Oponentní posudek doktorské disertační práce

Univerzita Tomáše Bati ve Zlíně

Fakulta aplikované informatiky

Autor doktorské disertační práce: Ing. Ivo Motýl

Školitel: doc. Mgr. Roman Jašek, Ph.D.

VÝZKUM VYUŽITÍ MOŽNOSTÍ FRAKTÁLNÍ GEOMETRIE PRO ZABEZPEČENÍ INFORMAČNÍCH SYSTÉMŮ

Aktuálnost tématu doktorské disertační práce

V předkládané disertační práci jsou řešeny aktuální problémy využití principů fraktální geometrie v oblasti kryptografického zabezpečení komunikace v informačních systémech.

Aktuálnost tématu této práce vychází především z toho, že moderní prostředí informačních systémů je a bude pod hrozbou kyberterorismu. Této oblasti se nyní dostává velmi velké pozornosti světových mocností zejména v oblasti vojensko-hospodářské. Proto toto téma považuji za perspektivní a svým rozsahem a hloubkou uváděných závěrů za velmi užitečné.

Správně byl autor práce školitelem směrován na systémovou analýzu fraktálních struktur pro šifrovací a dešifrovací procesy. Tím tato práce je náročná a potřebná pro možné způsoby testování vůči kryptoanalytickým metodám.

Splnění cíle

Cíle práce, uvedené na str. 20., jsou velmi dobře rozpracovány a dávají možnost posoudit jednotlivé kroky autora uvedené v deklarované struktuře práce. Uvedená teoretická východiska od str.22. dávají představu o šířce vybraného zaměření práce a jsou dobrým vodítkem pro posouzení jednotlivý kroků autora v následujících kapitolách a také svědčící o správném pojetí celé práce. Proto v dalších kapitolách jsou cíleně vymezeny oblasti řešení vedoucí k aplikaci navrženého řešení pro modelování systému. Tím je tato práce průkaznější a dává možnost aktivně sledovat výsledky práce.

Autor splnil uvedené cíle a popsal je v přehledné hierarchické struktuře této disertační práce.

Oceňuji stručné vyjádření současného stavu zkoumané oblasti a dále zajímavý popis řešení a výsledky práce.
Těmito kapitolami autor naplnil modelovou představu vedoucí ke splnění zadaných cílů.

Postup řešení problému a výsledky disertační práce

Konstrukce navrhovaného modelu uvedená správně v kapitolách „Praktická část" charakterizuje odpovídající výzkum. V cílených podkapitolách popisuje autor velmi dobře systémovou představu modelovaného a modelujícího prostředí. Uvedený postup řešení problému je velmi zajímavý a dává náměty pro další možné řešení zadaného problému.

Význam pro praxi a pro rozvoj vědního oboru

Z hlediska konstrukce uvedeného prostředí autor velmi dobře využil svých zkušeností a dobře je popsal v kapitole dvanácté. Méně se věnoval teoretickým přínosům práce a také vědním přínosům práce.

Význam práce pro rozvoj vědního oboru spatřuji především v systémovém vyjádření modelu a to v kontextu s novými požadavky oboru v informační a znalostní ekonomice.

Předložená práce má své místo v oblasti řešených disertačních prací v oboru.

Formální úprava disertační práce

Kriticky hodnotím některé citační nepřesnosti - neúplné citace u obrázkové částí a pouze jedinou vlastní publikaci uvádí v seznamu použité literatury.

Práce je napsána přehledně a velmi dobře a splňuje nároky na současné doktorské disertační práce.

Otázky do rozpravy:

1. V čem spatřujete použití metod umělé inteligence v generování fraktálních struktur?
2. Jaké další prostředky navrhujete na určení odolnosti vůči kryptografickým

metodám?

Závěr

Předkládanou práci doporučuji k obhajobě před příslušnou komisí a po úspěšném jejím obhájení udělit jmenovanému titul Ph.D. v uvedeném oboru.

V Brně 8. září 2012

prof. Ing. Jiří Dvořák, DrSc.
Vysoké učení technické v Brně
Fakulta podnikatelská
Ústav informatiky

Oponentský posudek disertační práce

Název disertační práce: Výzkum využití možností fraktální geometrie pro zabezpečení informačních systémů

Autor: Ing. Ivo Motýl
Oponent: doc. RNDr. PaedDr. Eva Volná, PhD.
Ostravská univerzita Ostrava

Téma práce a splnění cíle

Tato disertační práce se zabývá využitím principů fraktální geometrie v oblasti kryptografického zabezpečení komunikace v rámci informačních systémů. Z hlediska aktuálnosti lze konstatovat, že práce se zabývá aktuálním tématem ve zvolené oblasti a odráží potřebu nových netradičních metod.

Disertační práce splnila všechny sledované cíle, odpovídá oboru disertace a zabývá se perspektivní problematikou zapojení fraktální geometrie do oblasti informační bezpečnosti.

Přínos v oblasti poznání

Výsledky práce přinášejí nové pohledy na řešení problémů týkajících se zabezpečení v rámci informačních systémů. Navržené řešení vychází z oblasti interaktivních fraktálů vytvořených pomocí algoritmu TEA.

Publikační činnost disetanta je vyrovnaná a vztahuje se k období 2009 - 2012. Ing. Ivo Motýl je autorem či spoluautorem 24 publikací presentovaných zejména na národních a mezinárodních konferencích.

Přínos ve společenské praxi

V práci byly jednotlivé části navrženého systému s úspěchem testovány na odolnost vůči kryptoanalytickým metodám. Je zřejmé, že předložený návrh vychází ze zkušeností autora s realizací podobných problémů v praxi.

