Hodnocení průběhu studia DSP pana ing. Jiřího Giesla

Pan ing. Jiří Giesl absolvoval magisterské studium na Univerzitě Tomáše Bati ve Zlíně v roce 2007 a v témže roce byl přijat ke studiu doktorského studijního programu na mnou vypsané téma: **Metodiky zpracování a syntézy multimediálních signálů založené na postupech a parametrech chaotických systémů**.

Ve všech předmětech předepsaných individuálním studijním plánem dosahoval ing. Giesl výborných výsledků. Mohu s uspokojením konstatovat, že studijní plán, který jsem mu předepsal, splnil ve všech termínech včetně termínu Státní závěrečné zkoušky v roce 2010. V závěru roku 2010 pak vypracoval disertační práci, kterou se nyní chystá obhajovat.

Průběh jeho studia je možné charakterizovat také jako vzornou representaci v oblasti vědecké činnosti. O tom svědčí výčet jeho publikační činnosti, který je výrazně orientovaný na řadu prestižních mezinárodních konferencí a sympozií, z nichž bylo několik garantováno organizací IEEE. Dokladem o kvalitě publikovaných prací jsou i časopisecké články v zahraničních renomovaných vědeckých časopisech.

Jako nezbytnou součást práce na vypsaném tématu doktorské disertace je možné vyzdvihnout vytvoření původního programového vybavení, pomocí kterého pan ing. Giesl provedl řadu experimentů a tak vytvořil bohatou škálu výsledků, které jsou hodnoceny v jeho disertační práci a které dokládají výjimečné vlastnosti jím vytvořených chaotických šifer, které jsou použitelné při šifrování obrazu. Principy chaotického šifrování použil s podobným úspěchem i v případě zvukových signálů.

Svými pracemi dosáhl ocenění i na mezinárodním studentském semináři PAD 2009, kde byl oceněn druhým místem za práci Zrychlení algoritmu chaotické šifry pro obrazy. Hodnotící komise složená ze zástupců školitelů vysokých škol vyhodnotila v uvedené práci zejména originalitu algoritmů, ale i způsob implementace metod chaotických šifer a způsob jejich aplikace v oblasti multimediálních signálů.

Vážený pane předsedo, vážení členové komise, je pro mne milou příležitostí, že mohu doporučit disertaci pana ing. Giesla k obhajobě jako práci s výjimečně dobrými a v praxi použitelnými výsledky vědecké práce.

Ve Zlíně 22. února, 2011

prof. ing. Karel Vlček, CSc., školitel.

Posudek disertační práce

Název práce: **Kryptografický systém pro obrazy založený na deterministickém chaosu**

Autor: Ing. Jiří Giesl

Oponent: doc. Mgr. Roman Jašek, Ph.D.

Rozsah práce: 127 stran včetně obrázků a příloh

Předložená práce je strukturována do devíti kapitol, které jsou vhodně rozděleny do části teoretické a praktické. První a druhá kapitola uvádí do problematiky řešené v práci a vytyčuje cíle disertační práce. Třetí kapitola pojednává o základech kryptologie, zabývá se proudovými a blokovými kryptografickými systémy, principy difůze a konfúze a podává přehled metod s krátkou charakteristikou jednotlivých kryptoanalytických útoků. Kapitola je uzavřena přehlednou částí zaměřenou na šifrování obrazu. Čtvrtá kapitola je zaměřena na základní vlastnosti deterministického chaosu. Představuje několik chaotických systémů jak v diskrétní, tak ve spojité oblasti. Dle mého názoru i vhodně obsahuje informaci o podivných atraktorech. Do kapitoly je vložena samostatná část zaměřená pro nastavení citlivosti na počáteční podmínky (Ljaponovův exponent). Pátá kapitola rozebírá problematiku chaosu v kryptografii a řeší i „současný stav chaotických šifer obrazu". Pátou kapitolou teoretická část končí. I přes celkovou stručnost teoretické části **konstatuji dobrou orientaci v problematice, přesné vyjadřování a znalost odborné literatury.**

Praktická část začíná kapitolou šestou, která je těžištěm celé disertační práce. Obsahuje návrh kryptografického systému pro obrazy s celým šifrovacím procesem a také je zde provedena detailní analýza bezpečnosti zašifrovaných obrazů. Pozitivně hodnotím srovnání se stávajícími chaotickými šiframi. Sedmá kapitola popisuje waveletové transformace pro extrakci a jejich využití pro zrychlení kryptovacího procesu. Osmá kapitola představuje útoky na navržený kryptografický systém pomocí diferenciální evoluce.

