# Softwarové nástroje pro ověřování pravosti digitálních fotografií

Mariana Borisová

Bakalářská práce
2020



Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

# Univerzita Tomáše Bati ve Zlíně

## Fakulta aplikované informatiky

Ústav počítačových a komunikačních systémů

Akademický rok: 2019/2020

# ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

| | |
|---|---|
| Jméno a příjmení: | **Mariana Borisová** |
| Osobní číslo: | **A17010** |
| Studijní program: | **B3902 Inženýrská informatika** |
| Studijní obor: | **Informační technologie v administrativě** |
| Forma studia: | **Prezenční** |
| Téma práce: | **Softwarové nástroje pro ověřování pravosti digitálních fotografií** |
| Téma práce anglicky: | **Software Tools for Verifying the Authenticity of Digital Photographs** |

## Zásady pro vypracování

1. Vypracujte literární rešerši na dané téma.
2. Srovnejte možnosti dostupných softwarových nástrojů pro ověřování pravosti digitálních fotografií.
3. Popište metody, s jakými dané nástroje pracují.
4. Připravte vhodné vzorky upravovaných fotografií pro otestování vybraných nástrojů.
5. Otestujte spolehlivost vybraných nástrojů na připravených vzorcích, přičemž se zaměřte na neplacené služby.
6. Doporučte návod, jak postupovat při podezření na nepravost digitální fotografie.

Rozsah bakalářské práce:
Rozsah příloh:
Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam doporučené literatury:


1. DOBEŠ, M. *Zpracování obrazu a algoritmy v C#*. Praha: BEN – technická literatura, 2008.
2. FREEMAN, M. Fotografie v praxi: digitální úpravy. Brno: Zoner Press, 2012.
3. MURRAY, J. D a W. VANRYPER. *Encyklopedie grafických formátů II*. Praha: Computer Press, 2001.
4. KASÍK, P. Nenechte se napálit fotomontáží. Odhalte, co je na fotce upraveného. In: *Technet.cz* [online]. 2014 [cit. 2019-11-11]. Dostupné z: https://technet.idnes.cz/fotomontaze-hoax-fake-photoshop-doo-/software.aspx?c=A090317_114241_software_pka
5. NEFF, O. VerifEyed po roce a půl. In: *DigiNEFF* [online]. 2012 [cit. 2019-11-11]. Dostupné z: https://digineff.cz/verifeyed-po-roce-a-pul
6. Four Free Fake Image Detector – Analyze Photoshopped Photos. In: *Gecko&Fly* [online]. 2019 [cit. 2019-11-11]. Dostupné z: https://www.geckoandfly.com/10023/analyze-photoshopped-photos-with-fbi-csi-and-cia-fotoforensics-software


Vedoucí bakalářské práce: **doc. Ing. František Gazdoš, Ph.D.**
Ústav řízení procesů

Datum zadání bakalářské práce: **19. prosince 2019**
Termín odevzdání bakalářské práce: **27. května 2020**


**doc. Mgr. Milan Adámek, Ph.D.**
děkan

**doc. Ing. Martin Sysel, Ph.D.**
garant oboru

Ve Zlíně dne 19. prosince 2019

**Prohlašuji, že**

- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

**Prohlašuji,**

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne 10.8.2020

Mariana Borisová v. r.
podpis diplomanta

## ABSTRAKT

Bakalářská práce se zabývá softwarovými nástroji pro ověřování pravosti digitálních fotografií. První část je tvořena rešerší o článcích obsahující toto téma, popisem jednotlivých nástrojů a metod, které využívají. V druhé části jsou představeny autorčiny zkušenosti s testováním vybraných nástrojů na vlastních vzorcích upravovaných fotografií. V závěru práce je provedeno srovnání výsledků všech nástrojů a jejich ohodnocení, s jakou spolehlivostí pracovaly a také stručný návod, jak postupovat při podezření na nepravost fotografie.



Klíčová slova: digitální fotografie, ověřování pravosti, fotomontáže, softwarové nástroje.



## ABSTRACT

This bachelor thesis is focused on software tools used for verification of the authenticity of digital photographs. The first part od this thesis consist of the search on articles about the given topic and the description of individual tools and methods they use. The second partpresents the author's experience with testing selected tools on their own samples of edited photographs. In conclusion, all of the results of all toys are compared and evaluated, how reliable they were. In the end is a brief guide on how to proceed if a photo is suspected.



Keywords: digital photograph, authenticity verification, fake photos, software tools.

Tímto bych chtěla poděkovat vedoucímu doc. Ing. Františku Gazdošovi, Ph.D. za jeho cenné rady, které mi poskytoval při zpracování mé bakalářské práce a za čas, který mi věnoval.

Prohlašuji, že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

# OBSAH

# ÚVOD

Na internetu jsme obklopeni obrovským množstvím informací. Tyto informace však nemusí být vždy pravdivé a mohou sloužit pouze jako jednoduchý zdroj výdělku. K tomu, abychom dokázali vydělat slušný balík peněz, mnohdy stačí pouze zajímavý a poutavý titulek, který nelze přejít bez povšimnutí. Většina lidí se ani nezdržuje tím, aby si článek důkladně pročetli a ihned jej sdílí na sociálních sítích a desinformace se tak šíří raketovou rychlostí. Nejenom klamné informace, ale i fotografie a videa napomáhají k tomu, aby se po síti šířily lži, kterým mnoho lidí jednoduše uvěří. Na druhou stranu máme však výhodu, že v dnešním světě existuje mnoho nástrojů, díky kterým můžeme zkusit pravost ověřit. Právě díky své přesvědčivosti jsou fotografie velmi často využívány k manipulaci. Nemusí vždy jít o závažné věci, mnohdy se jedná pouze o žert, jindy však fotomontáž může překročit hranici a vést k dezinformaci či vydírání. S důležitostí ověřování se můžeme setkat v mnoha okruzích. Ať už se jedná o politiku, média, pojišťovnictví a v některých případech i kriminalistiku. Odhalení fotomontáže nám mnohdy může ušetřit spoustu peněz a problémů.

Cílem této práce je objevit a prozkoumat běžně dostupné nástroje pro ověřování pravosti digitálních fotografií a otestovat jejich spolehlivost. V teoretické části bude vypracována literární rešerše na toto téma. Ve stručnosti se podíváme do minulosti na to, jak vypadaly fotografické montáže před desítkami let, jak se vyvíjely a jak vypadají nyní. Dále se pak seznámíme s nástroji a jejich dovednostmi. Konkrétně zde vyzkoušíme 4 online nástroje, které jsou volně dostupné na internetu. Blíže se zaměříme, jakým způsobem s nimi pracovat a na metody, dle kterých odhalují na fotografiích různé nesrovnalosti.

V praktické části se pak zaměříme na spolehlivost a vyhodnocení funkčnosti nástrojů. K otestování použijeme mnou připravené vzorky fotografií. Na závěr práce si řekneme pár tipů a rad, jak postupovat při podezření na nepravost digitální fotografie.

# I. TEORETICKÁ ČÁST

# 1 REŠERŠE TÉMATU

V článku [1] na portále idnes.cz se můžeme dočíst o tom, jak a proč vznikají fotomontáže. Na fotomontáže můžeme narazit v novinách, na sociálních sítích i v marketingu. Vytvořit koláž, inscenaci nebo retuš nebylo nikdy jednodušší, proto je dobré vědět, jak tyto falzifikáty odhalit. Fotografie jsou hojně využívaným prostředkem k manipulaci, protože je na první pohled vidět, čeho se týká. V článku je zmíněno i několik důvodů, proč montáže vznikají. Mezi hlavní důvody řadíme politický záměr, dezinformaci, ale také z recese, pro pobavení a někdy i k vydírání. Nechybí zde ani pár rad, jak fotomontáž odhalit. Tyto rady jsou shrnuty v poslední části této bakalářské práce. Jsou zde také popsány čtyři typy nejčastější fotomanipulace, mezi které patří retuš, koláž, inscenace a falešný kontext. Když k fotografii přidáme popisek, který nepravdivě popisuje dění na ní, jedná se o falešný kontext. Je poměrně snadné ho odhalit, stačí jen zapátrat na internetu a pokusit se najít stejný obrázek a zjistit, kdy a v jakém kontextu byl pořízen. V tomto případě tedy nemusíme do fotografie nijak zasahovat. Když chceme z fotografie smazat nějakou část, nebo upravit osobu na ní, jedná se o retuš. Díky retuši, klonovacím a vyhlazovacím nástrojům dokážeme poměrně ve velké míře změnit původní obsah fotografie. Hojně se využívá při zdokonalování křivek modelek a celebrit. Další praktikou pro manipulaci je vytvoření koláže. K její výrobě jsou potřeba minimálně dvě fotografie, se kterými se dále pracuje. Pokud fotografie vznikly ve stejný čas a na stejném místě, je velmi těžké rozpoznat, že se nejedná o autentickou fotografii. Naaranžovaná falešná situace neboli inscenace, je odhalitelná nejhůře. Je však finančně náročnější než předchozí metody, proto se s ní v praxi nesetkáváme až tak často. [1]

Na webové stránce www.digineff.cz nalezneme článek [2] od autora Ondřeje Neffa, který zde popisuje metody, kterými lze odhalit nepravost fotografie. Zmiňuje zde také software s názvem VerifEyed, díky kterému lze pravost fotek ověřit. I sebemenší úprava digitální fotografie zanechá ve struktuře digitálního obrazu stopu. Princip detekce tedy spočívá v hledání nepřirozených souvislostí uvnitř obrazu. Mezi metody sloužící k odhalení patří například detekce nekonzistence chromatických vad, detekce několikanásobné JPEG komprese, detekce nekonzistentního šumu, duplikovaných oblastí nebo detekce založená na druhové analýze zdrojového zařízení. Všechny tyto vyjmenované metody lze používat v několika odvětvích. Jsou jimi například pojišťovnictví, bankovnictví, logistika, státní správa, ale i v méně důležitých sférách, jakými jsou internetové seznamovací portály apod. [2]

Fungování softwaru VerifEyed popisují jeho vývojáři Babak Mahdian a Radim Nedbal v rozhovoru pro český portál www.lupa.cz [3]. Aplikace dokáže dle slov Mahdiana s téměř 100% jistotou zjistit, zda byl snímek či naskenovaný dokument pozměněn. V ojedinělých případech umí také rozpoznat, zdali je daná fotografie stažená z internetu či nikoliv. Nápad vytvořit aplikaci, která toto dokáže, se stvořil po shlédnutí tutoriálů na YouTube, které radily, jak spáchat pojistný podvod například pomocí změny důležitých údajů ve skenovaných dokumentech a fotografiích. [3]

Na internetu nalezneme také články, ve kterých jsou zmíněny konkrétní online nástroje pro ověření pravosti fotografií. Jeden z takových článků nalezneme na webové stránce www.stopfake.org [4]. Je zde zmíněn například bezplatný nástroj Findexif.com, kterým můžeme odhalit, kdy a jakým přístrojem byla fotografie pořízena. Dále web FotoForensics, který díky analýze chyb komprese, dokáže rozpoznat změny v obraze. Poté je zde zmíněn i Google Search by Image a TinEye, které slouží pro zpětné vyhledávání fotografií na internetu. Způsoby vyhledávání a testování jednotlivých nástrojů se budu zabývat v dalších částech této práce. [4]

Pět jednoduchých kroků, jak spolehlivě ověřit fotografii na internetu zmiňuje Tomáš Pika ve článku [5] pro portál www.houpaciosel.cz. Žádný z těchto pěti kroků není sám o sobě stoprocentní, ale pokud jich využijeme většinu, nejlépe všechny, může se nám s velkou jistotou podařit falešnou fotografii odhalit. Stěžejním bodem je zjistit původ dané fotografie. Dále pak ověřit zdroj a EXIF data. Do těchto informací řadíme datum zachycení, typ fotoaparátu, druh závěrky, expozici, GPS informace a mnohé další. Je také vhodné ověřit místo, kde mohla pravděpodobně být fotografie pořízena. V neposlední řadě nám může pomoci odhalit původ fotografie očitý svědek, který celou situaci viděl a zažil, ovšem zjistit autora fotografie či svědky, může být v některých případech velmi těžké, spíše až nemožné. [5]

Náklady na vytvoření fotomontáže jsou v dnešní době skutečně minimální. Stačí na to několik minut (nebo hodin, pokud chceme, aby byl výsledek co nejdokonalejší) a pokročilý program pro úpravu bitmapových dat. Pochopitelně lze využít například i obyčejnější programy jakými jsou Gimp nebo PaintShop Pro. V praxi se nejčastěji používá Photoshop od firmy Adobe. Pokud bychom chtěli někomu znepříjemnit život, určitě bychom si na kvalitě fotomontáže dali opravdu záležet. Některé obrázky jsou však zcela neškodné a mají za úlohu nás pouze pobavit a je na první pohled zřejmé, že se jedná o fotomontáž. [1]

Velký rozmach při ověřování pravosti fotografií nastal kolem roku 2010. Na jeden upravený digitální snímek tehdy připadalo 2500 pojistných událostí. O dva roky později na jeden snímek vycházelo už 500 až 700 událostí. Rychlý nárůst těchto podvodů nemohl zůstat bez povšimnutí. Babak Mahdian v roce 2008 založil firmu ImageMetry s.r.o., se kterou v roce 2011 vyhrál v soutěži Česká hlava v kategorii Industrie. Dále vyvinul software VerifEyed a za tento projekt získal ocenění od několika předních organizací, včetně ceny Next Idea města New York (2011). [6]

V oblasti pojišťovnictví je v nynější době zaznamenáno mnohem více upravených fotografií, než tomu bylo v dřívějších dobách. Napomáhá tomu rozvoj všech možných technologií sloužících právě k úpravě fotografií. Cesta k vytvoření tohoto softwaru nebyla z počátku jednoduchá. Mahdian uvádí, že pro úplné pochopení potřeb koncových uživatelů, museli vývojáři spojit síly s partnery z pojišťovacího sektoru a navzájem si vyměňovat zkušenosti. Pouze tato spolupráce dokázala vychytat co nejvíce možných chyb a vytvořit co nejlepší software pro banky a pojišťovny. V diskuzi byl také systém pro běžného uživatele, který ovšem pracuje na jiném principu než obdobný pro větší instituce. Bylo to z důvodu ochrany před hackery, kteří se snažili zjistit, na jaké bázi tento systém funguje. [6]