Formální úprava, publikace

Doktorská disertační práce má 119 stran, ke kterým jsou přidány 3 přílohy a životopis autora. V úvodní teoretické části autor popisuje problematiku týkající se fraktální geometrie

za účelem výběru vhodné skupiny fraktálů pro potřeby disertační práce. Tato část se zaměřuje na vysvětlení základních pojmů a metod použitých při řešení disertační práce.

V praktické části jsou uvedeny poznatky popisující chování a vlastnosti jednotlivých částí šifrovacích a dešifrovacích procesů a výstupy analýzy odolnosti navrženého systému vůči kryptoanalytickým metodám.

Práce je napsaná čtivou formou, má logickou strukturu a je na slušné jazykové úrovni. Rušivě však působí časté odkazy na předchozí a následující kapitoly. Některé obrázky nemají požadovanou kvalitu, např. obrázek 35.

Dotazy a připomínky

1. Ve vaší práci postrádám podrobnější rešeršní části. Současný stav řešené problematiky disertační práce je zpracován nedostatečně pouze na 2 stranách. Mohl byste proto ve stručnosti uvést, jakými dalšími metodami byla řešena daná problematika.

2. Mohl byste doložit svůj podíl na společných publikacích.

3. Mohl byste provést srovnání dosažených výsledků i s jinými přístupy.

Závěr

Předložená práce splňuje požadavky kladené na doktorskou disertační práci a to jak z pohledu teoreticko - metodologické úrovně, tak ve využitelnosti v praxi. Práce obsahuje původní výsledky.

Doporučuji předloženou disertační práci k obhajobě a rovněž doporučuji, aby na základě úspěšné obhajoby byla panu Ing. Ivo Motýlu udělena vědecká hodnost Ph.D. v oboru Inženýrská informatika.

V Ostravě 20.9.2012

doc. RNDr. PaedDr. Eva Volná, PhD.

Posudek disertační práce

Autor: Ing. Ivo Motýl, Fakulta aplikované informatiky, UTB ve Zlíně
Název práce: Výzkum využití možností fraktální geometrie pro zabezpečení informačních systémů

Aktuálnost tématu, obsah a struktura práce

V disertační práci je popisována a studována problematika využití zabývá využitím principů fraktální geometrie v oblasti kryptografického zabezpečení komunikace v rámci informačních systémů. Práce se skládá z 13ti kapitol. Obsahuje úvod do problematiky kryptologie, její implementace a následně i využití fraktální geometrie. Navržené postupy a metodiky jsou podloženy „experimentální" částí realizovanou v simulačním prostředí. Práce je podložena doktorandovou publikační činností, ale i dlouholetými zkušenostmi pracoviště doktoranda.
Z hlediska aktuálnosti lze konstatovat, že se práce zabývá aktuálním tématem v oblasti kryptologie pomocí fraktální geometrie a odráží potřebu nových netradičních metod v oblasti šifrování. Práci lze v tomto směru považovat za úspěšný krok.

Úroveň zpracování a splnění stanovených cílů

Na úroveň zpracování lze pohlížet ze dvou směrů a to ze směru grafického a formálního. V obou ohledech nelze práci nic vážnějšího vytknout. Z grafického hlediska je práce na velmi dobré úrovni.
Po formální stránce je práce velmi dobrá a splňuje všechny požadavky kladené na vědeckou práci. Obsahuje jak část teoretickou, tak simulační. Co se týče splnění cílů disertace, mám za to, že byly splněny.

Zvolené metody zpracování

V práci byla použita a popsána problematika využití využití zabývá využitím principů fraktální geometrie v oblasti kryptografického zabezpečení komunikace v rámci informačních systémů. Výstupy práce dizertanta byly rovněž publikovány na konferencích a workshopech. Použité metody a postupy jsou moderní a plně použitelné na problematiku v rámci práce.
Z těchto důvodů lze považovat použití zvolených metod za plně oprávněné a pro účely disertační práce dostačující.

Výsledky disertační práce a nové poznatky, které přináší

Vzhledem k faktu, že celá práce je postavena jako vyvážený celek teorie a aplikovaných algoritmů a v práci je uveden disertantův přínos, lze konstatovat, že práce obsahuje původní poznatky.

Připomínky a dotazy

V práci jsem se zaměřil na fakta a technickou stránku věci. V tomto směru mám následující připomínky a dotazy:

1) Po pravdě v práci není jasně vysvětleno, jak vlastně funguje vaše metoda. Prosím vysvětlete jasně a stručně podstatu věci.
2) Prosím specifikujte blíže co znamená unikátní a neunikátní klíč.
3) V práci postrádám hlubší porovnání se současnými kryptologickými metodami.

Závěr posudku

Disertant Ing. Ivo Motýl vypracoval a ověřil metody využitím principů fraktální geometrie v oblasti kryptografického zabezpečení komunikace v rámci informačních systémů. Problematiku související s disertační prací publikoval spolu se svým školitelem a kolegy na příslušných konferencích. Vzhledem k výsledkům z experimentální části soudím, že jde o řešení funkční a životaschopné, nicméně další výzkum by byl vhodný.
Ve své disertační práci prokázal Ing. Ivo Motýl schopnost samostatné tvořivé vědecké práce. Předložená disertační práce splňuje všechna potřebná ustanovení pro udělení titulu Ph.D. a tudíž ji doporučuji k obhajobě.

prof. Ing. Ivan Zelinka, Ph.D.
V Ostravě
Katedra informatiky
Fakulta elektrotechniky a informatiky
17. listopadu 15
VŠB-TU Ostrava