PRAKTICKÉ ASPEKTY INDOOR NAVIGAČNEJ APLIKÁCIE

Bc. Peter Juhas

Školiteľ: RNDr. Miroslav Opiela, PhD.

Ústav informatiky, Prírodovedecká fakulta UPJŠ, Jesenná 5, 041 01 Košice

In the past few years Global Navigation Satellite System (GNSS) has became very popular tool to navigate people all around the world. In the outside world GNSS is very precise and reliable form of outdoor navigation. Unfortunately this technique is not so accurate in indoor environments, thanks to degradation of satellite signals caused by thick walls and small deviation in localization via GNSS. Our thesis aims to improve indoor navigation solutions with focus on practical applicability and sustainability by exploring and improving existing methods of indoor navigation.

In our thesis we decided to compare indoor navigation algorithms with an emphasis on behavior of the sensors in the smartphone. We tested algorithms which are using accelerometer sensor as their primary source of data. To do correct testing, we proposed a template to test and verify accuracy and applicability of indoor navigation algorithms.

Literatúra:

1. Mendoza-Silva, G.M., Torres-Sospedra, J. and Huerta, J., 2019. A meta-review of indoor positioning systems. Sensors, 19(20), p.4507.
2. Džama J. Smartphone-based indoor navigation application. Master's thesis, Košice: P.J.Šafárik University, 2021.
3. Potorti, F. et al., 2021. Off-line Evaluation of Indoor Positioning Systems in Different Scenarios: The Experiences from IPIN 2020 Competition. IEEE Sensors Journal.
4. Vezočnik, M. and Juric, M.B., 2018. Average step length estimation models' evaluation using inertial sensors: A review. IEEE Sensors Journal, 19(2), pp.396-403.

UTILIZATION OF NEURAL NETWORK TRAINED ON PARTICULAR BUILDING IN INDOOR POSITIONING

Bc. Viktória Mária Štedlová

Školiteľ: RNDr. Miroslav Opiela, PhD.

Ústav informatiky, PF UPJŠ, Jesenná 5, 040 01 Košice

Since indoor navigation cannot be achieved solely by using a GPS, there are many types of research using various methods and sensors to make the navigation as close as possible to the real location of the user. In this work, we are presenting how can neural networks be used to utilize indoor navigation. We aim to do it for one specific building so we can use characteristic features of the building. We have decided to use magnetometer field features in combination with data from a smartphone camera for our study. Magnetometer field data is convenient to use since compared to other indoor localization methods it is unique from building to building caused by the presence of ferromagnetic materials and it has temporal stability which is very suitable for our purpose. While magnetometer data can be limited by their low discernibility, we have eliminated this problem by training LSTM neural network that uses time series data, which is more unique and reliable. For training, we used sequence data from trajectories that each represent part of specific corridors from our building.

Literatúra:

1. Mendoza-Silva, G.M., Torres-Sospedra, J. and Huerta, J., 2019. A meta-review of indoor positioning systems. Sensors, 19(20), p.4507.
2. 2. Noroozi, M. and Favaro, P., 2016, October. Unsupervised learning of visual representations by solving jigsaw puzzles. In European conference on computer vision (pp. 69-84). Springer, Cham.
3. 3. Qiu, X., Sun, T., Xu, Y., Shao, Y., Dai, N. and Huang, X., 2020. Pre-trained models for natural language processing: A survey. Science China Technological Sciences, pp.1-26.