Výsledky disertační práce jsou shrnuty v deváté kapitole, kde je provedena úplná diskuse nad výsledky experimentů. Samotná diskuse je rozebrána v šesti bodech, které ukazují na dosažené výsledky a předkládají další otázky pro možná další řešení. Předložené body jsou samy o sobě dalšími náměty.

Konstatuji:

Cíle práce byly splněny a obsahová úroveň odpovídá požadavkům kladeným na disertační práci.

Formální náležitosti práce a její úprava jsou na vysoké úrovni, práci byla věnována náležitá pozornost. Je zřejmé i velice kvalitní metodické vedení školitelem.

Otázky:

Kde vidíte možnost reálného uplatnění návrhu vašeho kryptografického systému (případně obecně kryptografických systémů založených na deterministickém chaosu)?

Zdůvodněte tvrzení v kapitole 6.2.8 „.. zabezpečení zašifrovaného obrazu je přímo úměrné počtu šifrovacích rund ...". Existuje zde nějaká hranice smysluplného počtu šifrovacích rund?

Závěrečné stanovisko:

Disertační práce je psána jasně, srozumitelně a s přehledem. Jde o kvalitní práci, **doporučuji ji k obhajobě** a v případě úspěšného obhájení udělení titulu Ph.D.

Ve Zlíně dne 18.listopadu 2010

doc. Mgr. Roman Jašek, Ph.D.

Ústav informatiky a umělé inteligence

Fakulta aplikované informatiky UTB ve Zlíně

Slezská univerzita v Opavě
Filozoficko-přírodovědecká fakulta v Opavě
Ústav informatiky
Bezručovo nám, 13, 746 01 Opava
Tel.: 553 684 368, fax: 553 684 370, e-mail: cs@fpf.slu.cz

Posudek doktorské disertační práce p.Ing. Jiřího Giesla na téma „Kryptografický systém pro obrazy založený na deterministickém chaosu.“

Postup řešení

Předložená disertační práce je zaměřena do oblasti kryptografie obrazových dat. Autor na začátku práce definuje všechny pojmy nezbytné pro vysvětlení problematiky a základy kryptografických systémů. Na konci kapitoly přechází ke kryptovacím systémům pro obrazová data. Ve 4 kapitole vysvětluje pojem deterministický chaos a chaotické systémy a zavádí tzv. „podivný atraktor“, jedná se o atraktor Cliffordova systému.

Tento atraktor Cliffordova systému byl rozšířen z dvoudimenzionální verze do čtyř dimenzionální verze tak, aby mohly být zašifrovány informace o poloze pixelu, jeho barvonosné složce a následně i modifikace hodnoty výsledného pixelu. Fakticky díky tomu, že pro počáteční podmínky Cliffordova systému jsou použity samy pixely, je umožněno vygenerovat rozdílné permutační předpisy pro stejnou pozici v obraze. Cenou za poměrně mohutný kryptografický systém je časová náročnost, kterou autor řeší waveletovou transformací a místo obrazových pixelů používá koeficienty waveletové transformace. Tato jistá verze komprese vede k redukci informace a snížení časové náročnosti.

Autor velice detailně prověřuje charakteristiky kryptografického systému a uvádí množství obrázků a tabulek jako dokumentaci.

Autor rovněž ověřuje resistenci kryptografického systému proti útokům evolučních algoritmů. Bohužel zde používá poměrně standardní evoluční či genetické algoritmy, přičemž se zdá, že nastavení počtu chromozomů v generaci při experimentech je poměrné malé, tudíž i variabilita generace je poměrně malá.

Rozvoj vědního oboru a aplikační potenciál

Vědecký přínos disertační práce vidím v rozšíření nových metod kryptografie obrazové informace, odolnějších vůči napadení. Vědecký přínos, tedy i jádro disertační práce, je obsažen v kapitolách 5, 6 a 7.

Aplikační přínos je naznačen od poloviny 7. kapitoly. Dle mého názoru je možné přímé využití šifrování obrazových dat v bezpečnostních složkách v medicíně atp. Velice přínosné by mohlo být zařazení do protokolu DICOM.

Formální úprava

Disertační práce je napsaná velice pečlivě, s kvalitní obrazovou dokumentací. V práci se objevují chyby jen sporadicky např. (Obrázek 4.4:.. atraktor), ve vzorci (6.4 modT), formulace (str. 43., 5. řádek chybí „je“). Myslím si, že tato disertační práce nemá daleko k monografii, či po přidání dalších publikací a splnění náležitých podmínek, k habilitační práci.

