FAKULTA
APLIKOVANÝCH VĚD
ZÁPADOČESKÉ
UNIVERZITY
V PLZNI

odb. as. Ing. Kamil Ekštein, Ph.D.
Katedra informatiky a výpočetní techniky
Fakulta aplikovaných věd Západočeské univerzity
Univerzitní 22, CZ-30614 Plzeň
Tel.: (+420) 377 63 2406
E-mail: kekstein@kiv.zcu.cz

Hodnocení vedoucího diplomové práce

Bc. František Pártl

Návrh hashovacího algoritmu pro biometrický podpis uživatele

Diplomová práce Bc. Františka Pártla, jejíž zadání souvisí s vědeckovýzkumným projektem z programu *MPO Aplikace* aktuálně řešeným na Katedře informatiky a výpočetní techniky Fakulty aplikovaných věd Západočeské univerzity, se věnuje problému nalezení vhodného algoritmu tzv. *biometrického hashování*, tedy výpočetního postupu vedoucího k jednoznačné prosté projekci v tomto konkrétním případě audiovizuálního záznamu obličeje hovořící osoby do prostoru unikátních klíčů s cílem používat takto transformovaný multimediální obsah jako elektronický podpis zaznamenané osoby.

Jedná se o velice teoreticky náročné vědeckovýzkumné zadání, které vyžadovalo načerpat řadu znalostí a dovedností, které nejsou součástí běžné výbavy typického absolventa. Autor si nicméně s touto výzvou dobře poradil, čímž prokázal nejen své kvality, ale stal se i platnou součástí řešitelského týmu projektu, od jehož finálního produktu se očekává masivní komerční využití.

Autor práce je velmi nadaný, zodpovědný a pracovitý student. K práci přistoupil velice aktivně, důkladně prostudoval řadu komplikovaných pokročilých technik z oblasti zpracování (akustického) signálu, které nepokrývá (nebo ne zcela) běžná výuka v předmětech navazujícího magisterského studia informatiky. Vyhledal a přečetl řadu odborných publikací, např. teoreticky velmi náročných konferenčních příspěvků, z nichž čerpal poznatky potřebné k návrhu a implementaci hashovacího algoritmu. Na velmi vysoké úrovni byl i management projektu a implementace prostředky jazyka C++ v podobě jeho posledních publikovaných norem.

Spolupráci s autorem práce hodnotí vedoucí jako vzornou: Na konzultace docházel pravidelně, výborně připraven, a tak byly diskuse věcné a efektivní. Naneštěstí se v průběhu práce na řešení zadaného problému objevila celá řada problémů, z nichž tím nejzásadnějším byl fakt, že se autorovi ve spolupráci s vedoucím práce poměrně dlouho nedařilo vymyslet fungující prostou projekci transformovaného akustického signálu do libovolné obecné množiny klíčů. Autor implementoval značné množství různých transformačních algoritmů jen proto, aby zjistil, že získané zobrazení do množiny klíčů opět není prosté. I v této fázi práce autor psychicky vydržel, což hodnotím z pozice vedoucího jako jeden z velmi zásadních kladných elementů. I díky tomu se nakonec podařilo vhodnou transformaci „objevit".

Na připomínky vedoucího reagoval autor okamžitě a velmi ochotně požadované úpravy ihned zapracovával do software, resp. posléze do textu práce. Průvodní text práce byl dostatečně a včas konzultován.

Práce je původní. Autor při řešení zadání vycházel z dostupných materiálů, z literatury a diskusí s vedoucím práce, nicméně vzhledem k tomu, že žádné existující např. open-source řešení zadaného problému neexistuje, neměl šanci se ani inspirovat jiným produktem a musel vložit do realizace značný díl vlastní invence.

Celý velice rozsáhlý zdrojový kód díla je původním dílem autora, k implementaci využívá především aplikační framework Qt 5 a dále několik knihoven pro zpracování vstupního multimediálního záznamu a jeho akustické stopy (FFmpeg, KissFFT, atd.). Užití knihoven je zcela v souladu s trendy v oboru, neboť implementace např. FFT vlastními silami by byla zbytečná a zřejmě suboptimální.

Citace v textu i bibliografie na konci práce jsou provedené v souladu s požadavky. Uvedené zdroje literatury (30) jsou dostatečné a relevantní. Většinou jde elektronické dokumentace a tutoriály k použitým vývojovým nástrojům, frameworkům a v nich používaným technologiím, knihovnám, apod. a o články publikované na významných oborových konferencích, přičemž jejich výběr považuji za naprosto adekvátní.