IDENTIFIKÁCIA PODOZRIVÝCH FORENZNÝCH ARTEFAKTOV

Boris Hamadej

Mgr. Eva Marková

Ústav informatiky, Prírodovedecká fakulta UPJŠ, Jesenná 5, 040 01 Košice

Digitálna forenzná analýza sa stala nevyhnutnou súčasťou reakcie na počítačové bezpečnostné incidenty ako aj súčasťou vyšetrovania kybernetickej kriminality. Dôležitými krokmi forenzného vyšetrovania sú identifikácia digitálnych stôp potenciálnych útočníkov, ich zber, analýza a ich následné zdokumentovanie. V našej práci sa venujeme metódam a postupom na čo najpresnejšie identifikovanie podozrivých forenzných artefaktov v operačnom systéme Windows a ich efektívnemu využitiu pri analýze a detekcii anomálií. Ako náš modelový prípad používame „Prípad ukradnutej sečuánskej omáčky“ z portálu DFIR Madness. Tieto dáta sme predspracovali a na upravenom datasete sme otestovali niekoľko existujúcich metód na detekciu anomálií bez učiteľa, ako napríklad ECOD, IForest či PCA. Analyzovali sme výsledky a úspešnosť jednotlivých metód pri detekcii anomálií, čím sme získali lepší prehľad o možnostiach ich uplatnenia pri digitálnej forenznej analýze. Na základe našej analýzy sme vybrali najlepšie metódy a implementovali ich do jednoduchého nástroja, ktorý užívateľom poskytne možnosť vybrať si metódy, ktoré chcú použiť. Tento nástroj následne porovnáva čas behu jednotlivých metód a ich výsledky, čo užívateľom umožní lepšie porozumieť výhodám a nevýhodám jednotlivých metód a vybrať si z nich tie najvhodnejšie pre ich konkrétny prípad.

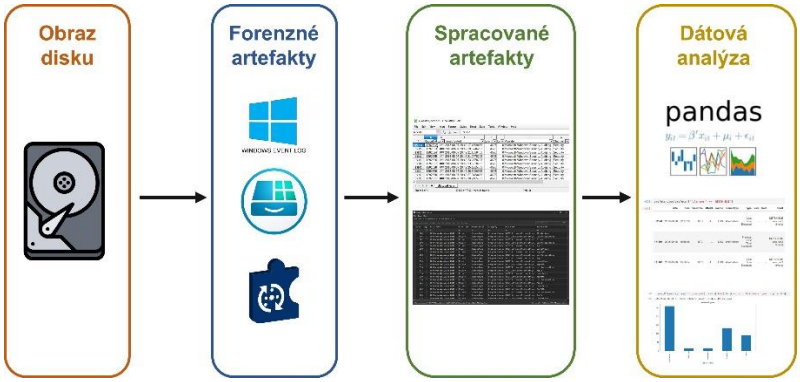
AUTOMATIZOVANÉ SPRACOVANIE FORENZNÝCH ARTEFAKTOV OPERAČNÉHO SYSTÉMU WINDOWS

Henrieta Paločková

Školiteľ: doc. RNDr. JUDr. Pavol Sokol, PhD.

Ústav informatiky, Prírodovedecká fakulta UPJŠ, Jesenná 5, 040 01 Košice

S narastajúcim trendom kybernetických hrozieb sa riešenie bezpečnostných incidentov stáva nepopierateľnou súčasťou každej organizácie. Tento proces zahŕňa niekoľko krokov počínajúc od zberu a zaisťovania digitálnych stôp, cez ich spracovanie, až po ich celkovú analýzu. Digitálne stopy sa vo svetle digitálnej forenznej analýzy zvyknú označovať aj ako forenzné artefakty. Sú to objekty, ktoré majú nejakú forenznú hodnotu a teda obsahujú dáta alebo dôkazy o tom, že sa niečo stalo a tak tvoria dôležitú súčasť forenznej analýzy [1]. Forenznú analýzu definujeme ako detailný proces vyšetrovania, detekcie a dokumentácie dôvodu, priebehu a následkov bezpečnostného incidentu [2]. Takáto analýza je často zdĺhavá a náročná z hľadiska neprehľadnosti dát. V tejto práci sa venujem výberu forenzných artefaktov, ktoré sú využiteľné vo forenznom vyšetrovaní a ich spracovaním pomocou nástrojov na parsovanie dát. Nad týmito dátami následne pomocou programovacieho jazyka Python vykonávam základnú analýzu za účelom získania štatistických informácii o zariadení, z ktorého boli dáta vyextrahované a o udalostiach, ktoré sa na ňom udiali. Výstupom tejto práce je nástroj, ktorý po navrhnutí, implementácii a vyhodnotení slúži na automatizované spracovanie forenzných artefaktov z operačného systému Windows a prispieva tak k zníženiu času analytickej činnosti. Na Obr. 1 je uvedený všeobecný postup spracovania forenzných artefaktov.



Obr. 1 Postup spracovania forenzných artefaktov

Literatúra:

1. Harichandran, Vikram S., et al. "Cufa: A more formal definition for digital forensic artifacts." *Digital Investigation* 18 (2016): S125-S137.
2. Daniel, Larry, and Lars Daniel. "Digital forensics for legal professionals." *Digital Forensics for Legal Professionals* (2012).