Nejen banky a pojišťovny mohou tuto službu využívat. Prospěšná je i pro OSN a další mezinárodní organizace, které řeší pravost digitálních záznamů hlavně skrze válečné konflikty. V České republice pomáhá tento systém v Ústavu teorie informace a automatizace, který se snaží Kriminalistickému ústavu přinést nástroj, který jim pomůže s analýzou fotografií a zlepší kvalitu videí. Dalším úspěchem pro Mahdiana byla Prémie Otta Wichterleho pro rok 2013, kterou Akademie věd uděluje svým nejnadanějším pracovníkům do 35 let. [6]

Za zmínku stojí také videa, které se staly nástrojem pro vytváření falešných skutečností. Tyto videa jsou známé pod anglickým názvem Deepfake. Deepfake neboli hluboký podvod je vytváření obrazů či videí zobrazující falešný obsah. K vytvoření takového klamného videa je zapotřebí vlastnit špičkový počítač s výkonnými grafickými kartami. Samotná technologie je založená na bázi umělé inteligence, kdy počítač obdrží velký objem podkladových obrázků a zvuků cílové osoby za účelem jejího napodobení. S využitím dostatečného počtu těchto algoritmů můžeme vyrobit video s vyobrazením osoby hovořící prakticky o čemkoli a chovající se jakkoli. [7]

Poprvé se tato videa začala objevovat před pár lety, jedná se tedy o poměrně čerstvou záležitost, jejíž kvalita se neustále vyvíjí a roste. Existují takzvané „Deep Video Portraits“, které

působí už velmi realisticky. Jde o reprodukci pohybů, výrazů obličeje a řeči jedné osoby za pomoci tváře osoby druhé. Tato technika spočívá v tom, že dokáže rozpoznat, co tvoří obličej, obočí, koutky úst a pozadí ve videu osoby, kterou chceme napodobit. Následným sledováním těchto orientačních bodů na námi vytvořeném videu dokážeme zkreslit obličej napodobované osoby do pohybů a výrazů, kterých chceme dosáhnout. V konečném výsledku se tedy osoba, kterou chceme napodobit, chová a tváří naprosto totožně s obličejem ze zdrojového videa. Systém je tak dobře vyvinutý, že dokáže pracovat i se stíny za konkrétní osobou. [8]

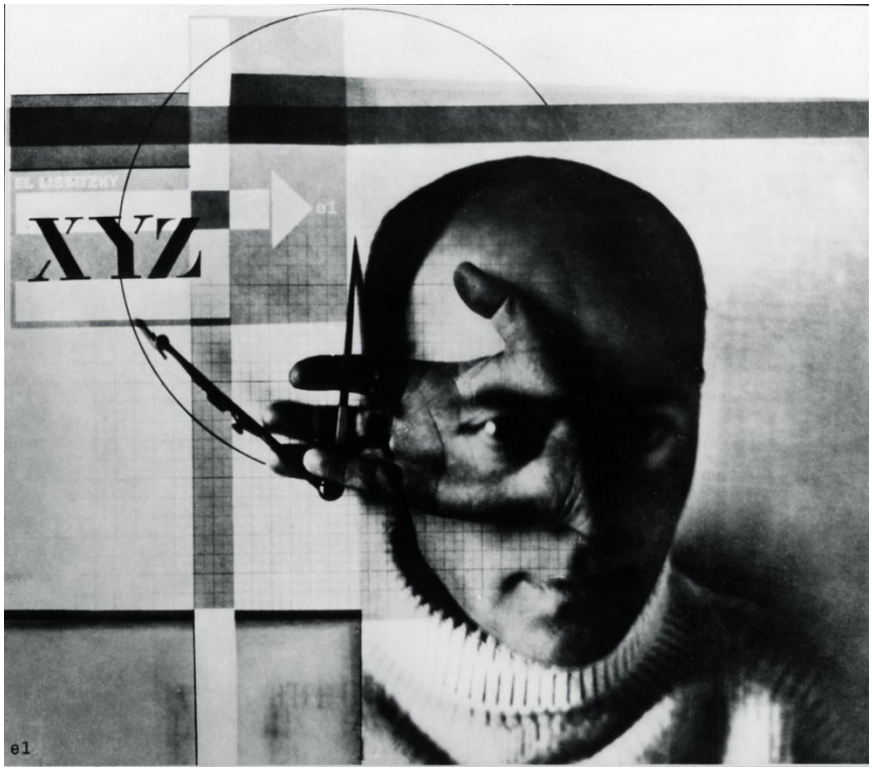
Je více než jasné, že je zde nová technologie, kterou si donedávna nedokázal nikdo z nás ani představit. Videí s klamným obsahem a negativním vlivem bude stále více, proto bychom si měli dávat pozor, z jakých zdrojů čerpáme informace. Naštěstí se však rozrůstá vývoj technologií a způsobů k jejich detekci. [9]

## 1.1 Stručná historie a současnost fotografických montáží

Fotografická montáž v sobě kombinuje různé podoby skutečnosti a tím vytváří novou skutečnost. Využití fotografické montáže zaznamenáváme již před rokem 1900. Patřili k nim nejenom fotografie z bojišť, ale také rodinné fotografie, ze kterých nenápadně mohl zmizet nepohodlný člen rodiny. Stalo se tak i v roce 1889, kdy se korunní princ rakousko-uherské monarchie Rudolf zastřelil spolu se svou sedmnáctiletou milenkou. Jeho otec František Josef II. ho poté nechal ze všech rodinných fotografií „vyretušovat“. Známou fotomontáží je také snímek bojiště ze 2. světové války, kdy původní obloha je zcela bílá, zatímco na svět se dostala fotografie rámovaná těžkými mračny. Postupné uvolňování morálky v poválečných letech přineslo do výtvarné fotografie doslova masivní nástup tvůrců, kteří se fotografickou montáží zabývali. Jako vzor pro ostatní tvůrce působil Sam Haskins, který zdůrazňoval ženské tělo s neobvyklými artefakty. Mezi českými tvůrci můžeme v poválečném období slýchat jména jako je Jan Šplíchal nebo Jiří Škoch. [10]

Dále můžeme zmínit autory z Ruska, kterými jsou Alexandr Rodčenko a El Lisickij, kteří vytvářeli experimentální fotomontáže s geometrickými prvky. Fotomontáže zasahovaly také

do politiky. Berlínský umělec John Heartfield se svou fotomontáží Adolfa Hitlera vysmál německému šovinismu. Jeho nejznámější práce je z emigrace proti hitlerovské třetí říši. [11]




*Obrázek 1: El Lisickij – Autoportrét Konstruktér (1924) [12]*

*Obrázek 2: John Heartfield - Adolf Superman (1932) [13]*

Mezi autory z domácí půdy můžeme zařadit například Jindřicha Štýrského, který pomocí seskupení různých předmětů dokázal navodit mnohovýznamové a mnohdy i poetické situace. Často hledal inspiraci na poutích a v cirkusech. Dalším významným českým autorem je Karel Teige, který vytvořil přes tři sta surrealistických koláží. [11]

Přesuneme-li se do 21. století, nalezneme již autory, kteří pracují s digitálním obrazem. Německá fotografka Loretta Lux do své tvorby použila dětské portréty bez výrazných emocí. Děti na výsledných kolážích působí zasněně, skoro až jako z jiného světa. Velmi zvláštní koláže vytvořil také čínský autor Daniel Lee. Jeho soubor Manimals v sobě skrývá slova Man (člověk) a Animal (zvíře). A jak je již z názvu patrné, dílo spojuje člověka a zvíře. Podle čínského zvířetníku je totiž každému kalendářnímu roku přiřazeno konkrétní zvíře, které charakterizuje povahu a vlastnosti lidí narozených v daném roce. Jak můžeme vidět na obrázku níže, Lee zkombinoval tváře lidí narozených v konkrétních letech s příslušnými zvířaty dle čínského zvěrokruhu. [11]

*Obrázek* 3*: Karel Teige – Koláž č. 198 (30. léta 20. století) [14]*

*Obrázek 4: Daniel Lee - Year of the Rat (1993) [15]*

*Obrázek 5: Nathan Baker - Scooter Shop (2003) [16]*

Američan Nathan Baker zaznamenává pracovní procese pomocí velkoformátové kamery na negativní materiál. Zachycuje vždy pouze jednu osobu z jednoho úhlu pohledu. Výsledný záběr vyobrazuje interiér obchodů či dílen, kde se objevuje pouze jedna osoba, ale při více činnostech. [11]

Sama jsem podobný typ montáže zkoušela vytvořit. Konkrétně jsem se fotila na více místech v knihovně. Vznikl z toho podobný obraz jako od autora Nathana Bakera.

*Obrázek 6: Vlastní tvorba*

Mezi české autory z tohoto období bychom mohli zařadit umělce Jiřího Davida. Ten vytvořil cyklus Bez soucitu. Vlivným osobnostem (např. Václavu Havlovi) přidal na tvář slzy. Zajímavostí tohoto díla je, že David vybíral pouze osobnosti mužského pohlaví, aby poukázal na fakt, že je obtížné zachytit muže při projevu emocí. [11]

Úprava fotografií je v současné době velmi probírané téma. Často si klademe otázky, jestli fotografie upracovat či neupravovat, zdali upravená fotka ještě ukazuje realitu a do jaké míry je vyretušovaná fotografie pravá. Dle mého názoru by měla být fotografie upravená pouze do té míry, kdy úpravy nebudou zřejmé na první pohled. Jednoduše řečeno, aby laik neměl šanci rozpoznat, že je fotografie do jisté míry vylepšená. Záleží samozřejmě také na daném fotografovi a jeho osobním stylu a vkusu. Existují fotografové, kteří se cíleně snaží, aby

fotografie byla viditelně upravovaná. Takovýto typ úprav se hodí spíše do abstraktně zaměřených děl, než například do svatebních fotografií.

Lain Stanley ve svém článku o upravených fotografiích zmiňuje několik důvodů, proč si myslí, že fotografie upravená ve Photoshopu nutně neznamená, že ji musíme považovat za nepravou. Kupříkladu černobílé fotografie krajinek od amerického fotografa Ansela Adamse taky nepovažujeme za nepravé z důvodu, že nejsou barevné. [17]

Fotografie níže, pořízená v roce 1942, je jasným důkazem, že tento autor prostě fotit černobíle chtěl, protože v této době již barevný film k dispozici byl. Ovšem nyní by zřejmě nebyl proslulý svými černobílými fotografiemi.

*Obrázek 7: Ansel Adams - The Tetons - Snake River (1942) [18]*

Moderní fotoaparáty a zařízení nám pomáhají vytvářet neuvěřitelné věci. Jednou z nich je fotografování pomocí dlouhé expozice. Díky této funkci lze dosáhnout iluzi plujících mraků po obloze nebo třeba tekoucí vody. Pak už stačí jenom správně nastavit fotoaparát a pár minut si počkat na nádherný výsledek. [17]

Stále si však klademe otázku, jsou tyto fotografie skutečné? Takto přece mraky nevypadaly ve chvíli, kdy fotograf zmáčkl spoušť. Názor ať si každý udělá sám.

# 2 VYBRANÉ NÁSTROJE PRO OVĚŘOVÁNÍ PRAVOSTI DIGITÁLNÍCH FOTOGRAFIÍ

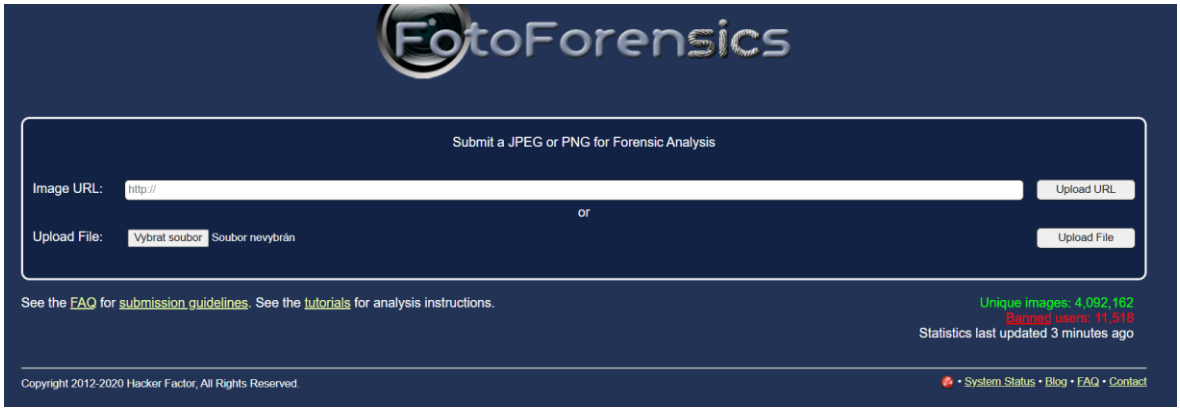
Nástroje pro ověřování pravosti digitálních fotografií se v posledních letech velmi rozšířily. Důvodů, proč fotografie ověřovat stále přibývá, proto je dobré mít alespoň malý přehled o základních nástrojích a principu jejich fungování. Do této bakalářské práce jsem vybrala čtyři nástroje, které jsou dostupné zdarma a zmíním zde dva, za jejichž služby je nutné zaplatit. Nejvíce doporučované a nejpoužívanější jsou FotoForensics a Forensically. Jejich zdánlivě podobný název nás může nabádat k myšlence, že fungují oba stejně. Opak je ale pravdou a v mnohých funkcích se od sebe tyto dva nástroje liší.