Implementační část předloženého díla je plně funkční, vytvořené knihovny, mobilní aplikace pro sběr audio-vizuálních záznamů osob (multimediálních podpisů), program pro grid search optimálního nastavení hyperparametrů transformační techniky i demonstrační a ověřovací systém pracuje správně a je stabilní. Dosažená míra unikátnosti (tj. „prostosti zobrazení") transformace vstupního akustického signálu 82 % představuje *vynikající výsledek*, ač sama o sobě vlastně problém zcela neřeší (na to by musela být 100 %, což je patrně stejně nedosažitelné).

K vývoji byl použit jazyk C++ bez orientace na konkrétní platformu (autor používal při vývoji GNU/Linux). Implementace je velmi rozsáhlá (zhruba 43 tisíc řádek zdrojového kódu), zdrojový kód programového řešení je zapsán

čitelně, přehledně, za dodržení všech doporučení a zvyklostí. Autor si velmi libuje ve výrazových prostředcích, které nabízejí poslední normy jazyka C++ (C++17), a proto je značná část kódu zapsána s plným využitím generiky, šablon funkcí i tříd, lambda funkcí, apod. Syntaktická podoba těchto konstrukcí z hlediska čitelnosti a srozumitelnosti je ovšem poněkud diskutabilní (aspoň pro vedoucího práce) a domnívám se, že by stejně dobrého výsledku bylo lze dosáhnout i za použití méně extrémních výrazových prostředků jazyka C++, čímž by se zdrojový kód zpřístupnil většímu množství programátorů a zejména výzkumníků v oblasti zpracování digitálního signálu, kteří nemusejí použité syntaktické konstrukty znát, příp. spolehlivě ovládat. Chyba to ale určitě není.

Textová část díla má mírně větší rozsah než je obvyklé – včetně příloh 84 stran. Autorovo vyjadřování je čtivé a srozumitelné: Text je jasný, autor dobře ovládá a používá technickou češtinu a jeho myšlenky lze v textu dobře sledovat. Gramatické chyby se v textu prakticky nevyskytují, stejně jako překlepy či odchylky od typografických zvyklostí.

Grafická úroveň dokumentu je vynikající a naprosto profesionální, je vysázen v LaTeXu a autor se důsledně postaral i o ty nejmenší podrobnosti, mj. např. vektorové obrázky vysázel pomocí jazyka PGF/TikZ, čímž zajistil kontrolu LaTeXu nad velikostí a řezem písma popisků v obrázcích. Dokument působí mimořádně harmonickým dojmem.

Struktura textu odpovídá typu a rozsahu práce. Práce je dobře logicky strukturovaná a poměr jednotlivých částí je vyvážený. Text je vhodně doplněn obrázky, grafy, schématy a vzorci, které jej žádoucím způsobem obohacují a jsou vysázené v odpovídající kvalitě.

Drobnou výhradu mám k bibliografii, kde na str. 72, položka [28], autorovi „utekla“ konzistence grafické úpravy a jména autorů citované knihy jsou vysázena verzálkami namísto všude jinde používaných kapitálek. Také u titulů [16] a [26] se uchyluje k použití zkratky „et al.“ namísto vypsání jmen všech spoluautorů, což může být vnímáno jako neuctivé.

Autorem implementovaná technika transformace digitálního akustického signálu na kryptografický otisk je využita jako klíčová součást realizovaného řešení výzkumného projektu z programu MPO Aplikace, tzn. autorem dosažené výsledky jsou tedy přímo využitelné (a okamžitě využívané) v rámci „živého“, aktuálně řešeného projektu. O jejich užitečnosti, hodnotě a využitelnosti tedy nelze v žádném případě pochybovat.

Všechny body zadání byly splněny. Práce je bez jakékoliv pochybnosti vynikajícím inženýrsko-vědeckým dílem. Autor prokázal nejen výborné programátorské schopnosti, ale i mimořádný potenciál pro další vědeckou práci včetně naprosto nezbytné vlastnosti vydržet a ustát situaci, kdy se řešení problému neubírá směrem, který si řešitel vybral a naplánoval.

Práci bez výhrad **doporučuji k obhajobě** a hodnotím klasifikačním stupněm

„výborně“.

Ing. Kamil Ekštein, Ph.D.
KIV FAV ZČU

V Plzni dne 2. června 2020