BIOMETRIC FINGERPRINT LIVENESS DETECTION

Tomáš Váňa

Master Degree Programme (2), FEEC BUT

E-mail: xvanat00@stud.feec.vutbr.cz

Supervised by: Lukáš Smital

E-mail: smital@feec.vutbr.cz

Abstract: This paper deals with biometric fingerprint liveness detection. A software-based liveness detection approach using neural network is proposed. To distinguish between live and fake samples, three image quality features extracted from one image are used. The algorithm is tested on LivDet database comprising real and fake images acquired with three sensors.

Keywords: Biometric system, fingerprint, liveness detection, LivDet database, neural network

1. ÚVOD

Biometrický systém je složen z několika komponent (snímač, registrační modul, extraktor rysů, databáze a porovnávací modul). Každá tato komponenta biometrického systému ovšem představuje potencionální zranitelné místo. Tento článek je zaměřen na přímý útok proti biometrickému systému, který spočívá v přiložení umělého biometrického znaku na senzor. Metoda opatření spočívá v rozpoznání živosti prstu umožňující detekovat falešný otisk a následně ho odmítnou, čímž se zvýší robustnost systému a také jeho úroveň zabezpečení [2], [3].

2. DETEKCE ŽIVOSTI

V tomto článku byla zvolena softwarová metoda využívající přístupu založeného na hodnocení kvality obrazu s otiskem prstu. Obecně je totiž předpokládáno, že obraz pořízený falešným otiskem prstu bude mít rozdílnou (horší) kvalitu, než kdyby byl použit živý prst uživatele. Snímek otisku prstu pořízený umělým prstem obsahuje ve většině případů artefakty vzniklé pořízením otisku. Hlavní myšlenkou tohoto procesu je nalezení množiny charakteristik, které umožní vytvořit vhodný klasifikátor (v podobě neuronové sítě), pomocí něhož je na základě extrahované množiny charakteristik stanoveno rozhodnutí, zda na snímač byl přiložen živý nebo umělý prst [2].

2.1. VYBRANÉ PŘÍZNAKY

K rozpoznání živosti prstu je v tomto článku navrhnuta kombinace tří příznaků. Konkrétně se jedná o jeden příznak z článku [3], zbývající dva pochází z článku [2]. Předzpracování obrazu spočívá v segmentaci samotného otisku prstu za pomoci prahování. Pixely získané prahováním, které se navíc nacházejí v dostatečně blízké vzdálenosti od sebe, jsou sloučeny do jedné oblasti, jenž je nakonec aproximována elipsou za účelem získání pouze otisku prstu.

Prvním z nich je příznak Q_E, který měří rozložení energie ve frekvenční oblasti pomocí entropie. K extrakci energie ze spektra je použita skupina rovnoměrně rozložených pásmových propustí, které byly vytvořeny odečtením dvou po sobě jdoucích přenosových funkcí Butterworth filtrů typu dolní propust [1]. Vysokého hodnoty Q_E dosahují obrazy s kvalitním otiskem prstu (úzký tmavě červený prstenec energie ve výkonovém spektru), zatímco obrazy s nízkou kvalitou otisku prstu nabývají nízké hodnoty Q_E (rozprostření energie ve výkonovém spektru), viz obrázek 1.

Další dva příznaky (Q_{SPE} a Q_{GPE}) využívají k hodnocení kvality obrazu dostupnost původního obrazu a referenčního obrazu, který vznikne filtrací původního obrazu dolní propustí ve tvaru Gaussovy

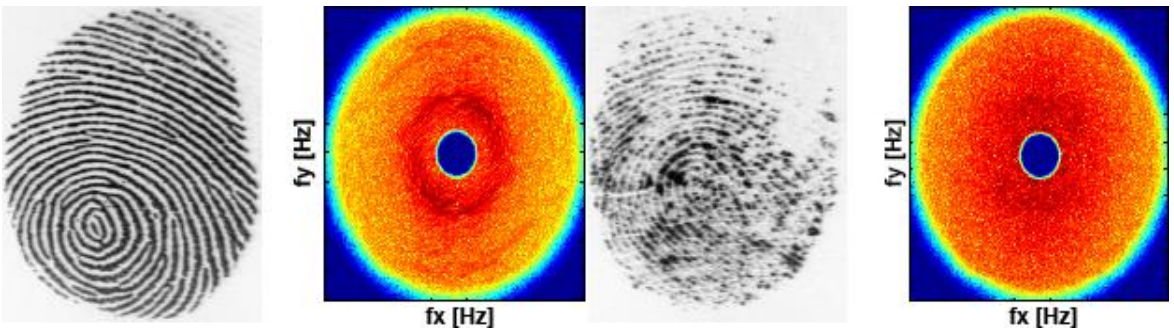
křivky (σ = 0,5). Velikost masky filtru byla zvolena 3 × 3 pixely [2]. Vlivem filtrace dojde v referenčním obrazu ke zkreslení. Příznak Q_{SPE} hodnotí kvalitu obrazu pomocí odchylky mezi fázovou složkou spektra původního obrazu a zkresleného obrazu dle rovnice 1:

$$Q_{SPE}(I, I_R) = \frac{1}{NM} \sum_{i=1}^{N} \sum_{j=1}^{M} \left| \arg(F_{i,j}) - \arg(F_{Ri,j}) \right|^2 . \quad (1)$$

K hodnocení kvality obrazu lze využít důležité vizuální informace získané z gradientů obrazu. Strukturní zkreslení v obrazu se projeví jako změna jeho gradientů [2]. Příznak Q_{GPE} hodnotí kvalitu obrazu na základě chyby ve fázi gradientu, viz rovnice 2:

$$Q_{GPE}(I, I_R) = \frac{1}{NM} \sum_{i=1}^{N} \sum_{j=1}^{M} \left| \arg(G_{i,j}) - \arg(G_{Ri,j}) \right|^2 , \quad (2)$$

kde mapa gradientů G je definována jako $G = G_x + iG_y$, G_x a G_y jsou gradienty dle osy x a y.