Než se pustíme do samotného zkoumání fotografie, můžeme její originál nejprve zkusit najít na jiných zdrojích. Jedním z největších vyhledávačů obrázků je Google Images. Hlavní výhodou je jeho obrovská webová databáze. Právě díky ní je Google nejlepší detektor obrazu při zpětném vyhledávání původního obrazu. Celý proces je velmi jednoduchý a nezabere víc než pár minut. Mezi další obdobné vyhledávací moduly můžeme zařadit Bing Image Match, Yandex image nebo TinEye, který ovšem není tak velký, jako Google Images, a z toho důvodu nedokáže poskytnout tak přesné výsledky. [19]

V některých případech nám bohužel samotné zpětné vyhledávání obrazu nepomůže a my nedostaneme uspokojující výsledek. Proto musíme sáhnout po jiných nástrojích, které nám umožní zjistit, zda bylo s obrázkem digitálně manipulováno.

## 2.1 FotoForensics

FotoForensics poskytuje přístup k nástrojům pro zkoumání fotografií jak amatérům, tak profesionálům. Pomocí použitých algoritmů může kdokoliv zkusit zjistit, zdali bylo s fotografií jakýmkoliv způsobem manipulováno. V některých případech dokáže i určit, jak byl obraz upraven. Cílem tohoto online nástroje je zjednodušit proces hodnocení detailů na obraze. Program se snaží co nejvíce poukázat a specifikovat místa na fotografii, které by mohly být změněny. Odvádí práci, kterou by nebylo schopné lidské oko vidět. Funguje podobně jako mikroskop. Pomůže nám rozklíčovat data, ale sám o sobě nevyhodnotí, zdali je obrázek upravený či nikoli. [20]

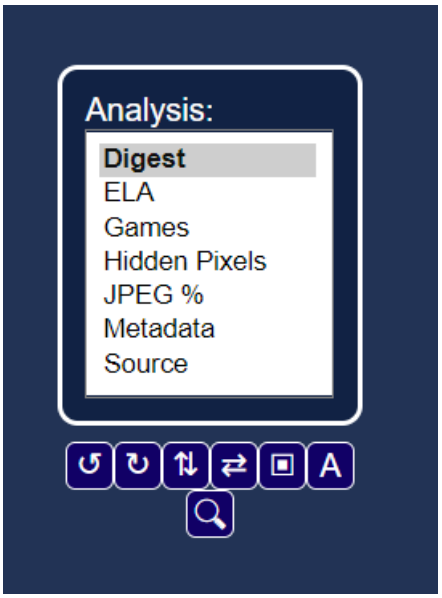



*Obrázek 8: Úvodní obrazovka FotoForensics [21]*

Základní informace o fungování tohoto nástroje jsem čerpala přímo z oficiálních webových stránek. Na samotné stránce můžeme pak také nalézt podrobný návod, jak FotoForensics používat. Přečtení návodu nám pomůže pochopit, jak při analýze postupovat. Následně si po pročtení praktických ukázek uděláme alespoň částečný obrázek o tom, jak celý web funguje a na co je potřeba se ve výsledcích analýzy zaměřit. Na webu máme dvě různé možnosti pro nahrání obsahu. Pokud je obrázek dostupný online, můžeme jej nahrát pomocí adresy URL. [21] Pokud obrázek máme v počítači, jednoduše jej vybereme a nahrajeme. Bohužel nemůžeme nahrát úplně cokoliv a pro některé obrázky platí určitá omezení. Na FotoForensics lze nahrát pouze obrázky ve formátu JPEG, PNG nebo WebP. Velikost souboru může být maximálně 10 MB. Rozměry obrázku by měly být větší než 100x100 pixelů a zároveň menší než 10,000x10,000 pixelů. Zpracování obrázku s příliš velkými rozměry by trvalo velmi dlouho. Naopak malé obrázky jsou s velkou pravděpodobností oříznuty nebo je změněna jejich velikost a takové modifikace jsou zřídkakdy identifikovatelné. FotoForensics podporuje nejaktuálnější webové prohlížeče, takže nejlépe funguje s HTML5 a CSS3. Jelikož je server veřejný, je zakázáno nahrávání souborů se sexuálním obsahem. [22]

Jakmile na server nahrajeme obrázek ať už jedním nebo druhým způsobem, zobrazí se nám stránka s analýzou. V horní části obrazovky nalezneme námi nahraný obrázek. Pokud tento obrázek přejedeme myší, okamžitě se nám zobrazí analýza obrazu a my můžeme ihned vidět případné změny. Nalevo si pak ze seznamu můžeme vybrat, pomocí jaké metody chceme obraz rozebrat. Jako první v tomto seznamu nalezneme souhrn informací o obrázku. Aplikace nám dokáže poskytnout celý název obrázku, datum a čas jeho vytvoření, rozměry, velikost, formát a další. Nás ovšem nejvíce zajímá druhá položka v pořadí, tudíž ELA. ELA je anglická zkratka pro takzvaný Error Level Analysis (dále jen „ELA“). V překladu tato zkratka znamená analýzu úrovně chyb. Ta nám dokáže nejvíce odhalit případné změny na

obraze. Bližší popis této funkce nalezneme v další kapitole. Pro pobavení a odlehčení zde nalezneme také hru, která nám ukáže alternativní způsoby, jak obraz vidět. Po kliknutí na tlačítko start se námi nahraný obrázek promění na několik různě přemístěných obdélníků. Naším úkolem je s co nejmenším počtem kliknutí vrátit obraz do původního stavu. Další funkcí je odhalení skrytých pixelů. Jednoduše se nám zobrazí zpráva, jestli zde skryté pixely jsou, či nikoliv. Odhadovaná JPEG kvalita nám odhalí, v jaké kvalitě byl obraz naposledy uložen. Kvalita se určuje dle kvantizačních tabulek, které JPEG kódovaly. Předposlední funkce v seznamu je hlubší popis souboru. Můžeme zde například nalézt na jaký typ mobilního telefonu nebo digitálního fotoaparátu byl snímek pořízen, což se v některých případech může hodit. Poslední funkcí je vyhledání zdroje obrázku.



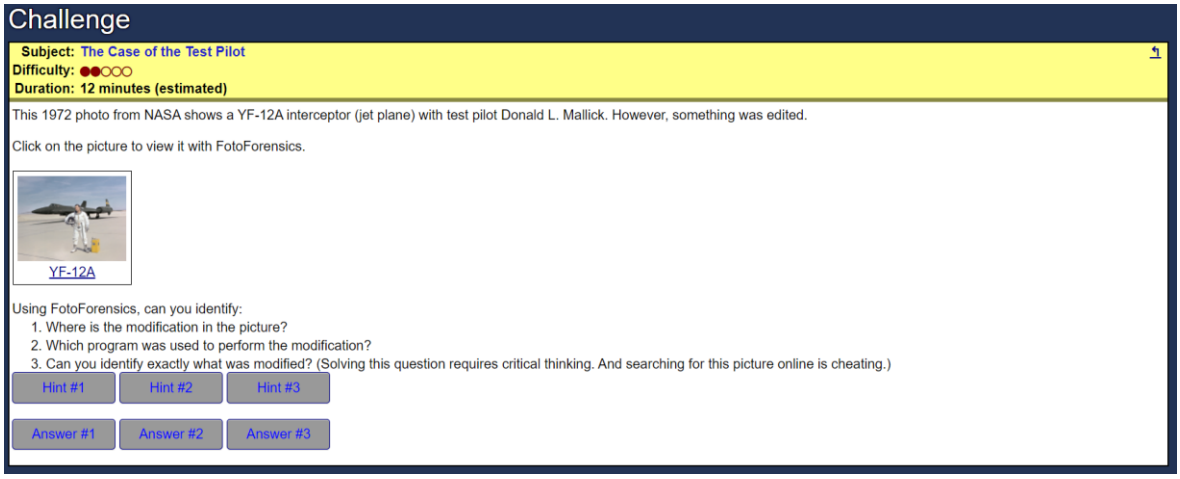

*Obrázek 9: FotoForensics - seznam analýz [21]*

Pod tímto seznamem nalezneme několik málo ikonek, které slouží k dodatečné úpravě obrázku. Můžeme jej libovolně otáčet, přidat barvy, text nebo rychle najít podobné obrázky pomocí Google Image Search, Microsoft Bing Image Search, RootAbout nebo Karma Decay. Pod hlavním obrázkem nalezneme výsledný obrázek, což využijeme v případě, kdy chceme vidět originál a výslednou analýzu vedle sebe. Ve spodní části se pak nachází různé odkazy, například odkaz na nahraný zdrojový obrázek, rychlá tlačítka pro sdílení analýzy na sociálních sítích nebo odkaz na návody.

Co mě osobně zaujalo ze všeho nejvíce, byly předpřipravené tutoriály k otestování samotného nástroje. Nalezneme zde 10 výzev, které jsou rozděleny do několika kategorií dle ná-

ročnosti odhalení fotomontáže. Web nejprve nabádá uživatele, aby vyzkoušeli odhalit montáž bez nápovědy. Jsou zde praktické rady, jak co nejlépe daný problém vyřešit. Ke každé výzvě je připsána časová náročnost, což je ale v některých případech velmi subjektivní.

Pro příklad zde zmíním tutoriál s názvem The Case of the Test Pilot (Případ zkušebního pilota). Fotografie pochází z NASA a byla dodatečně upravována. Autor nám pokládá tři otázky, na které dostaneme odpověď pomocí použití FotoForensics a našeho vlastního logického uvažování. Pokud si nevíme rady, jsou nám poskytnuty nápovědy. Jakmile si myslíme, že známe odpověď na otázku, můžeme rozkrýt její odpověď. Velmi oceňuji tento způsob prezentování celého nástroje. Je to praktické, naučné, v mnohých případech zábavné a nápadité. Tutoriály vás doslova pohltí a donutí vás zkoušet a testovat, co všechno tento nástroj dovede. [23]




*Obrázek 10: FotoForensics – Challenge [23]*

## 2.2 JPEGSnoop

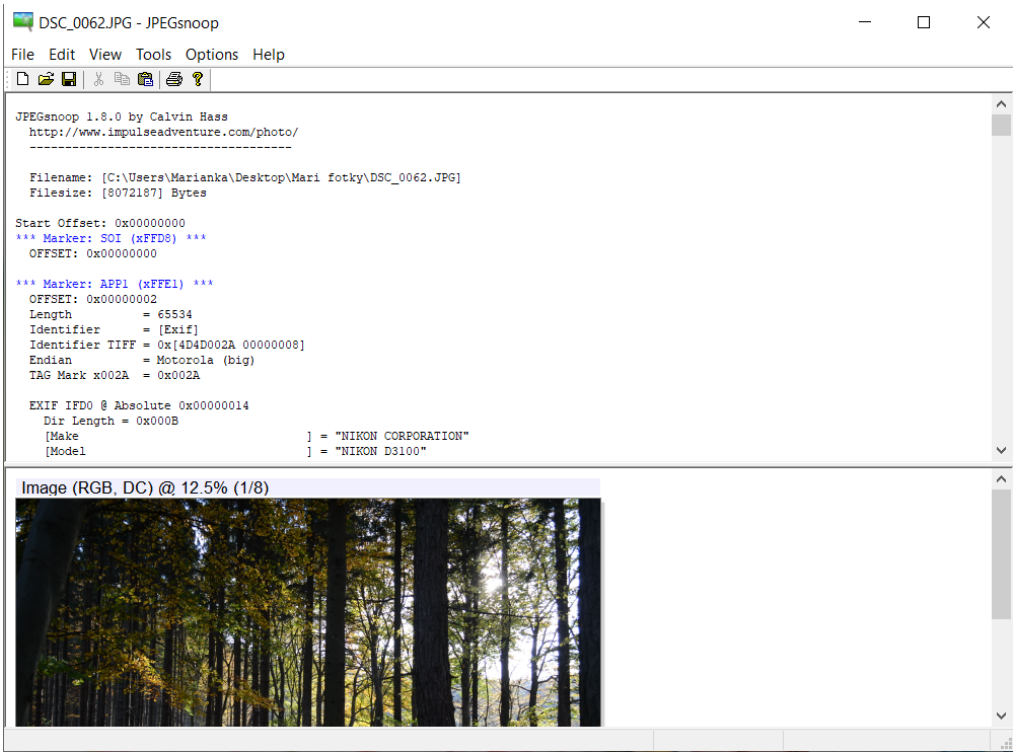
Aplikace JPEGSnoop je bezplatný nástroj pro Windows. Slouží k bližšímu zjištění informací o vloženém souboru. Hlavní funkcí této aplikace je zkoumání a dekódování vnitřních detailů JPEG, MotionJPEG AVI a Photoshop souborů. Každá digitální fotografie obsahuje velké množství informací a právě díky této aplikaci, se o fotografii můžeme dozvědět všechny podrobnosti. Využít lze ale také k ověření pravosti fotografie. Nejenže je možné zjistit různá nastavení, která byla použita při pořizování fotografie, ale lze také vyčíst informace o kvalitě a kompresi obrázků JPEG, které jsme získali při ukládání souboru. V některých případech dokáže odhalit jaké digitální fotoaparáty nebo software mohli být použity pro vytvoření upraveného obrazu. [20]

Mezi podporované formáty patří:

- .JPG
- .AVI
- .DNG
- .PSD
- .MOV
- .PDF

Jak si můžeme všimnou, vkládat můžeme nejen obrázky, ale i videa. Zajímavostí je, že vývojář této aplikace poskytl zdrojový kód pro všechny, kdo by měli zájem o podílení se na vylepšení funkcí a uživatelského rozhraní. [24]

Po vložení fotografie se nám vypíše dlouhý text, ve kterém nalezneme informace o fotografii. Také ihned vidíme, jakým fotoaparátem byla fotografie pořízena a v jakém softwaru byla upravena. V porovnání s ostatními nástroji JPEGSnoop bohužel nedokáže přesněji určit, ve kterém místě se na dané fotografii nachází nějaké úpravy, čímž pomyslně klesl na nejnižší příčku. Pokud nám ale stačí zpráva o tom, že byl k úpravě fotografie použit nějaký software, pak je JPEGSnoop dostačující.