Slezská univerzita v Opavě
Filozoficko-přírodovědecká fakulta v Opavě
Ústav informatiky
Bezručovo nám, 13, 746 01 Opava
Tel.: 553 684 368, fax: 553 684 370, e-mail: cs@fpf.slu.cz

Publikace studenta vzhledem k jádru disertační práce

Dvě časopisecké publikace vztahující se k jádru disertační práce jsou články uveřejněné v recenzovaných renomovaných časopisech. Ostatní tvoří 4 publikace ve sbornících zahraničních konferencí, 6 publikací na domácích konferencích a jedna ve sborníku zahraniční konference je v tisku. Dle mého je tedy publikační činnost studenta doktorského studia na velmi dobré úrovni.

Dotazy či návrhy na rozpravu

V rámci dotazů, či rozpravy by mě zajímalo, jaké jsou přednastavené parametry atraktoru Cliffordova systému Obr. 6.1.? Jakým způsobem by ovlivnilo využití pokročilých metod genetických algoritmů nalezení globálního extrémů? Pokročilými metodami GA je myšleno využití operátorů omezené doby života jedince, operátor migrace a operátor sexuální reprodukce. Dále by mě zajímalo dle jakého postupu, či metody byl zvolen počet chromozomů v jedné generaci, dle mého počet 150 je poměrně malý pro dostatečnou variabilitu inicializační a dalších generací.

Doporučení k obhajobě

Z následujících důvodů:

1. **formální úprava na velmi dobré úrovni,**
2. **aktuální řešená problematika s vědeckým vlastním přínosem a s velmi pravděpodobnými aplikačními výstupy,**
3. **publikační činnost vztahující se k jádru disertační práce na velmi dobré úrovni,**

doporučuji disertační práci pana Ing. Jiřího Giesla na téma „Kryptografický systém pro obrazy založený na deterministickém chaosu“ v oboru Inženýrská informatika k obhajobě před disertační komisí.

Dne 7. 2. 2011 v Opavě.

Doc. Ing. Petr Čermák, Ph.D.

Posudek disertační práce

Jiřího Giesla

Kryptografický systém pro obrazy založený na deterministickém chaosu
(Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky)

Text, který mi byl předložen k posouzení, má 127 stran a je členěn do devíti kapitol (Úvod, Cíle disertační práce, Kryptografický systém, Deterministický chaos, Využití chaosu v kryptografii, Kryptografický systém pro obrazy, Optimalizace rychlosti kryptografického systému, Kryptoanalýza pomocí evolučních algoritmů, Závěr). Kapitoly 1 až 5 mají všeobecně popisný charakter. Za zásadní lze považovat obsah kapitol 6 až 8, kde kde je konkrétněji popisován disertantův přínos.

Za rozhodující považuji skutečnost, že šifrování obrazu založené na chaosu je významná a prakticky důležitá oblast, která se zejména v poslední době rychle rozvíjí. Disertantem zvolené téma lze tedy považovat za významné. V práci disertant deklaruje vytvoření nového algoritmu pro šifrování, což lze opět považovat za přínos, který je z hlediska požadavků kladených na disertační práci zcela dostačující. Z předloženého seznamu publikací disertanta, jakož i nahlédnutím do databáze Web of Science lze zjistit, že autorem navržené přístupy byly již také dostatečně publikovány. Např. na Wef of Science lze nalézt celkem 5 publikací pojednávajících o dané problematice, u nichž je pan disertant autorem nebo spoluautorem. S ohledem na právě uvedené je mé základní hodnocení předložené disertační práce pozitivní. K práci mám ovšem i některé připomínky, které uvádím dále.

Kapitoly 3 a 4 jsou do značné míry pouze přehledem vybraných teoretických základů. Kapitola 5 zabývající se využitím chaosu v kryptografii je poměrně stručná a stručný je zejména popis „state of the art" ve zvolené oblasti, jemuž je v práci věnována podklapitola 5.3 mající pouhé dvě strany, což se mi zdá poněkud málo. Autor mohl věnovat popisu současného stavu více prostoru. Mohly být uvedeny některé další práce, zejména práce z poslední doby, kterých je citováno poměrně málo.

Při návrhu svého vlastního algoritmu se disertant mohl lépe vymezit vůči autorům a algoritmům existujícím (na které nedostatky jiných podobných algoritmů autor reaguje, v čem je navržený algoritmus jiný a v čem zase naopak podobný ve srovnání s algoritmy existujícími). Testování a srovnání s jinými algoritmy mohlo být provedeno rozsáhleji. Poznámku na straně 59, že většina algoritmů nemá ukazatele NPCR a UACI zveřejněny, a proto s nimi nelze provést srovnání, přijímám s rozpaky. Nebylo-li možné jinak, mohl je disertant naiplementovat a hodnoty sám zjistit. Srovnání s jinými kryptografickými systémy tedy mohlo být provedeno důkladněji. V předložené podobě navržený algoritmus vnímám jako poněkud odtržený od jeho případných konkurentů.

