj na preusporiadanie (permutáciu) obrazových prvkov statického obrazu. V dobe, keď sa uvažovalo o jeho použití v oblasti blokových šifier bolo potrebné parametrizovať toto

zobrazenie tak, aby výstupný obraz (resp. v tomto prípade blok dát) bol závislý na určitých vstupných parametroch (v oblasti kryptografie známe ako kľúče). Už v [5] bola uvedená podmienka periodicity pre AZ: absolútna hodnota determinantu matice (teda statického obrazu) |D| musí byť rovná jednej. V prípade predpisu (1) si môžme všimnúť, že |D| = 1.2 – 1.1 = 1, takže táto podmienka je splnená. Táto podmienka platí aj pre predpis (2) uvedený v [3, 8]:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} (mod N) \tag{2}$$

kde (x', y') sú súradnice po zobrazení obrazového prvku so súradnicami (x, y), x, y, x', y' ε {0, 1, 2, ..., N-2, N-1}, a, b ε {1, 2, 3, ..., N-2, N-1} a N je šírka, resp. výška štvorcového statického obrazu v obrazových prvkoch.

Vplyv hodnôt parametrov a a b sa prejavuje na výstupnom obraze spôsobom, ktorý je ilustrovaný na Obr. 5.



Obr. 5 Závislosť obrazu po prvej iterácii ZAZ na hodnotách parametrov

Pre použitie v kryptografických systémoch je dôležitým parametrom aj počet použiteľných kľúčov. Tento parameter vyjadruje počet kľúčov, ktoré sa dajú využiť pri šiforvaní, resp. dešifrovaní. Ako môžme vidieť z Obr. 5, pre N = 4 je tento počet rovný deviatim. Vo všeobecnosti sa počet použiteľných kľúčov pre ZAZ dá vypočítať ako (3):

$$PPK = (N-1)^p \tag{3}$$

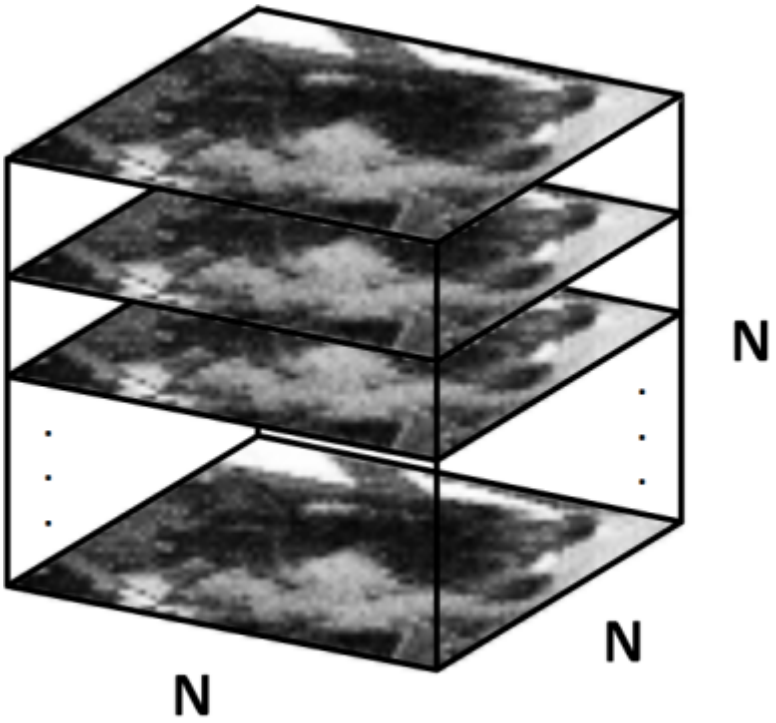
kde p je počet parametrov ZAZ a N je šírka, resp. výška štvorcového statického obrazu v obrazových prvkoch.