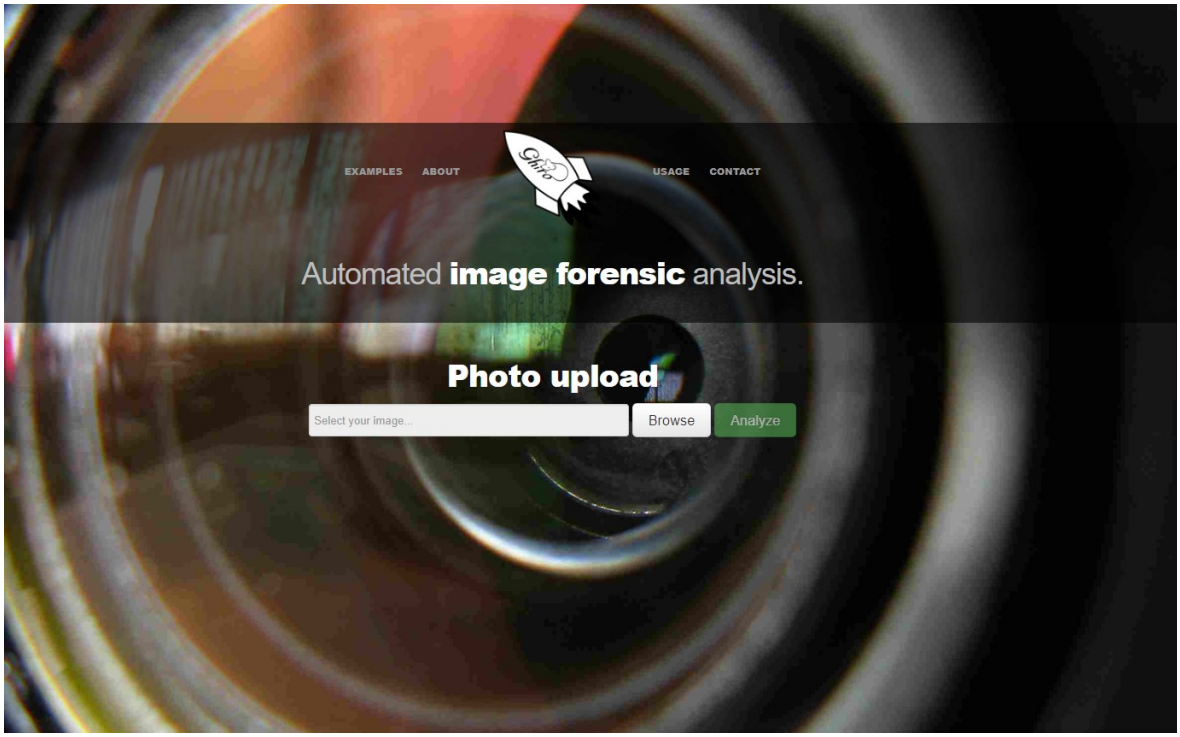



*Obrázek 11: Ukázka prostředí JPEGSnoop*

## 2.3 Ghiro

Ghiro je plně automatizovaný nástroj určený k odhalení nesrovnalostí. Hravě si dokáže poradit i s větším množstvím obrázků najednou. Všechny funkce této aplikace lze ovládat prostřednictvím webového rozhraní. Mezi hlavní funkce patří získání metadat z obrázku a jejich následné roztřídění v závislosti na kategorii, do které spadají. Metadata mohou být zapsána do digitálního fotografického souboru a informují nás o autorských právech, kdo je vlastníkem, jaká kamera soubor vytvořila spolu s informacemi o expozici a popisnými informacemi o fotografii. [25]

V některých případech dokáže lokalizovat kde byla fotografie pořízena a zobrazit konkrétní místo na mapě. Program také pracuje s analýzou úrovně chyb (ELA). Dokáže detekovat rozdíl mezi miniaturami. Někdy se totiž při úpravě fotografie upraví původní obrázek a miniatura nikoli. Miniatury a data s nimi spojená jsou uloženy pro případnou kontrolu. Stejně jako JPEGSnoop je Ghiro projekt skupiny dobrovolníků, kteří poskytli zdrojový kód pro kohokoli, kdo by měl zájem podílet se na vylepšení tohoto nástroje. Stejně jako předchozí zmíněné nástroje je zcela zdarma, ale je zde i možnost vývojáře podpořit a zaslat jim finanční podporu za jejich práci. Vyzkoušet si, jak funguje lze přes https://www.imageforensic.org/. [25] [26]




*Obrázek 12: Úvodní stránka Ghiro [25]*

## 2.4 Forensically

Forensically je sada nástrojů, které dokáží detekovat klony, úrovně chyb a další. Hned na úvodní stránce webu nalezneme testovací fotografii, na které můžeme vyzkoušet funkčnost všech používaných nástrojů. Jako první zde narazíme na funkci lupy, která nám přiblíží část fotografie, na kterou najedeme myší. Nástroj detektor klonů zvýrazní zkopírované oblasti v obraze, což nám může napomoct při odhalení, zdali bylo s obrazem manipulováno. Při použití nástroje detektor klonů se nám na obrázku vykreslí pomocí růžových přímek přesná místa odkud a kam byla daná část obrazu naklonována. Skvěle je funkčnost vidět přímo na příkladu uvedeném od Forensically na obrázku níže. [27]

*Obrázek 13: Forensically - detektor klonů [27]*

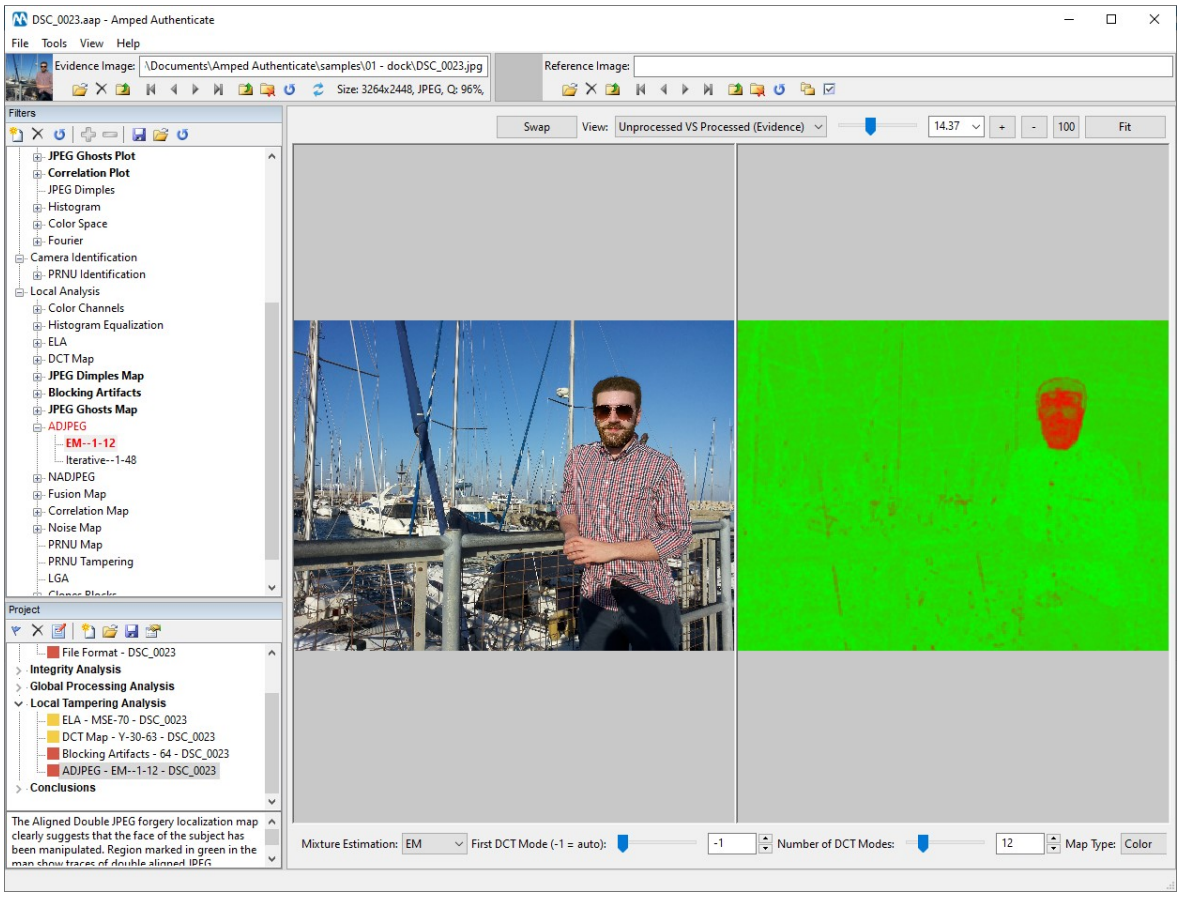
Další funkcí je již mnohokrát zmiňovaný ELA. Na kvalitních fotografiích skvěle pracuje s analýzou šumu. Dokáže odhalit manipulaci s obrazem pomocí nástrojů airbrushing, deformace nebo klonování.

Každá fotografie obsahuje přirozený šum napříč barevným spektrem. Pokud se však v některých částech fotografie šum nevyskytuje, nebo má odlišný charakter, znamená to digitální úpravu, kterou odhalíme právě díky analýze šumu. Vidět v obrázku na první pohled šum, může být poměrně složité. Když jsou však fotografie nějakým způsobem modifikovány, šum zanechává stopu, kterou nám pomáhá odhalit právě nástroj Forensically. [28]

Mezi další funkce patří poskytnutí metadat. Můžeme zde najít nejenom datum a čas, kdy byla fotografie pořízena, ale také datum její úpravy. Skvělé je také vyhledávání místa, kde byla fotografie pořízena. Pomocí jednoho kliknutí můžeme místo zobrazit na Google Maps nebo najít fotografie pořízené na stejném místě na webu Flickr. Pokud to je možné, můžeme si zobrazit i původní neupravenou fotografii. [27]

## 2.5 Amped Authenticate

Amped Authenticate je dalším softwarem pro detekci manipulace jak na digitálních fotografiích, tak i v dokumentech, avšak na rozdíl od předchozích zmíněných aplikacích, je tento software placený. Poskytuje jednoduché uživatelské rozhraní a umožňuje otevřít obraz v běžných formátech jakými jsou JPEG, PNG, TIFF, BMP atd. Vybrat si můžeme z několika nástrojů k otestování obrázku. Algoritmy, s jakými tyto placené softwary pracují si jejich vývojáři pečlivě střeží, tudíž je obtížné nalézt na jakém principu software přesně pracuje. [20]




*Obrázek 14: Prostředí Amped Authenticate [29]*

## 2.6 VerifEyed

Na tomto systému pracovali vývojáři téměř 7 let bez jakýchkoliv předchozích zkušeností. VerifEyed dokáže během několika vteřin s velkou pravděpodobností rozpoznat, zda bylo s naskenovanou fotografií nebo dokumentem manipulováno. Umí ověřit nejenom oskenované dokumenty ale také zjistit pravost notářských zápisů, výpisů z rejstříků atd. Jako jeden příklad, proč je výhodné si tuto službu zaplatit, můžeme uvést praktiky jedné německé společnosti. Ta nabízí poskytnutí půjčky ve výši několik stovek eur pouze za nahrání vašeho občanského průkazu na jejich webové rozhraní. Zde jasně můžeme vidět, že systém musí pracovat velmi spolehlivě. V některých případech také dokáže určit, zda byla fotografie stažena z internetu či nikoli. [6]

Absolventi Českého vysokého učení technického a zároveň vývojáři VerifEyed, Babak Mahdian a Radim Nedbal, vyhráli se softwarem VerifEyed absolventskou kategorii v soutěži města New York nazvané Next Idea. Konkurence na této mezinárodní soutěži byla velká. Se svým projektem dokázali uspět mezi 150 dalšími projekty ze 30 zemí světa. Za tuto výhru si odnesli v přepočtu 340 tisíc korun. Dalším bonusem byl půlroční pronájem kanceláří v centru New Yorku zcela zdarma. [30]

Software VerifEyed od společnosti Imagemetry s.r.o. nenabízí zkušební verzi zadarmo. Je nutné si zakoupit placenou verzi, přičemž za ověření 20 fotografií zaplatíme 5 dolarů. Pro velké společnosti, jejichž zisky závisí na spolehlivosti správného ověření fotografií, je zde i balíček Premium Plus, který stojí 500 dolarů a za tuto sumu prověří 4200 obrázků či dokumentů. [2]

Sami bohužel nemůžeme software otestovat, ale na internetu nalezneme mnoho příkladů upravených fotografií, které dokázal VerifEyed odhalit. Například britský politik Winston Churchill byl zachycen, jak si užívá svého doutníku. Ten byl odstraněn poté, co bylo kouření označeno za nezdravé. [31]

*Obrázek 15: Odhalená změna pomocí VerifEyed [31]*

Nyní se podíváme na tři obrázky, ve kterých dokázal program VerifEyed odhalit úpravy. Na prvním snímku můžeme vidět poničený vůz. Takto upravenou fotku poslal klient pojišťovně za účelem získání finančního obnosu za poškozené auto. Na další fotografii můžeme vidět, jak program odhalil upravená místa. Třetí fotografie ukazuje skutečný stav vozu a neupravenou fotografii. [2]

*Obrázek 16: Snímek pro pojišťovnu [2]*

*Obrázek 17: Snímek s odhalenými změnami programem VerifEyed [2]*

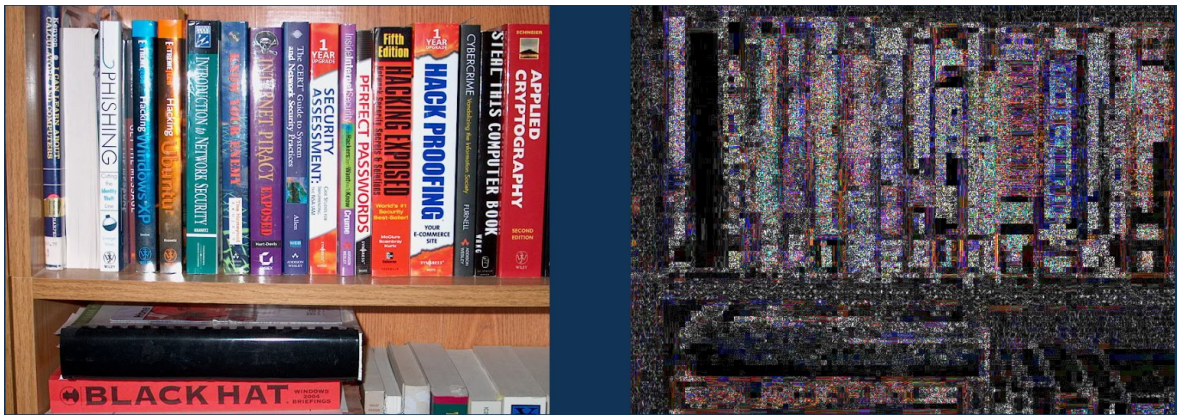
*Obrázek 18: Skutečný stav automobilu [2]*

Některé parametry bohužel z fotografií nezjistíme, ani kdybychom sebevíc chtěli. Například, pokud na mobilním telefonu nemá uživatel povolen přístup k poloze, GPS data nedokáže vykouzlit žádný z výše zmiňovaných softwarů.