Obrázek 1: Otisk prstu vysoké kvality a jeho výkonové spektrum vlevo, vpravo je uveden otisk prstu nízké kvality spolu s jeho výkonovým spektrem [1].

2.2. ALGORITMUS ROZPOZNÁNÍ

Pro vlastní rozpoznání otisků prstů na pravé (živé) a falešné bylo v článcích [2], [3] využito lineární diskriminační analýzy. V tomto článku byl navržen klasifikátor v podobě vícevrstvé neuronové sítě. Konkrétně se jedná o dopřednou neuronovou síť se zpětným šířením chyby. Neuronová síť se skládá ze dvou vnitřních vrstev, každá obsahuje deset neuronů se sigmoidální aktivační funkcí. Výstupní vrstva je tvořena jedním neuronem s lineární aktivační funkcí. Hodnota z výstupní vrstvy je následně prahována za účelem získání binární odpovědi sítě na vektor příznaků získaných z klasifikovaného otisku prstu. K naučení sítě byl zvolen algoritmus gradientního sestupu s krokem učení 0,1. Velikosti prahů a vah neuronů byly zvoleny náhodně. Dále byly zvoleny následující parametry učení sítě: 1000 epoch učení, hodnocení výkonu sítě pomoci střední kvadratické odchylky.

3. TESTOVÁNÍ NAVRŽENÉHO ALGORITMU

Navržený algoritmus byl otestován na databázi LivDet 2009 obsahující pravé a falešné otisky prstů. Databáze je rozdělena na otisky prstů určených k naučení klasifikátoru a na otisky určené k testování. Ke snímání byly použity tři různé optické snímače [2]. Mezi falešné otisky prstů byly použity pouze ty otisky, které byly vyrobeny ze silikonu. Struktura databáze je uvedena v tabulce 1. Na obrázku 2 je uveden živý a falešný otisk pořízený snímačem Biometrika.

Výkon navrženého algoritmu je odhadnut za pomocí průměrné chyby klasifikace ACE (Average Classification Error), která je definována jako průměr hodnot FLR a FFR. Hodnota FLR (False Living Rate) představuje procento falešných otisků klasifikovaných jako živé, zatímco hodnota FFR (False Fake Rate) je procento pravých otisků klasifikovaných jako falešné. Výsledky rozpoznání jsou uvedeny v tabulce 2. Hodnoty FLR_2 a FFR_2 byly získány prohozením dat, testovací data sloužila k naučení klasifikátoru a data k naučení byla testována [3].

Snímač	Data k naučení (Pravý/Falešný)	Testovací data (Pravý/Falešný)
Biometrika	520/520	1473/1480
CrossMatch	310/310	930/930
Identix	250/250	750/750

Tabulka 1: Struktura databáze LivDet 2009.

Obrázek 2: Pravý otisk prstu vlevo, falešný otisk prstu (silikon) vpravo.

Snímač	FLR_1/FLR_2 [%]	FFR_1/FFR_2 [%]	ACE_1/ACE_2 [%]	ACE [%]
Biometrika	16,4/17,8	22,8/25,6	19,6/21,7	20,7
CrossMatch	19,0/14,8	26,6/21,3	22,8/18,1	20,5
Identix	15,6/12,8	33,6/19,1	24,6/15,6	20,1
Celkově	**17,0/15,1**	**27,7/22,0**	**22,3/18,5**	**20,4**

Tabulka 2: Výsledky rozpoznání živosti.

4. ZÁVĚR

Hlavním cílem tohoto článku byla realizace algoritmu s využitím trojice příznaků k rozpoznání živosti prstu na základě jeho otisku. Celková chyba klasifikačního algoritmu dosahuje hodnoty 20,4 %. Nejlépe byly klasifikovány otisky pořízené senzorem Identix, chyba 20,1 %. Z většiny chybně klasifikovaných otisků prstů byly spíše pravé otisky označeny za falešné než naopak. Navrženým algoritmem bylo u snímače Biometrika dosaženo chyby 20,7 %, zatímco chyba přístupu z článku [3] dosahovala vyšší hodnoty (26,5 %). V ostatních případech bylo dosaženo horších výsledků, jelikož použité příznaky nedokáží u zbylých snímačů dostatečně přesně rozpoznat živost.

PODĚKOVÁNÍ

Tento příspěvek vznikl za podpory projektu MŠMT LD14013.

REFERENCE

[1] CHEN, Y. *Fingerprint Quality Indices for Predicting Authentication Performance*. Springer [online]. 2005 [cit. 2015-01-02]. Dostupné z: http://link.springer.com/chapter/10.1007/11527923_17.

[2] GALBALLY, J., MARCEL, S. *Image Quality Assessment for Fake Biometric Detection: Application to Iris, Fingerprint, and Face Recognition*. IEEE Xplore Digital Library [online]. 2014 [cit. 2015-01-01]. Dostupné z: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6671991.

[3] GALBALLY, J. *A high performance fingerprint liveness detection method based on quality related features*. ScienceDirect [online]. 2010 [cit. 2015-01-01]. Dostupné z: http://www.sciencedirect.com/science/article/pii/S0167739X1000244X.