Autori viacerých článkov vo svojich prácach konštatovali, že najmä pri malých blokoch dát je počet použiteľných kľúčov pri ZAZ nedostatočný [3, 8]. Preto bol neskôr vytvorený predpis (4), ktorý rozširuje ZAZ do troch rozmerov:

$$\begin{bmatrix} x' \\ y' \\ z' \end{bmatrix} = \begin{bmatrix} 1 & 0 & a \\ bc & 1 & abc+c \\ bcd+b & d & abcd+ab+cd+1 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} (mod N) \tag{4}$$

kde (x', y', z') sú súradnice po zobrazení obrazového prvku so súradnicami (x, y, z), x, y, z, x', y', z' ε {0, 1, 2, ..., N-2, N-1}, a, b, c, d ε {1, 2, 3, ..., N-2, N-1} a N je šírka, resp. výška každého z množiny N zobrazovaných štvorcových statických obrazov v obrazových prvkoch.

Z predpisu (4) vidíme, že takéto zobrazenie upravuje aj amplitúdu (súradnicu na osi z) obrazových prvkov. V tomto prípade sa však nejedná o výpočet novej amplitúdy, ako je to v prípade transformácií, ale o preusporiadanie amplitúd obrazových prvkov viacerých statických obrazov. Práve skutočnosť, že pre trojrozmerné ZAZ je potrebná množina obrazov, obmedzuje využiteľnosť tohto zobrazenia, keďže je potrebné použiť práve N statických obrazov s rozlíšením NxN obrazových prvkov. Trojrozmerné ZAZ sa teda nedá použiť na spracovanie jediného statického obrazu, ale dajú sa ním preusporiadať napr. súradnice obrazových prvkov v jednotlivých snímkach videosekvencie. Táto problematika je načrtnutá na Obr. 6.



Obr. 6 Množina statických obrazov zobrazená ako kocka s hranou rovnou N

3. Prehľad použití Arnoľdovho zobrazenia

Ako už bolo viackrát spomenuté, AZ bolo využité vo viacerých návrhoch symetrických blokových šifier [1]. Okrem tejto oblasti bolo aplikované aj v steganografických algoritmoch, na „predspracovanie“ obrazu s tajnou informáciou, pred vložením do krycieho obrazu. Táto operácia umožňuje zmeniť obraz so zreteľnou informáciou na obraz, ktorý nedáva zmysel. Tento prístup bol použitý aj v [9], kde bol obraz s tajnou informáciou pozmenený AZ s počtom iterácií, ktorý bol daný vstupným parametrom. O možnosti použitia AZ s využitím Cannyho detektora hrán sa píše v zdroji [10]. Blokové spracovanie vstupného obrazu s tajnou informáciou pred samotnou AZ opisuje článok [11]. Takýto prístup čiastočne zmierňuje jeden z nedostatkov AZ – potrebu štvorcového statického obrazu. Aplikácia AZ v oblasti digitálnej vodotlače je popísaná v [12].

Úplne odlišná myšlienka bola prezentovaná v [1]. V tomto prípade sa uvažuje o využití jedného z chaotických zobrazení (v prípade tohto článku ide o Pekárske zobrazenie – Baker’s map) na preusporiadanie súradníc na osiach x a y a na použitie inej funkcie pre získanie upravenej súradnice na osi z. Takýto postup by však pri nevhodne zvolenej funkcii mohol narušiť periodicitu AZ.

4. Záver

V tomto článku sme predstavili chaotické zobrazenie, ktoré pracuje so štvorcovými statickými obrazmi. Vďaka podmienke periodicity sa po každej iterácii AZ získa obraz s rovnakým rozlíšením, aké mal vstupný obraz. Poukázali sme na vplyv počtu iterácií na výsledný obraz, opísali sme problematiku periódy AZ a jej výpočtu. Ďalej sme uviedli aj príklady duchov, miniatúr a taktiež aj otočeného vstupného obrazu, ktoré nastávajú po určitom počte iterácií pri niektorých hodnotách rozlíšenia spracovávaného obrazu. Venovali sme sa aj zovšeobecnenej a trojrozmernej verzii AZ. Uviedli sme niekoľko zdrojov, v ktorých je bližšie popísané použitie AZ v konkrétnych aplikáciách.