# 3 NEJČASTĚJI POUŽÍVANÉ METODY NÁSTROJŮ

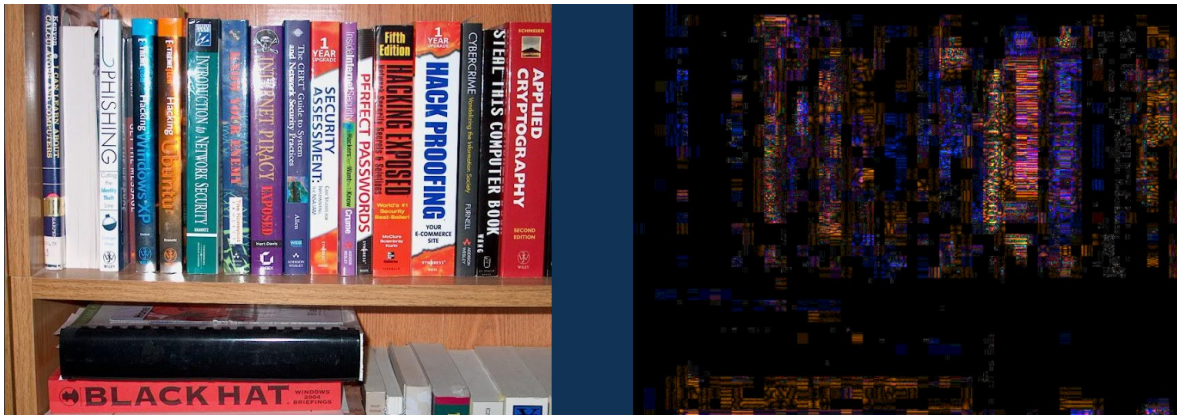
Nejdůležitější pro naše potřeby je vyhodnocení pomocí nástroje ELA. Ten nám umožňuje identifikovat takové oblasti v obraze, které mají různé úrovně komprese. U obrázků ve formátu JPEG by měl být celý obrázek zhruba na stejné úrovni. Pokud je část nebo části obrázku na výrazně odlišné úrovni, pravděpodobně to znamená, že byl obrázek digitálně upraven. Zaměřit bychom se měli především na hrany, textury a povrchy. Všechny podobné hrany by měly mít v ELA podobný jas. Záleží na daném obrázku, jestliže má hrany s vysokým kontrastem, všechny hrany by pak měly vypadat podobně. Stejně tomu tak je i u hran s nízkým kontrastem. Všechny textury, by také měly mít přibližně stejnou úroveň ELA. Toto pravidlo platí i u povrchů bez ohledu na jejich skutečnou barvu. Na nás tedy je, abychom si výslednou analýzu pořádně prohlédli a snažili se najít významné rozdíly mezi kontrasty a identifikovat oblasti, které mohly být digitálně změněny. [32]

Nyní se pojďme podívat na příklad, který nám na svých webových stránkách poskytl FotoForensics. Na prvním snímku vidíme originální obraz, bez žádných úprav. Napravo od něj potom výsledek ELA. Tento výsledek má vysoké hodnoty ELA reprezentované bílou barvou. Černé části na fotografii odpovídají bílé knize na obrázku nalevo. Je to z důvodu, že jednobarevné komprese se dobře komprimují, tudíž mají minimální úroveň chybovosti. [33]




*Obrázek 19: Originální snímek a jeho výsledek v ELA [33]*

Na dalším obrázku byla fotografie jednou znovu uložena. Jak můžeme vidět, s originální verzí se nestalo nic, co by bylo okem viditelné, kdežto ELA vykazuje mnohem více tmavší barvu. Pokud by byl obrázek obnoven ještě jednou, získal by opět nižší (tmavší) hodnotu ELA. [33]




*Obrázek 20: Obnovený snímek a jeho výsledek v ELA [33]*

Na posledním snímku již můžeme v originále vidět, že fotografie byla digitálně upravena. Byly zkopírovány knihy, které nahradily jiné knihy. Vložen byl také dinosaurus. Na výsledku ELA můžeme zřetelně vidět, že upravené oblasti mají vyšší (světlejší) hodnoty ELA. [33]


*Obrázek 21: Upravený snímek a jeho výsledek v ELA [33]*

Při vkládání obrázku záleží na tom, zdali je uložen ve ztrátovém nebo bezeztrátovém formátu. Zatímco bezeztrátové formáty si uchovávají přesné informace o barvě pixelů, ztrátové formáty nám nezaručují, že barvy zůstanou stejné. Ztrátový formát JPEG při každém obnovení obrazu ztrácí svou kvalitu. Konkrétně algoritmus JPEG pracuje na mřížce 8x8 pixelů. Každý čtverec o těchto rozměrech je komprimován nezávisle. Pokud tedy není na obraze provedena žádná změna, všechny tyto čtverce budou mít podobné pravděpodobnosti chyb. Pokud je obraz pouze obnoven, ale není na něm provedena žádná digitální úprava, každý čtverec by měl mít podobnou úroveň chybovosti. Pokud je obrázek upraven, pak každý čtverec 8x8 pixelů bude mít vyšší úroveň chybovosti než zbytek obrazu. [34]

Originální snímky budou mít velmi světlý výsledek ELA. Po jejich opětovném uložení se sníží úroveň chybovosti, čímž získáme tmavší výsledek. Proto bychom měli vždy testovat originální obrázek nebo alespoň jeho nejkvalitnější verzi. Přestože je ELA velmi spolehlivým nástrojem, v některých případech chybu odhalit nedokáže. Pokud například provedeme drobnou úpravu barev či pixelu, nemusí to vyvolat znatelnou změnu v ELA. Jelikož JPEG pracuje na mřížce, změna jakékoliv její části bude mít pravděpodobně dopad na celý čtverec, proto nebude možné určit, který pixel v mřížce byl změněn. Barvy s vysokým kontrastem, které se nacházejí ve stejné mřížce obvykle mají vyšší hodnoty ELA než barvy podobné. Mezi kontrastní barvy řadíme například černou a bílou, nebo oranžovou a modrou. Photoshop může při uložení obrázku automaticky zaostřit textury a hrany a automaticky tak vytvořit vyšší úroveň chybovosti. Tuto změnu uživatel pravděpodobně neprovedl úmyslně, avšak na výsledku ELA se může zdát jako chtěná úprava. ELA je pouze jeden algoritmus pro nalezení změn na obraze a nemusí vždy odhalit vše, proto je důležité zkusit obraz ověřit i jinými technikami a algoritmy. [33] [34]

Užitečné informace můžeme získat také pomocí metadat. Díky nim si můžeme fotografie snadno roztřídit nebo dohledat. Do metadat řadíme EXIF, IPTC nebo XMP. Základní metadata (EXIF) jsou k fotografii připsány ve fotoaparátu hned ve okamžiku jejího pořízení. [35]

Řadíme sem například:

- Informace o modelu fotoaparátu
- Expoziční hodnoty fotografie (čas uzávěrky, clona objektivu, hodnota ISO)
- Údaje o objektivu a ohniskové vzdálenosti
- Informace o nastavení blesku
- Datum a čas pořízení snímku
- GPS souřadnice

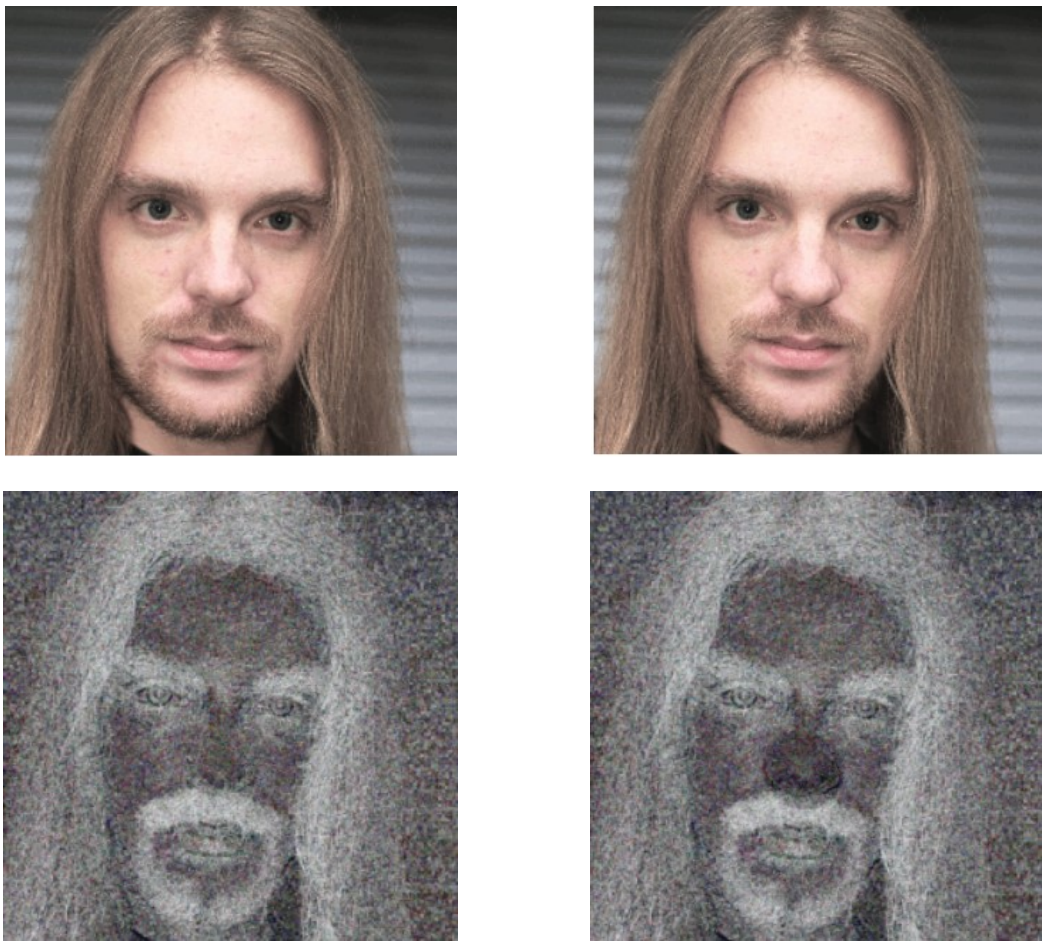
Díky EXIF datům se z nás mohou stát lepší fotografové. Jestliže se nám nějaká fotografie nepovedla a je rozmazaná, může za to pravděpodobně expoziční čas. Stačí se pak pouze poučit z chyb a příště vyzkoušet za podobných podmínek jiné nastavení fotoaparátu nebo použít stativ. Můžeme také prozkoumat EXIF data u fotografie pořízené fotografem, od kterého bychom se rádi něco přiučili a zkusit nastavit fotoaparát podle informací, které jsme získali z jeho fotografie. [35]

Rozšiřující IPTC data jsou k souborům většinou přidávány v editorech pro úpravu fotografií a většinou nám usnadňují organizaci našich fotografií. Jedná se o:

- Popis fotografie
- Klíčové slova
- Hodnocení snímku
- Barevné štítky

XMP data informují o procesu zpracování fotografie ve foto editoru. [35]

V jediném nástroji, ve kterém se setkáme s funkcí analýza šumu, je Forensically. Základní myšlenka tohoto nástroje je velmi prostá. Obrázky jsou plné šumu, takže když nějakou část změníme, šum nám zanechá v obraze viditelné změny. Jako příklad zde můžeme vidět fotografii muže níže, kterému byl lehce zvětšen nos. Úprava není nijak zásadní a rozhodně bychom na první pohled neměli podezření, že by se nemuselo jednat o jeho skutečný nos. Při použití analýzy šumu však můžeme vidět změnu šumu a tím pádem zjistit, že byl nos zvětšen. [28]



*Obrázek 22: Forensically - odhalení zvětšení nosu [28]*

Jako další metodu můžeme zmínit detekci klonů. Detektor klonů zvýrazňuje podobné oblasti na obrázku. To může znamenat, že s obrázkem bylo manipulováno pomocí nástroje klonování. Vyhledává místa v obraze, které se zde objevili po transformacích, mezi které patří posun, otočení, změna velikosti atd. U nástroje Forensically jsou podobná místa označena modrou barvou a spojena červenou čarou. V nástroji je možné nastavit parametry, dle kterých mají být klony hledány. [27]