METHODS OF IMAGE MODIFICATION FOR NEURAL NETWORK IMAGE CLASSIFICATION

Martina Kuchtová

Školiteľ: RNDr. Miroslav Opiela, PhD.

Adresa: Ústav informatiky, Prírodovedecká fakulta UPJŠ, Jesenná 5, 040 01 Košice

Data pre-processing is a common approach to neural network-based image classification. We have decided to take a look at the impact that different methods of computer vision have on the results of classification. However, our focus was more on the image data that is fed into an already trained neural network, i.e. validation and testing data. The aim is to see if there are any methods that can be used to improve the accuracy of the results, despite the fact that the network has not been trained on such pre-processed data; conversely, which methods will give us significantly worse results than on the original data. These methods also allow us to simulate a wide range of different types of inputs, even those that are not ideal. We investigated the application of a range of compression and enhancement operations, filtering, segmentation and transformation, utilising image whitening and working with other colour models as well. By building on the analysis that we performed on 2 different image datasets and CNNs, we came to the conclusion that not all methods have the same impact on diverse data and networks. For a more accurate result, though, a more comprehensive analysis is required, involving a number of networks and data sets. Even so, there are methods that have a similar effect - in our case: they do not rapidly degrade the accuracy of the results, so that it remains roughly the same.

DETEKCIA SKÓRE V ŠÍPKACH POMOCOU ALGORITMOV POČÍTAČOVÉHO VIDENIA

Matej Uhrin

Školiteľ: RNDr. Miroslav Opiela, PhD.

Ústav informatiky, Jesenná 5, 04001 Košice

V dnešnej dobe dokáže počítač vidieť viac, ako si myslíme. Počítačové videnie výrazne prispieva k automatizácii procesov, ktoré donedávna vykonávali iba ľudia. Cieľom tejto práce je naučiť počítač lokalizovať šípku zapichnutú v šípkarskom terči a priradiť takejto lokalizácii príslušné skóre podľa pravidiel šípok. Využíva sa pri tom viacero techník počítačového videnia ako napr. geometrické transformácie, prahovanie, hľadanie aktívnych kontúr, detekcia hrán, čiar a rohov, ale aj bežné matematické operácie na obrázkoch. Správne a spoľahlivé fungovanie takejto detekcie môže byť základom softvérovej aplikácie, ktorá by mohla pomôcť šípkarom v ich tréningovom procese.

Obr. 1. Lokalizácia hrotu šípky v terči.

Literatúra:

1. SZELISKI, R. 2022. Computer Vision: Algorithms and Applications. 2nd ed. 2022 edition. Cham: Springer.

THREAT INTELLIGENCE MODEL PRE ŠKODLIVÉ EMAILY

Monika Rapavá

Školiteľ: Mgr. Eva Marková

Ústav informatiky, Prírodovedecká fakulta UPJŠ, Jesenná 5, 040 01 Košice

Indikátory kompromitácie (IOC) sú časti údajov, ktoré identifikujú potencionálne malicióznu aktivitu v sieti alebo v systéme. Threat intelligence (TI) tvorí množina takýchto nazbieraných dát, ktoré sú posúdené a použité v súvislosti s bezpečnostnými hrozbami a zraniteľnosťami. Preto zohrávajú dôležitú úlohu v oblasti kybernetickej bezpečnosti. V tejto práci analyzujeme indikátory kompromitácie v škodlivých e-mailoch a následne pomocou TI obohacujeme tieto nazbierané dáta. Výstupom tejto práce je súhrn štatistík z extrahovaných atribútov pred a po obohacovaní a taktiež hľadanie vzťahov medzi indikátormi kompromitácie z rôznych e-mailov pochádzajúcich z karantény Office365 na našej univerzite. Týmto spôsobom je možné zjednodušiť prvotnú analýzu škodlivých e-mailov, čo slúži ako pomoc pri včasnom reagovaní na útoky rôzneho druhu.

Literatúra:

1. LEGG, Phil; BLACKMAN, Tim. Tools and techniques for improving cyber situational awareness of targeted phishing attacks. In: 2019 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA). IEEE, 2019. p. 1-4.
2. CONTI, Mauro; DARGAHI, Tooska; DEHGHANTANHA, Ali. Cyber threat intelligence: challenges and opportunities. In: Cyber Threat Intelligence. Springer, Cham, 2018. p. 1-6.
3. COHEN, Aviad; NISSIM, Nir; ELOVICI, Yuval. Novel set of general descriptive features for enhanced detection of malicious emails using machine learning methods. Expert Systems with Applications, 2018, 110: 143-169.
4. TOUNSI, Wiem; RAIS, Helmi. A survey on technical threat intelligence in the age of sophisticated cyber attacks. Computers & security, 2018, 72: 212-233.

