Review of Master's Thesis

Student: Firc Anton, Bc.
Title: Applicability of Deepfakes in the Field of Cyber Security (id 23761)
Reviewer: Homoliak Ivan, Ing., Ph.D., DITS FIT BUT

1. Assignment complexity — **more demanding assignment**

Zadanie bolo obtiažnejšie vzhľadom na jeho šírku.

2. Completeness of assignment requirements — **assignment fulfilled**

3. Length of technical report — **exceeds requirements**

Práca obsahuje 90 latex-om vysádzaných strán, vrátane referencií; čo je podľa môjho odhadu blízko hornej hranici rozsahu. Keďže zadanie bolo široké a v mnohých bodoch voľné, študent sa snažil túto voľnosť využiť a spracoval veľké množstvo príbuzných oblastí a ich zdrojov.

4. Presentation level of technical report — **90 p. (A)**

Práca je pre čitateľa pochopiteľná, jednotlivé kapitoly na seba logicky nadväzujú. Rozsahy a prehľadnosť väčšiny kapitol sú prípustné, no niektoré kapitoly sú príliš verbalistické a určitá časť obsahu sa v nich opakuje. Vlastná práca má vedecko-experimentálny charakter, kde študent najskôr definuje výskumné otázky a potom ich empiricky skúma a adresuje.

Práca na druhej strane obsahuje aj niekoľko nepresností. Študent uvádza, že podľa zdroja [10] neboli žiadne úspešné pokusy o obídenie klasifikačných schopností biometrických systémov založených na hlasovom rozpoznávaní, no tesne pred tým cituje zdroj z konferencie BlackHat, ktorý taký útok uskutočnil na Apple Siri a MS Speaker Recognition.

V tabuľke 6.13 a data mining sekcii, študent analyzuje a zdôrazňuje existenciu korelácie dosiahnutého skóre pre originálne vzorky a deepfake vzorky. No treba si uvedomiť, že táto korelácia je očakávaný jav keďže cieľom deep fake vzoriek je napodobiť originálne vzorky. S týmto súvisí aj skúmaná otázka pýtajúca sa na vzorce podobnosti medzi originálnymi a deep fake vzorkami. Keby vzorce podobnosti v dosiahnutom skóre neexistovali, tak deep fake prístup nebude nikdy úspešný.

Je ťažké vyhodnotiť skutočný prínos experimentu popísaného v sekcii 6.5.2, ktorý využíva autorom vytvorený dataset pozostávajúci z piatich subjektov. Prezentované výsledky by mali ukazovať aj skóre pre "cudzích" užívateľov a to by malo byť porovnané s deep fake.

Študent vykonal dotazníkovú štúdiu, ktorá skúma klasifikáciu hlasových vzoriek človekom na deep fake alebo originále. Výsledkom štúdie bolo, že až 30% vzoriek bolo klasifikovaných nesprávne. Mám k tomuto dve poznámky. Vzorky som si prešiel a na prvý pohľad som zistil, že ich kvalita je silno zavádzajúci faktor, a preto mnoho respondentov nesprávne označilo originálnu vzorku v telefónnej kvalite za deep fake a deep fake v takmer bezstratovej kvalite ako originál. Druhá poznámka je, že problém klasifikácie reprezentujúci autentizáciu konkrétneho jedinca je iný než problém klasifikácie deep fake / originál, aj napriek tomu, že oba problémy pracujú s binárnou klasifikáciou.

5. Formal aspects of technical report — **90 p. (A)**

Práca je písaná v anglickom jazyku a pravopisne je na vysokej úrovni, aj napriek tomu, že nejaká chyba alebo nesprávne slovné spojenie sa sem tam v nej vyskytne.

Ďalej, niektoré obrázky ako napr. 3.1, 3.2, 6.1, 6.12, 6.14 plávajú v strede stránky, namiesto typograficky správnejšieho zarovnania na vrch alebo spodok stránky. Poznámky pod čiarou sú typograficky nesprávne.

Názvy referencovaných obrázkov a tabuliek v texte sú uvedené s členom, čo je nesprávne.

6. Literature usage **95 p. (A)**

Práca s literatúrou je na vyhovujúcej úrovni. Zvolené študijné prameňe sú relevantné a sú aj odlíšené od vlastných výsledkov. Práca obsahuje spolu 63 referencií, v ktorých je rozumné zastúpenie vedeckých článkov.

7. Implementation results **95 p. (A)**

Práca má pekný realizačný výstup. Experimenty a implementácia sú na vysokej úrovni.

8. Utilizability of results

Výsledky sú využiteľné vo výskume. Študent publikoval článok na konferencii Excel@FIT, kde bol aj ocenený.

9. Questions for defence

V práci niekoľkokrát študent spomína, že žiadny biometrický autentizačný systém založený na hlase neobsahuje detektor živosti. Ako by mohol taký detektor vyzerať?

Ako funguje transfer learning a čo je jeho najvčäšou výhodou?

10. Total assessment **95 p. excellent (A)**

Práca je štandardne obtiažneho zadania. Zadanie bolo splnené vo všetkých bodoch. Študent volil vhodnú literatúru, Práca poskytuje ucelené výsledky a realizačný výstup, ktorý je aj dôkladne diskutovaný. Celkovo prácu hodnotím stupňom A **(95 bodov)**.

In Brno 9 June 2021

Homoliak Ivan, Ing., Ph.D.
reviewer