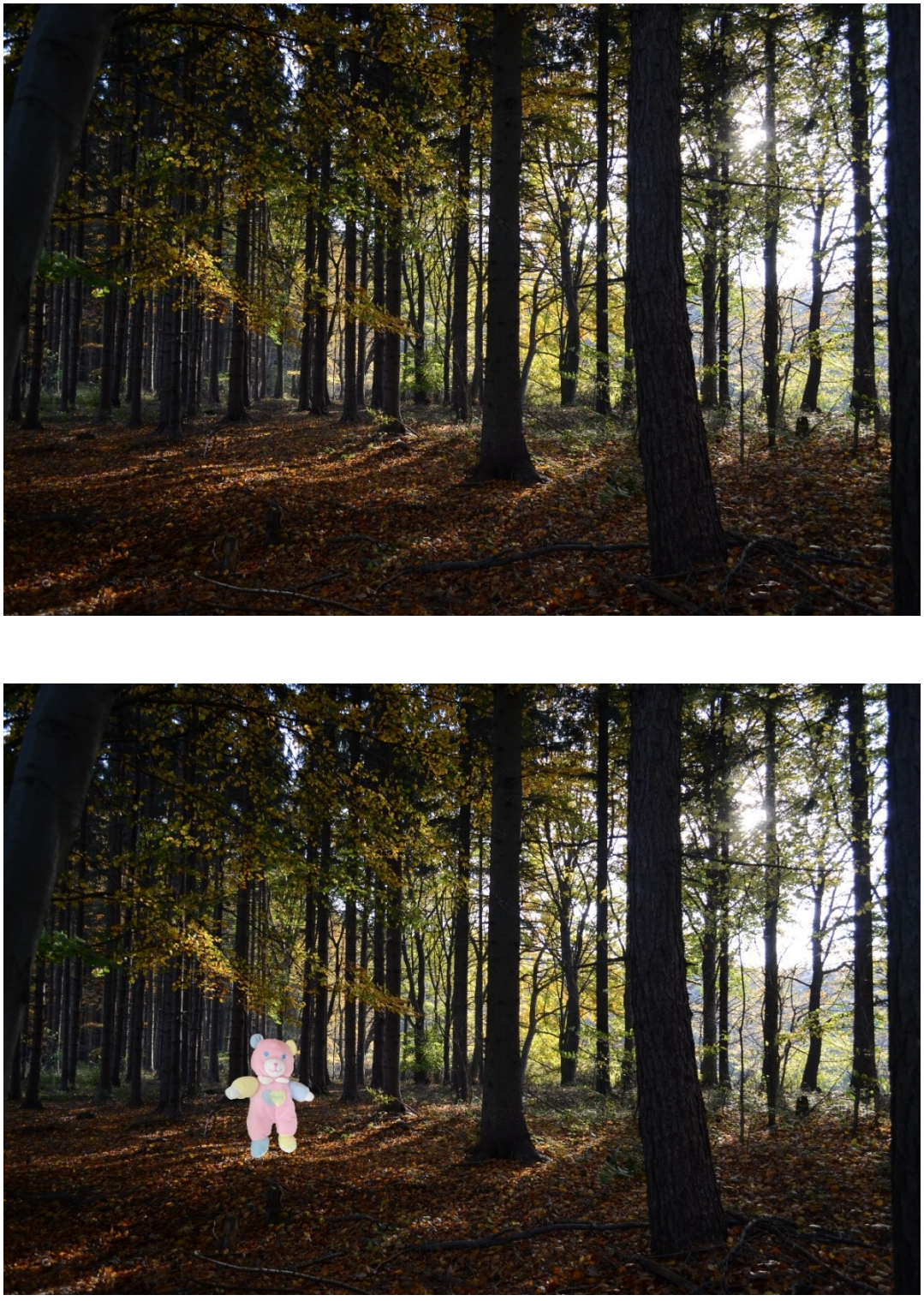
# II. PRAKTICKÁ ČÁST

# 4 VZORKY PRO TESTOVÁNÍ

Pro přípravu vzorků k testování jsem využila fotografie, které původně vznikly pouze za účelem zachycení vzpomínky. Nebylo potřeba fotografovat nové nebo speciální snímky, protože pro naše účely můžeme využít v podstatě jakoukoliv fotografii. Nalezneme zde fotografie jak z digitálního fotoaparátu, tak z mobilního telefonu. Konkrétně se jedná o fotoaparát NIKON D3100 a telefon Huawei, což nám dosvědčí i programy, které umí zobrazit EXIF data. Fotografie byly dále upraveny v programu Adobe Photoshop nebo Zoner Photo Studio X.

Uvedena je zde jako první vždy originální fotografie bez jakýchkoliv úprav a následně fotografie s úpravami. Cíleně jsem připravila velmi rozmanitou škálu testovacích vzorků. Nalezneme zde fotografie, u kterých je na první pohled zřejmé, že zde byla provedena nějaká změna. Záměrně byly použity také fotografie, na kterých by obyčejný smrtelník žádnou úpravu nehledal ani nečekal. U jednoduchých úprav byl proces velmi rychlý. U složitějších a propracovanějších fotografií jsem strávila úpravami i několik desítek minut.

Pro výběr medvídka na 1. fotografii níže byl použit rychlý výběr ve Photoshopu. Po jeho vložení byla upravena jeho velikost pomocí transformace. Pro vyjmutí a zkopírování jednodušších tvarů je možno použít i kouzelnou hůlku.



*Obrázek 23: Originál a upravená testovací fotografie č.1*

Letadlo na další upravené fotografii bylo ořezáno i s částí původní oblohy a vloženo na oblohu originální fotografie. Za pomoci klonovacího razítka, které bylo nastaveno na poloviční průhlednost, bylo okolí letadla rozmazáno do ztracena, aby splynulo s oblohou na originální neupravené fotografii. Pro výběr kačenek, jsem použila nástroj rychlý výběr.

*Obrázek 24: Originál a upravená testovací fotografie č.2*

Do této fotografie byl vložen obal od dětského nápoje. Úprava má evokovat reklamy nebo kresby, které můžeme často najít právě na vysokých budovách nebo obytných domech. Na první pohled by nám tedy nemělo být podezřelé, že se na snímku nachází něco špatně.


*Obrázek 25: Originál a upravená testovací fotografie č.3*

K vylepšení portrétu jsem nejprve použila nástroj zkapalnění. Jak můžeme jasně vidět, na upravené fotografii jsou zvětšené oči, zúžená tvář, optické prodloužení krku a mírné zúžení pasu a rukou. Pomocí nástroje zesvětlení jsem vybělila zuby. Dále jsem nástrojem záplata odstranila nedokonalosti na těle jako je akné a znamínka. K dalším úpravám byli ve většině případů použity klonovací nástroje nebo kouzelná hůlka. Mezi testovací fotografie zařadíme i obrázek, který nebude upraven, pouze bude převeden do jiného formátu, abychom zjistili, jakým způsobem se softwary zachovají při této nepatrné změně.

*Obrázek 26: Originál a upravená testovací fotografie č.4*

V poslední testovací fotografii jsem nahradila rozkrojený citron bezovými květy. Citron jsem vybrala pomocí nástroje rychlý výběr a úplně ho ze snímku vymazala. Zůstala tedy pouze bílá barva na pozadí. Následně jsem bezové květy označila kouzelnou hůlkou a zkopírovala. Vytvořila novou vrstvu, do které jsem nakopírovala tyto květy. Konkrétně jsem vytvořila tři kopie tak, aby se květy různě překrývaly a zakryla jimi prázdné místo vzniklé po citronu.

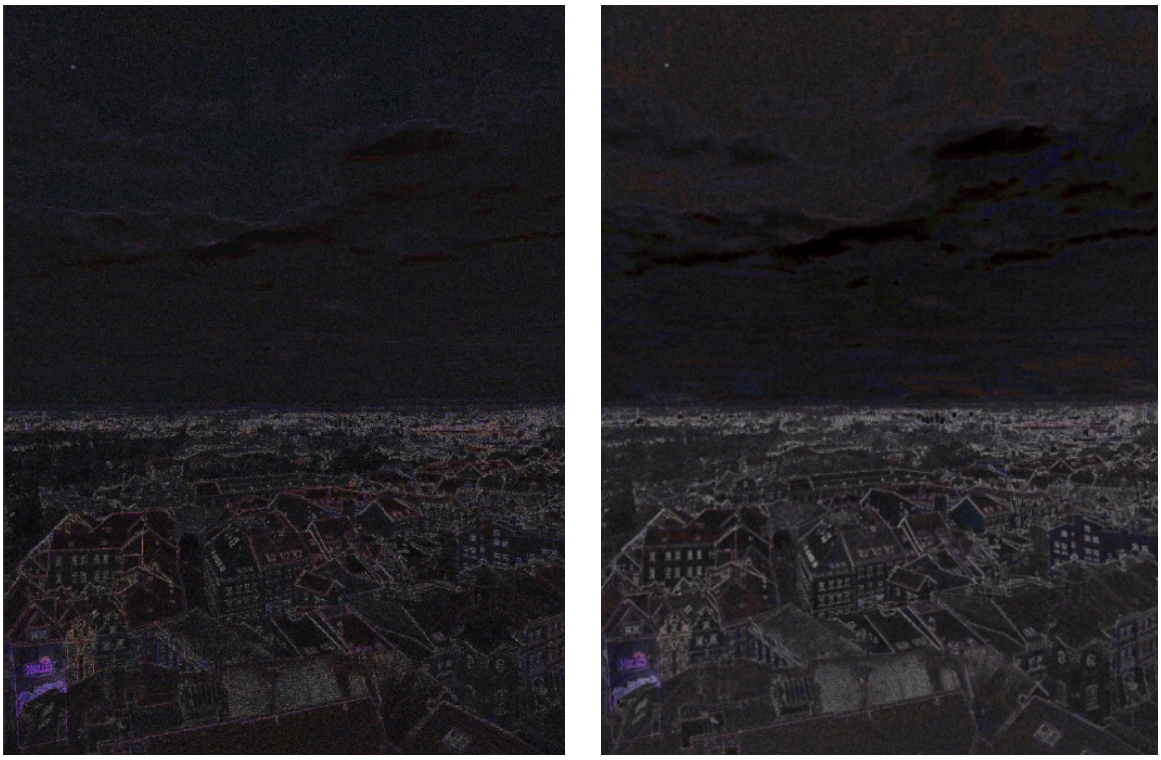
*Obrázek 27: Originál a upravená testovací fotografie č.5*

# 5 TESTOVÁNÍ SPOLEHLIVOSTI VYBRANÝCH NÁSTROJŮ POMOCÍ PŘIPRAVENÝCH VZORKŮ FOTOGRAFIÍ

Nahrání všech testovacích fotografií probíhalo ve většině případů velmi komfortně, jelikož zde často pracujeme pouze s webovým rozhraním a není potřeba nic stáhnout či instalovat. To se netýká aplikace JPEGSnoop, kterou je potřeba stáhnout a naistalovat. Je to ale velmi snadné a rychlé. Nahrávání některých fotografií trvalo delší dobu, což je ale zcela pochopitelné při velikostech těchto souborů. Pro větší získání přehledu o funkčnosti, přesnějších výsledků a také z vlastní zvědavosti, jsem nahrávala a testovala i jiné fotografie, které nejsou popsány výše a nejsou uvedeny ani v příloze.

## 5.1 Testování ELA

Při testování nástroje ELA se mi nejvíce osvědčilo Forensically. V ostatních programech někdy nebylo snadné si všimnout nějaké změny, kdežto ve Forensically byla změna patrná hned na první pohled. Výsledek ELA byl mnohem více barevnější a zřetelnější, jak můžeme vidět na porovnání analyzovaných fotografiích níže. V našem případě je zřejmé, kde je fotografie upravená, tudíž je výsledek ELA viditelný, avšak při důkladnější fotomontáži, by některé softwary mohly mít problém změnu odhalit.



*Obrázek 28: Analýza ELA - Forensically vs. FotoForencics*

Nejvíce mě překvapil výsledek testování fotografie s medvědem. Zde máme na první pohled patrné, že růžový plyšový medvídek do lesa rozhodně nepatří a byl uměle přidán. Očekávala jsem tedy, že výsledek ELA bude nejzřetelnější ze všech. Bohužel v tomto případě neuspěl ani výše pochvalovaný Forensically. Možná jsem měla na tuto fotografii přehnaně velké nároky, ale určitě mi dáte za pravdu, že výsledek mohl dopadnout mnohem lépe a být mnohem víc viditelný.

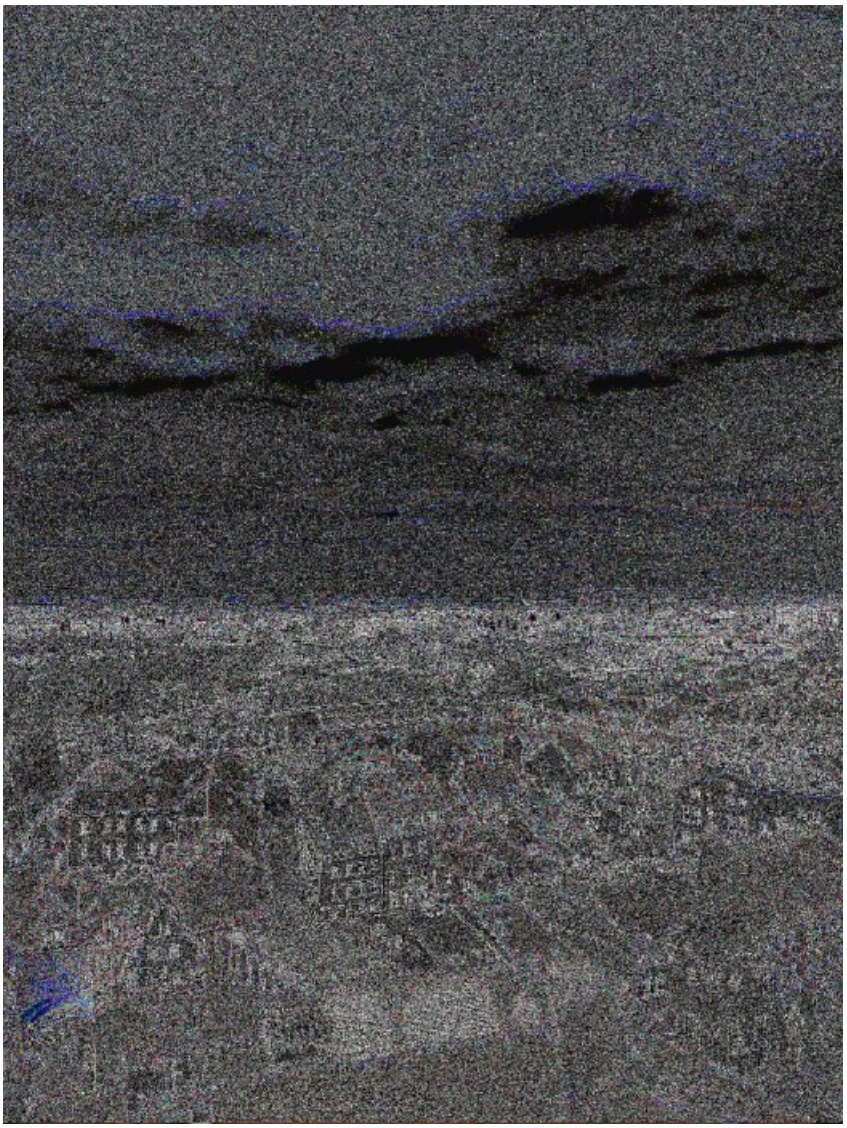
*Obrázek 29: Analýza ELA – Forensically*

Když porovnám výsledky ELA ve všech nástrojích (Forensically, FotoForensics a Ghiro) všechny dokázaly zanalyzovat fotografii stejně. Někde byla změna nepatrně viditelnější, ale v konečném důsledku všechny nástroje uspěly v odkrytí změn zhruba stejně.