V otázce výpočetní rychlosti se disertant soustřeďuje již pouze výlučně na jím navržený algoritmus. Údaje o rychlosti pro jiné algoritmy, což by umožnilo porovnání, opět neposkytuje.

Po formální stránce je práce vypracována vcelku pěkně. Jen ojediněle jsem narazil na překlepy. Formátování nadpisů hlavních kapitol (např. str. 78) je někdy poněkud překvapivé.

Závěr

Přestože připomínky, které jsem uvedl výše, nepovažuji za zanedbatelné, je mé celkové hodnocení práce dáno skutečností, že disertant, dle mého soudu, dostatečně prokázal schopnost vědecké práce tím, že navrhl nový algoritmus v oblasti, kterou lze považovat za významnou, a že své výsledky na přiměřené úrovni rovněž publikoval. Na základě výše uvedeného doporučuji práci k obhajobě.

Ostrava 31. 1. 2011

doc. Dr. Ing. Eduard Sojka

Posudek disertační práce

Název práce: **Kryptografický systém pro obrazy založený na deterministickém chaosu**

Autor: Ing. Jiří Giesl

Oponent: doc. Mgr. Roman Jašek, Ph.D.

Rozsah práce: 127 stran včetně obrázků a příloh

Předložená práce je strukturována do devíti kapitol, které jsou vhodně rozděleny do části teoretické a praktické. První a druhá kapitola uvádí do problematiky řešené v práci a vytyčuje cíle disertační práce. Třetí kapitola pojednává o základech kryptologie, zabývá se proudovými a blokovými kryptografickými systémy, principy difůze a konfúze a podává přehled metod s krátkou charakteristikou jednotlivých kryptoanalytických útoků. Kapitola je uzavřena přehlednou částí zaměřenou na šifrování obrazu. Čtvrtá kapitola je zaměřena na základní vlastnosti deterministického chaosu. Představuje několik chaotických systémů jak v diskrétní, tak ve spojité oblasti. Dle mého názoru i vhodně obsahuje informaci o podivných atraktorech. Do kapitoly je vložena samostatná část zaměřená pro nastavení citlivosti na počáteční podmínky (Ljaponovův exponent). Pátá kapitola rozebírá problematiku chaosu v kryptografii a řeší i „současný stav chaotických šifer obrazu". Pátou kapitolou teoretická část končí. I přes celkovou stručnost teoretické části **konstatuji dobrou orientaci v problematice, přesné vyjadřování a znalost odborné literatury.**

Praktická část začíná kapitolou šestou, která je těžištěm celé disertační práce. Obsahuje návrh kryptografického systému pro obrazy s celým šifrovacím procesem a také je zde provedena detailní analýza bezpečnosti zašifrovaných obrazů. Pozitivně hodnotím srovnání se stávajícími chaotickými šiframi. Sedmá kapitola popisuje waveletové transformace pro extrakci a jejich využití pro zrychlení kryptovacího procesu. Osmá kapitola představuje útoky na navržený kryptografický systém pomocí diferenciální evoluce.

Výsledky disertační práce jsou shrnuty v deváté kapitole, kde je provedena úplná diskuse nad výsledky experimentů. Samotná diskuse je rozebrána v šesti bodech, které ukazují na dosažené výsledky a předkládají další otázky pro možná další řešení. Předložené body jsou samy o sobě dalšími náměty.

Konstatuji:

Cíle práce byly splněny a obsahová úroveň odpovídá požadavkům kladeným na disertační práci.

Formální náležitosti práce a její úprava jsou na vysoké úrovni, práci byla věnována náležitá pozornost. Je zřejmé i velice kvalitní metodické vedení školitelem.

Otázky:

Kde vidíte možnost reálného uplatnění návrhu vašeho kryptografického systému (případně obecně kryptografických systémů založených na deterministickém chaosu)?

Zdůvodněte tvrzení v kapitole 6.2.8 „.. zabezpečení zašifrovaného obrazu je přímo úměrné počtu šifrovacích rund ...". Existuje zde nějaká hranice smysluplného počtu šifrovacích rund?

Závěrečné stanovisko:

Disertační práce je psána jasně, srozumitelně a s přehledem. Jde o kvalitní práci, **doporučuji ji k obhajobě** a v případě úspěšného obhájení udělení titulu Ph.D.

Ve Zlíně dne 18.listopadu 2010

doc. Mgr. Roman Jašek, Ph.D.

Ústav informatiky a umělé inteligence

Fakulta aplikované informatiky UTB ve Zlíně