PROBLÉM K-CESTNÉHO VRCHOLOVÉHO POKRYTIA V GRAFOCH

Stanislav Švec

Školiteľ: RNDr. Rastislav Krivoš-Belluš, PhD.

Ústav informatiky, Prírodovedecká fakulta UPJŠ, Jesenná 5, 040 01 Košice

Cieľom tejto práce bola implementácia a vytvorenie interaktívnej vizualizácie vybraných algoritmov na riešenie problému *k*-cestného vrcholového pokrytia v grafoch s využitím vizualizačnej knižnice. Podstatou tohoto NP-úplného problému je nájsť v grafe *G* takú množinu vrcholov *S*, že každá cesta rádu *k* v grafe obsahuje aspoň jeden vrchol z *S*, pričom mohutnosť *S* je najmenšia možná. Tiež sme sa zaoberali tzv. problémom váženého *k*-cestného vrcholového pokrytia, teda modifikáciou problému, kedy je každému vrcholu priradené kladné reálne číslo (váha), pričom cieľom je, aby súčet váh v množine S bol čo najmenší. V rámci práce sme sa zamerali na algoritmus hľadania optimálneho riešenia pre ľubovoľný súvislý graf na báze hrubej sily, pričom sme sa ho neskôr pokúsili čiastočne optimalizovať s využitím binárneho vyhľadávania a techniky exponenciálneho prehľadávania z jednej strany. Všetky tri varianty algoritmu sme porovnali otestovaním na všetkých vzájomne neizomorfných grafoch až do rádu 9 a urobili sme pre nich vizualizáciu, schopnú znázorniť priebeh každej implementácie algoritmu pre zadaný graf. Tiež sme sa venovali aj polynomiálnemu algoritmu na nájdenie optimálneho riešenia problému váženého k-cestného vrcholového pokrytia v grafoch typu cesta na báze dynamického programovania s časovou zložitosťou $O(nk)$, pre ktorý sme tiež urobili vizualizáciu.

Literatúra:

1. B. Brešar, F. Kardoš, J. Katrenič, G. Semanišin: Minimum k-path vertex cover, December 2010, Discrete Applied Mathematics 159(12), DOI: 10.1016/j.dam.2011.04.008
2. B. Brešar, R. Krivoš-Belluš, G. Semanišin, P. Šparl: On the weighted k-path vertex cover problem, November 2014, Discrete Applied Mathematics 177:14–18, DOI: 10.1016/j.dam.2014.05.042

VPLYV ANTI-FORENZNÝCH TECHNÍK NA DIGITÁLNE FORENZNÉ VYŠETROVANIE

Zuzana Hennelová

Školiteľ: Mgr. Eva Marková

Ústav informatiky, Prírodovedecká fakulta UPJŠ, Jesenná 5, 040 01 Košice

Útočníci sa častokrát pokúšajú zahladiť za sebou stopy, ktoré zanechali v kompromitovaných systémoch. Chcú totiž chrániť svoju identitu aj svoje postupy, ktoré používajú na preniknutie do systému. Používajú tzv. anti-forenzné techniky na oklamanie rôznych automatizovaných nástrojov a na spomalenie a zavádzanie forenzných vyšetrovateľov pri analýze digitálnych stôp. V tejto práci popisujeme štyri vybrané anti-forenzné techniky a ich vplyv na forenzné artefakty. Je dôležité poznať tieto vplyvy, aby bolo možné efektívnejšie analyzovať zaistené stopy z bezpečnostného incidentu. Keďže forenzná analýza sa už nevykonáva iba manuálne a je snaha mnohé procesy automatizovať, je dôležité poznať vplyv anti-forenzných techník aj na výsledky automatizovane vyhodnotených dát. Pri manuálnej analýze má síce timestomping (zmena časových pečiatok) menší vplyv ako mazanie súborov ale pri automatizovanej detekcii anomálií sa ukázalo, že timestomping ovplyvňuje výsledky oveľa viac ako mazanie.