## 5.2 Změna šumu

Forensically má nástroj pro analýzu šumu, který také dokáže vypátrat změny v obraze s poměrně velkou přesností. Analýza šumu nebyla součástí nástroje hned od jeho spuštění, nýbrž byla vyvinuta až později. Ostatní nástroje tuto službu neposkytují, tudíž ji není s čím porovnávat. Nejlépe si analýza šumu poradila s fotografiemi, které byly upraveny jednodušeji. Snímky, které byly propracovanější už neukazovaly až tak zřetelné výsledky. Nejlepší výsledky jsem viděla jen na fotografii poskytnuté přímo na webové stránce, což je logické, aby

bylo co nejlépe vidět, jak nástroj funguje. Je to jistě velmi dobrá funkce, ale hodně záleží na tom, jakými nástroji byla daná fotografie upravována.



*Obrázek 30: Analýza šumu - Forensically*

## 5.3 Detekce klonů

Nástroj detekce klonů fungoval velmi dobře. Avšak opět pouze ve Forensically. Když jsem nahrála originální fotografii bez úprav, webové rozhraní mi hned vypsalo zprávu o tom, že se na obrázku žádné klony nenacházejí. Funkce je nepotřebná ve chvíli, kdy obraz nebyl pozměněn klonováním, ale nějakými jinými nástroji. Pokud se na fotografii klony nachází, výsledek je vidět na první pohled. Dokonce je originál a klon spojen čarou pro lepší zřetelnost. Na ukázku je zde snímek obrazovky, kde můžeme jasně vidět, že zde místo původního citronu byla naklonována bezinka. Program našel podobnost a označil ji. Výsledek by mohl

být ještě přesnější, avšak na samotném webu je uvedeno, že nástroj nemusí být úplně přesný, ale pro naši potřebu je zcela dostačující.


*Obrázek 31: Detekce klonů v obraze*

## 5.4 Testování metadat

Testování metadat dopadlo ve všech případech úspěšně. Všechny výše zmíněné softwary dokázaly odhalit mnoho informací spojených s fotografií. Všechny také dokázaly rozpoznat, zda byl snímek dodatečně upravován v nějakém programu a konkretizovat v jakém. Problém však nastává v případě, kdy bychom rádi znali informace o snímku staženém z internetu. Tam jsme ve výsledku pouze viděli, v jakém formátu stažený obrázek je a jaké má rozměry. A k získání těchto informacím nepotřebujeme zrovna nějaký speciální nástroj. Na obrázku níže můžeme vidět výsledek, který dokázaly zobrazit všechny testované nástroje. Na obrázku je konkrétně výsledek aplikace Ghiro.


*Obrázek 32: Ghiro – EXIF*

## 5.5 GPS

GPS souřadnice šly samozřejmě zjistit pouze u obrázků, u kterých byly tyto data k dispozici. Vyzkoušela jsem vlastní fotografii s GPS souřadnicemi i staženou fotografii, u které jsem věděla, že jsou tyto data k dispozici a znala jsem místo jejího pořízení. Všechny nástroje tuto zkoušku úspěšně zvládly pouze s rozdílem, že u Forensically a FotoForensics byla ihned k nahlédnutí i mapa s přesným výsledkem. FotoForensics se u tohoto nástroje pojistil tím, že upozorňuje na výsledky, které nemusí být přesné. Já jsem otestovala několik fotografií a výsledky byly vždy velmi přesné, což mě mile překvapilo. U nástrojů JPEGSnoop a Ghiro byly pouze vypsány souřadnice, které jsem následně musela ručně zadat do mapy. Zklamáním pro mě bylo, že aplikace Ghiro slibovala i zobrazení na mapě, které ovšem nefungovalo, musela jsem se tedy spokojit pouze se souřadnicemi.


*Obrázek 33: Forensically - GPS*

## 5.6 Rámcové výsledky testování

Pro rámcové shrnutí všech nástrojů a jejich funkcí jsem vytvořila stručnou tabulku, ve které hodnotím své zkušenosti, jak jsem byla spokojena s jednotlivými výsledky. Hodnocení výsledků je klasifikováno jako na vysoké škole, tudíž od nejlepšího – výborný, po nejhorší – nedostatečný.

| Metody: / Nástroje: | ELA | Analýza šumu | Detekce klonů | Metadata | GPS |
|---|---|---|---|---|---|
| Foto-Forencis | Výborný | Neobsahuje | Neobsahuje | Výborný | Výborný |
| JPEGSnoop | Neobsahuje | Neobsahuje | Neobsahuje | Výborný | Dobrý |
| Ghiro | Dobrý | Neobsahuje | Neobsahuje | Výborný | Dobrý |
| Forensically | Výborný | Dobrý | Dobrý | Výborný | Výborný |

*Tabulka 1: Tabulka výsledku testování jednotlivých nástrojů*

Po otestování spolehlivosti výše zmiňovaných nástrojů jsem byla mírně v rozpacích. Všechny rozhodně nesplnily vše, co slibovaly, nebo alespoň ne tak dobře, jak jsem od nich očekávala. K otestování však byly použity pouze neplacené softwary, tudíž je jasné, že v některých případech nemusíme dostat vždy 100% výsledek. Nachystané vzorky byly většinou upraveny tak, aby byla úprava zřetelná na první pohled. Je však jasné, že s pokročilými úpravami od profesionálů, by měly softwary mnohem menší úspěšnost odhalení změny. O to více mě zaskočilo, když například výsledek ELA nebyl v některých případech vůbec zřetelný, i přesto, že změny v obraze byly vidět pouhým lidským okem.

V celkovém souhrnu bych ani jeden nástroj neoznačila za 100% funkční. Nejvíce bych sama za sebe důvěřovala softwarovému nástroji Forensically. S jeho webovým prostředím se mi pracovalo velmi dobře, obsahoval funkce, které ostatní softwary neměly a jeho výsledky byly dle mého názoru nejpřesvědčivější ze všech, což ovšem způsoboval také fakt, že obsahoval více funkcí k otestování pravosti. Na druhou pomyslnou příčku bych zařadila FotoForensics. Výsledky byly dostačující, nejlépe bych však ohodnotila zpracování jeho webových stránek jako takových. Skvěle zde mají popsáno, jak software pracuje a co od něj můžeme očekávat. Skvělé byly také zkušební obrázky, na kterých bylo možné si vyzkoušet práci detektiva a odhalit úpravy.

# 6 DOPORUČENÝ POSTUP OVĚŘOVÁNÍ PRAVOSTI FOTOGRAFIÍ

Čím dál častěji se na internetu vyskytuje zábava v podobě hraní si s fotkami. Nejčastěji tuto „hru“ hrají redaktoři, kteří za pomoci několik let staré fotografie a zajímavého titulku dokáží vytvořit takzvané „Fake News“. Fotografie se mnohdy vztahují ke zcela jiným situacím nebo okolnostem. Když se pak tato klamná zpráva začne šířit internetem, nikdo si nemůže být jistý, zda se jedná o pravdu či nikoliv. Je proto dobré, seznámit se s několika základními ověřovacími technikami, které nejsou časově náročné a zároveň nám ušetří spoustu starostí. Abychom nekritizovali pouze média, je nutno podotknout, že záměrné mystifikování fotografiemi se stává čím dál častěji denní praktikou mnoha politiků. [5]

## 6.1 Zjištění původu fotky či videozáznamu

Jedna z nejjednodušších a zároveň nejdůležitějších technik je pokusit se ověřit originalitu fotografie. Každý je schopný tuto verifikaci provést během krátké chvíle za použití funkce Google Images nebo jiných nástrojů fungujících na podobné bázi. Díky ověření originality fotografie můžeme zjistit, zda nás daný server či jedinec záměrně nemystifikuje použitím fotografie starší, patřící ke zcela jiným kontextům. Této možnosti mystifikace hojně využívají klamné fotografie za účelem zvýšení návštěvnosti a tím i zvýšení zisku z reklam. [5]

## 6.2 Ověření zdroje

Lidé o sobě sdílejí na internetu spoustu informací, proto je velmi snadné dohledat něčí digitální identitu, stopu a historii. K vyhledávání můžeme použít aplikaci Pipl, která dokáže vyhledat člověka i kontakt na něj. Další podrobnosti můžeme získat také skrze obchodní rejstřík. [5]

## 6.3 Ověření data

Každý digitální fotoaparát či chytrý telefon přikládá do souboru s fotografií při jejím pořízení také další informace jako je datum zachycení, typ fotoaparátu, rychlost závěrky, expozice, GPS informace a mnoho dalšího. Pomocí těchto dat tak můžeme zjistit nejen místo a čas pořízení fotografie, ale v některých případech nám tyto data mohou poskytnout důležité informace o zdroji. Pro získání těchto můžeme nahrát daný soubor s fotografií např. do Jeffrey Friedl’s Image Viewer, který dokáže rozkrýt fotoaparátem ukládané informace. Tak poznáme, zdali byla fotografie pořízena a užita v kontextech, v jakých je uváděna například v příspěvku na sociálních sítích. Podobně se na to můžete podívat v jakémkoliv grafickém

editoru pro úpravu fotografií, nicméně tyto informace není problém úplně vymazat nebo modifikovat. [5]

## 6.4 Ověření místa

Do fotografie jako takové není potřeba vždy zasahovat a měnit ji. Aby manipulátoři docílili požadovaného výsledku, stačí zaměnit kontext. Sociálních sítě jako je Twitter, Facebook nebo Instagram umožňují svým uživatelům přidat umístění, odkud jejich příspěvek na sociální síť připojili, nebo kde jej pořídili. Tyto informace by měly usnadnit práci s určením lokace fotografie. Problém však spočívá v tom, že je velice snadné s těmito informacemi manipulovat a měnit je, což se bohužel děje až příliš často. K určení místa pořízení fotografie mohou opět dopomoci také EXIF data, pokud jsou k dispozici. Bezpochyby je v určitých případech možné snažit se najít vizuální body, podle kterých pomocí Google Earth či Google Street View danou lokaci dohledáme a tím si ověříme, zda fotka skutečně byla pořízena tam, kde je uváděno. [5]

## 6.5 Motivace

Fotografie ve většině případů pořídí osoba, kterou můžeme považovat za očitého svědka celé situace. Tato osoba pak může být důležitou součástí celého příběhu. Danou situaci nám dokáže daleko líp popsat a vysvětlit, a v konečném důsledku můžeme zjistit, že to, co vidíme na fotografii, vlastně vůbec nemusí být pravda. Pokud by všechno probíhalo takto hladce, měli bychom vystaráno. Je důležité se však podívat na celou situaci ještě z druhého pohledu. Daná osoba může naschvál šířit klamné informace a cíleně se nás snažit oklamat. [5]

Nyní tedy podle těchto pěti základních kroků zhruba víme, co dělat, když chceme odhalit falešnou fotografii. Opravdu bychom neměli podceňovat zjištění zdroje. Pokud u fotografie není uveden autor nebo zdroj, rozhodně bychom měli zpozornět a nevěřit fotografii na první pohled. Zcela jistě je důležité se zaměřit na detaily. Pečlivě si prohlédnout vyobrazené osoby, objekty a místa. Další známkou, že s fotografií bylo nějakým způsobem manipulováno může být nepřirozená poloha některé z věcí na obrázku, přetočené končetiny nebo lidé či věci bez stínu. V případě, že fotografie nevypadá na první pohled upraveně, můžeme využít reverzní vyhledávání obrázků a zjistit, kde byl daný obrázek v minulosti použit. Když budeme mít štěstí, narazíme na více článků a zdrojů informací, ze kterých si můžeme po částech poskládat pravdu. Nakonec nezbývá nic jiného, než zkusit některý z představených nástrojů a také věřit vlastnímu rozumu a intuici. [36]

# ZÁVĚR

Cílem této bakalářské práce bylo provést literární rešerši na téma nástroje pro ověřování pravosti digitálních fotografií. Následně za pomocí testovacích vzorků blíže představit a vyzkoušet spolehlivost těchto nástrojů, přičemž se zaměřit na ty neplacené, volně přístupné.

V první části byly uvedeny důvody, proč vůbec fotomontáže vznikají a čtyři typy fotografické manipulace. Mnoho zajímavých informací také bylo obsaženo ve článku [6] spojeném se softwarem VerifEyed, o kterém jeho vývojáři Babak Mahdian a Radim Nedbal tvrdí, že dokáže poskytnout 100% výsledky. To jsme ovšem nemohli zjistit, jelikož je tento software placený a využívaný spíše v oblasti pojišťovnictví. V poslední části rešerše byly zmíněny podvodné videa, takzvané Deepfakes. Stručně bylo vysvětleno v čem spočívá technika výroby takového typu videa. V další části byly vyjmenovány některé fotografické montáže, jak starší, tak novější. Ke konci rešerše jsem se zamyslela nad tím, jak lidé mohou vnímat upravené fotografie.