Z prehľadu literatúry, ktorý sme vykonali, môžme konštatovať, že AZ sa v steganografických systémoch využíva len na „predspracovanie“ obrazu s tajnou informáciou pred jej vložením do krycieho obrazu. V tomto prípade sa ako jeho výhoda pred štandardnými šifrovacími algoritmami (ako napr. AES) javí hlavne jednoduchosť a teda aj rýchlosť. Avšak stále nebola zverejnená žiadna publikácia, ktorá by využila do istej miery modifikované AZ na vytvorenie podprahového kanála, slúžiaceho na vloženie tajnej informácie. Ako bolo spomenuté v kap. 3, takáto myšlienka už bola vyslovená, ale v tomto prípade je potrebné vytvoriť funkciu pre získanie novej súradnice na osi z (amplitúdy) tak, aby tieto nové súradnice vykazovali nejakú vlastnosť, ktorá by sa dala využiť na ukrývanie informácie (ako napr. nízky význam LSB, alebo porovnanie veľkosti koeficientov pri DCT flipping). Návrh funkcie, pri ktorej by vloženie tajnej informácie zmenilo priamo súradnice na osi z by viedol ku „znovuobjaveniu“ steganografickej metódy LSB, ktorá využíva práve tieto zmeny. Výhodou takto modifikovaného AZ využitého na vkladanie tajnej informácie, oproti metóde LSB by mohlo byť preusporiadanie obrazu, ktoré by vzniklo pri iterovaní potrebnom pre získanie pôvodného obrazu.

Použitá literatúra

1. J. Fridrich, „Symmetric Ciphers Based on Two-Dimensional Chaotic Maps,“ v International Journal of Bifurcation and Chaos, Vol. 8, No. 6, 1998, pp. 1259–1284.
2. J. Scharinger, „Fast encryption of image data using chaotic Kolmogorov flows,“ v Journal of Electronic Imaging, Vol. 7, No. 2, 1998, pp. 318–325.
3. G. Chen, Y. Mao, C. K. Chui, „A symmetric image encryption scheme based on 3D chaotic cat maps,“ v Chaos, Solitons and Fractals, Vol. 21, No. 3, 2004, pp. 749–761.
4. S. Katzenbeisser, F. A. P. Petitcolas, Information hiding: Techniques for Steganography and Digital Watermarking, Artech Hosue, Boston, 2000, ISBN: 978-1580530354, 220 pp.
5. V. I. Arnold, A. Avez, Ergodic Problems of Classical Mechanics, W. A. Benjamin, New Jersey, 1968, 296 pp.
6. F. Svanström, Properties of a generalized Arnold’s discrete cat map, diplomová práca, Linnæus University, Švédsko, 2014.
7. J. Bao, Q. Yang, „Period of the discrete Arnold cat map and general cat map,“ v Nonlinear Dynamics, Vol. 70, No. 2, 2012, pp. 1365–1375.
8. Y. Wu, S. Agaian, J. P. Noonan, „A New Family of Generalized 3D Cat Maps,“ draft zaslaný do IEEE Signal Processing Letters, 2012.
9. M. Mishra, A. R. Routray, S. Kumar, „High Security Image Steganography with Modified Arnold’s Cat Map,“ v International Journal of Computer Applications, Vol. 37,

No. 9, 2012, pp. 16–20.
10. R. Roy, A. Sarkar, S. Changder, „Chaos based Edge Adaptive Image Steganography,“ v Proceedings of International Conference on Computational Intelligence: Modelling Techniques and Applications, Vol. 10, 2013, pp. 138–146.
11. V. Mani Bharathi, M. Manimegalai, V. Sinduja, „Enhancement of Image Security with New Methods of Cryptography and Steganography,“ v International Journal of Advanced Information Science and Technology, Vol. 9, No. 9, 2013, pp. 59–64.
12. S. Rawat, B. Raman, „A Chaotic System Based Fragile Watermarking Scheme for Image Tamper Detection,” v International Journal of Electronics and Communications, Vol. 65, 2011, pp. 840–847.

Spoluautorom článku je doc. Ing. Ľuboš Ovseník, PhD., Katedra elektroniky a multimediálnych telekomunikácií, FEI TU Košice, Slovenská republika