V další teoretické části byly popsány konkrétní, volně dostupné nástroje pro ověřování pravosti digitálních fotografií. Nalezneme zde rámcový přehled, s jakými funkcemi dané nástroje pracují a jejich bližší popis. Do určité míry bylo také popsáno prostředí jednotlivých nástrojů. Ze zmíněných bych nejvíce vyzdvihla FotoForensics a Forensically. Tyto dva nástroje se ukázaly jako nejspolehlivější a nejlépe se s nimi pracovalo. Pro zajímavost jsou uvedeny dva placené nástroje, které bohužel nebylo možné otestovat.

Poslední teoretická část práce se zabývá používanými nejpoužívanějšími metodami nástrojů. Zde stojí za zmínku funkce, která má zkratku ELA a znamená analýzu úrovně chyb na obraze.

Vzorky upravených fotografií byly připraveny do praktické části bakalářské práce k otestování funkčnosti jednotlivých nástrojů. Byly použity takové úpravy fotografie, aby bylo co nejlépe poznat, jestli nástroje fungují tak, jak by měly. K tomuto účelu byly využity pouze neplacené služby. V závěru je uvedena stručná tabulka s hodnocením, jak testování dopadlo. Některé nástroje byly samozřejmě lepší, což jsem očekávala, poněvadž jsem si nejprve našla, nejpoužívanější a doporučované ostatními uživateli. Nejlépe ze všech zmíněných se mi pracovalo s Forensically. V nabídce mělo také nejvíce metod, dle kterých šly odhalit případné úpravy na fotografii. FotoForensics a Ghiro jsou podle mne oba na podobné úrovni. Nejhůře bych hodnotila nástroj JPEGSnoop. Poskytoval poměrně málo informací, v porovnání ostat-

ními. Navíc k jeho používání bylo nutné si software stáhnout. To může být trochu nepohodlné, když víme, že existují i aplikace, které fungují na webovém rozhraní a poskytují mnohem více informací o snímku.

V poslední části bylo doporučeno několik tipů, které pokud budeme aplikovat na upravenou fotografii, měli bychom s velkou pravděpodobností úspěchu dojít k závěru, že je nepravá a bylo s ní nějakým způsobem manipulováno.

Tato práce tak může posloužit komukoliv, kdo by měl zájem se dozvědět o problematice upravovaných fotografií něco více. Mnohdy někteří lidé ani netuší, že fotografie obsahuje informace, které nejsou zřejmé na první pohled. Z vlastní zkušenosti můžu říct, že jsem se doposud s žádnými podobnými nástroji ještě nesetkala. Nikdy jsem neměla potřebu fotografii nějak blíže zkoumat. O to více mě samotnou zajímalo, jak testování dopadne a jestli je vůbec možné nepravé digitální fotografie odhalit pomocí volně dostupného softwaru. Po zjištění, jaká kvanta fotografií jsou v dnešní době upravovány a měněny, budu zcela jistě dovednosti těchto nástrojů využívat nadále. Je nutné ovšem podotknout, že výsledky mohou být mnohdy zavádějící a je na samotném uživateli, jak s vyhodnocením naloží.

# SEZNAM POUŽITÉ LITERATURY

[1] KASÍK, Pavel. Nenechte se napálit fotomontáží. Odhalte, co je na fotce upraveného. Technet.cz [online]. 2014 [cit. 2020-08-03]. Dostupné z: https://www.idnes.cz/technet/software/fotomontaze-hoax-fake-photoshop.A090317_114241_software_pka

[2] NEFF, Ondřej. VerifEyed po roce a půl. Digineff.cz [online]. 2012 [cit. 2020-08-03]. Dostupné z: https://digineff.cz/verifeyed-po-roce-a-pul/

[3] ČURDA, Pavel. VerifEyed dobyl s projektem na rozpoznání falešných fotek New York. Lupa.cz [online]. 2011 [cit. 2020-08-03]. Dostupné z: https://www.lupa.cz/clanky/verifeyed-dobyl-s-projektem-na-rozpoznani-falesnych-fotek-new-york/

[4] 13 online nástrojů, které pomohou ověřit pravost fotografie. Stopfake.org [online]. 2014 [cit. 2020-08-03]. Dostupné z: https://www.lupa.cz/clanky/verifeyed-dobyl-s-projektem-na-rozpoznani-falesnych-fotek-new-york/

[5] PIKA, Tomáš. Fact-checking: pět kroků, jak ověřit fotografii na internetu. Houpaciosel.cz [online]. 2017 [cit. 2020-08-03]. Dostupné z: https://www.lupa.cz/clanky/verifeyed-dobyl-s-projektem-na-rozpoznani-falesnych-fotek-new-york/

[6] DAŇKOVÁ, Julie. Babak Mahdian: Odhalujeme falešné fotky pro pojišťovny i OSN. Ihned.cz [online]. 2013 [cit. 2020-08-03]. Dostupné z: https://archiv.ihned.cz/c1-60037270-odhalujeme-falesne-fotky-pro-pojistovny-i-osn

[7] SAMPLE, Ian. What are deepfakes – and how can you spot them? Theguardian.com [online]. 2020 [cit. 2020-08-03]. Dostupné z: https://www.theguardian.com/technology/2020/jan/13/what-are-deepfakes-and-how-can-you-spot-them

[8] ZEMANOVÁ, Milada. Nová DeepFake videa jsou k nerozeznání od reality. Focus-age.cz [online]. 2018 [cit. 2020-08-03]. Dostupné z: https://www.focus-age.cz/m-journal/aktuality/nova-deepfake-videa-jsou-k-nerozeznani-od-reality__s288x13750.html

[9] FENDRYCHOVÁ, Simona. Ukazuji, co je možné. Slovák vytváří deep fake videa a varuje před šířením lží. Aktualne.cz [online]. 2019 [cit. 2020-08-03]. Dostupné z: https://magazin.aktualne.cz/kultura/film/deep-fake-ctrl-shift-face-hbo/r~fd79df18047811eab259ac1f6b220ee8/

[10] KARÁSEK, Jiří. FOTOGRAFICKÁ MONTÁŽ. Fotoaparat.cz [online]. 2005 [cit. 2020-08-03]. Dostupné z: https://www.fotoaparat.cz/clanek/381/fotograficka-montaz-10056/

[11] MAŠA, Vojtěch. Rozumím - Razumem [online]. [cit. 2020-08-04]. Dostupné z: https://is.muni.cz/th/xm51e/vojtech_masa-master_thesis.pdf

[12] DORAZÍN, Martin. Moskvané stojí fronty před Treťjakovskou galerií. Událostí sezony se stala retrospektiva avantgardisty El Lisického. Radiozurnal.rozhlas.cz [online]. 2017 [cit. 2020-08-05]. Dostupné z: https://radiozurnal.rozhlas.cz/moskvane-stoji-fronty-pred-tretjakovskou-galerii-udalosti-sezony-se-stala-7182443

[13] Adolf The Superman. Heartfield's Famous Portrait Of Adolf Hitler Swallowing Money From Supporters To Spout Fascist Garbage. Johnheartfield.com [online]. [cit. 2020-08-05]. Dostupné z: https://www.johnheartfield.com/John-Heartfield-Exhibition/john-heartfield-art/famous-anti-fascist-art/heartfield-posters-aiz/adolf-the-superman-hitler-portrait

[14] Český modernismus zaplavuje New York. Tyden.cz [online]. 2007 [cit. 2020-08-05]. Dostupné z: https://www.tyden.cz/rubriky/kultura/umeni/cesky-modernismus-zaplavuje-new-york_27289.html?showTab=nejctenejsi-3

[15] LEE, Daniel. Manimals. Daniellee.com [online]. [cit. 2020-08-05]. Dostupné z: http://www.daniellee.com/projects/manimals

[16] The Digital Age. Jordanfullerphoto.blogspot.com [online]. 2011 [cit. 2020-08-05]. Dostupné z: http://jordanfullerphoto.blogspot.com/2011/10/digital-age-dun-dun-dun-dunhh.html

[17] LAIN, Stanley. 'That's Photoshopped!' Yeah, so Does That Mean All Our Photos Are Fake? Fstoppers.com [online]. 2020 [cit. 2020-08-03]. Dostupné z: https://fstoppers.com/originals/thats-photoshopped-yeah-so-does-mean-all-our-photos-are-fake-451724

[18] ADAMS, Ansel. The Tetons and the Snake River, Grand Teton National Park. Philamuseum.org [online]. [cit. 2020-08-05]. Dostupné z: https://www.philamuseum.org/collections/permanent/123315.html?mulR=977

[19] TIP#180: Jak najdu odkud pochází nějaká fotografie? Jak zjistím kdo je autorem? 365tipu.cz [online]. 2015 [cit. 2020-08-03]. Dostupné z:

https://365tipu.cz/2015/06/29/tip180-jak-najdu-odkud-pochazi-nejaka-fotografie-jak-zjistim-kdo-je-autorem/

[20] TENGYUEN, Ngan. 4 Free Fake Image Detector – Analyze Photoshopped Photos. Geckoandfly.com [online]. 2020 [cit. 2020-08-03]. Dostupné z: https://www.geckoandfly.com/10023/analyze-photoshopped-photos-with-fbi-csi-and-cia-fotoforensics-software/

[21] Submit a JPEG or PNG for Forensic Analysis. Fotoforensics.com [online]. [cit. 2020-08-03]. Dostupné z: http://fotoforensics.com/

[22] Frequently Asked Questions. Fotoforensics.com [online]. [cit. 2020-08-03]. Dostupné z: http://fotoforensics.com/faq.php

[23] Challenge. Fotoforensics.com [online]. [cit. 2020-08-03]. Dostupné z: http://fotoforensics.com/messages.php?read=1420247530700&challenge=1

[24] HASS, Calvin. JPEGsnoop 1.8.0 - JPEG File Decoding Utility. Impulseadventure.com [online]. 2017 [cit. 2020-08-03]. Dostupné z: https://www.impulseadventure.com/photo/jpeg-snoop.html

[25] What is Ghiro. Getghiro.org [online]. [cit. 2020-08-03]. Dostupné z: http://www.getghiro.org/

[26] Photo upload. Imageforensic.org [online]. [cit. 2020-08-03]. Dostupné z: https://www.imageforensic.org/

[27] Forensically [online]. [cit. 2020-08-04]. Dostupné z: https://29a.ch/photo-forensics/#forensic-magnifier

[28] WAGNER, Jonas. Noise Analysis for Image Forensics. 29a.ch [online]. 2015 [cit. 2020-08-03]. Dostupné z: https://29a.ch/2015/08/21/noise-analysis-for-image-forensics/

[29] PHOTO ANALYSIS AND TAMPERING DETECTION. Ampedsoftware.com [online]. [cit. 2020-08-05]. Dostupné z: https://ampedsoftware.com/authenticate

[30] KASÍK, Pavel. New York odměnil český program, který rozpozná zfalšované fotky. Idnes.cz [online]. 2011 [cit. 2020-08-05]. Dostupné z: https://www.idnes.cz/technet/software/new-york-odmenil-cesky-program-ktery-rozpozna-zfalsovane-fotky.A110411_114942_tec_technika_pka

[31] ENGLAND, Lucy. There's an algorithm that can see whether a photo has been faked. Businessinsider.com [online]. 2015 [cit. 2020-08-05]. Dostupné z:

https://www.businessinsider.com/verifeyed-czech-tech-startup-detects-fake-and-manipulated-images-2015-7#back-in-2004-a-group-of-scientists-and-digital-experts-led-by-babak-mahdian-came-together-in-prague-with-one-goal-to-build-a-toolkit-that-could-instantly-detect-whether-an-image-had-been-tampered-with-1

[32] Tutorial: Error Level Analysis. Fotoforensics.com [online]. [cit. 2020-08-05]. Dostupné z: https://fotoforensics.com/tutorial-ela.php

[33] Evaluating ELA. Fotoforensics.com [online]. [cit. 2020-08-03]. Dostupné z: http://fotoforensics.com/tutorial.php?tt=ela

[34] Lossy & Lossless. Fotoforensics.com [online]. [cit. 2020-08-05]. Dostupné z: http://fotoforensics.com/tutorial.php?tt=ela

[35] ZEMAN, Jan. Jak rozumět EXIFu aneb co jsou metadata a jak je využít. Milujemefotografii.cz [online]. 2018 [cit. 2020-08-03]. Dostupné z: https://www.milujemefotografii.cz/jak-rozumet-exifu-co-jsou-metadata

[36] ŠUTOVÁ, Marijana. OBRAZOVÝ HOAX: JAK HO ROZEZNAT. Zvolsi.info [online]. 2018 [cit. 2020-08-04]. Dostupné z: https://zvolsi.info/2018/09/23/obrazovy-hoax-jak-ho-rozeznat/

# SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

| | |
|---|---|
| ELA | Error Level Analysis |
| EXIF | Exchangeable Image File Format |
| IPTC | International Press Telecommunications Council |
| GPS | Global Positioning System |
| JPEG | Joint Photographic Experts Group |
| PNG | Portable Network Graphics |
| HTML | Hypertext Markup Language |
| CSS | Cascading Style Sheets |
| NASA | National Aeronautics and Space Administration |
| OSN | Organizace spojených národů |
| AVI | Audio Video Interleave |
| DNG | Digital Negative |
| PSD | Photoshop Document |
| MOV | QuickTime Movie |
| PDF | Portable Document Format |
| TIFF | Tagged Image File Format |
| BMP | Bitmap |
| XMP | Extreme Memory Profile |

# SEZNAM OBRÁZKŮ

# SEZNAM TABULEK

# SEZNAM PŘÍLOH

# PŘÍLOHA 1: ORIGINÁLNÍ TESTOVACÍ FOTOGRAFIE

# PŘÍLOHA 2: UPRAVENÉ TESTOVACÍ FOTOGRAFIE


HELLO
Multivitamin