Journal of Information Technologies, Vol. 9, No. 1, 2016, ISSN: 1337-7467

Ovplyvňovanie kvality fotografických diel chránených steganografiou a jej implementácia v prostredí Matlab

Influencing of the quality of photo works protected by steganography and its implementation in the MATLAB environment

Robert Halenár, Fakulta masmediálnej komunikácie, Univerzita Sv. Cyrila a Metoda v Trnave, Slovenská republika

Abstract: Protection of photographic works in the online environment is prior and necessary. One of the ways that is cheap and effective is an implementation of the safeguards identifier directly into the picture. For this purpose we use steganography infiltration. Implementation is automated and is provided in Matlab script that is simple and computing very fit and flexible. We reviews the way we implement this process. It is possible to see and understand the script that interprets the main algorithm for the steganography infiltration and also result in a photo in which it was placed steganography identifier in different bit depths.

Key words: Algorithm, photography, steganography, copyright

Abstrakt: Ochrana fotografických autorských diel je v online prostredí prioritná a potrebná. Jeden zo spôsobov, ktorý je lacný a účinný je aj implementácia ochranného identifikátora priamo do fotografie. Pre tento účel používame steganografickú infiltráciu. Implementácia je automatizovaná a je zabezpečená skriptom v prostredí Matlab, ktoré je jednoduché a výpčtovo veľmi zdatné a flexibilné. V článku uvádzame spôsob, akým sme tento proces implementovali. Je možné si prezrieť a pochopiť skript, ktorý interpretuje hlavný agoritmus vkladania steganografickej infiltrácie a zároveň aj výsledok na fotografii v ktorej bol identifikátor umiestnený steganografiou v rôznych bitových hĺbkach.

Kľúčové slová: Algoritmus, fotografia, steganografia, autorská ochrana

1 Ochrana autorských práv fotografických diel

Fotografia spĺňa podmienky vlastnej tvorivej duševnej činnosti autora a považuje sa za fotografické dielo. Autorovi takéhoto fotografického diela prislúchajú k fotografii autorské práva, ktoré sa skladajú z osobnostnej a majetkovej zložky. Autorské práva k fotografii

vznikajú už jej vytvorením a na preukázanie autorských práv k fotografii nie je potrebná žiadna registrácia, pretože tie vznikajú priamo zo zákona. Hoci je vznik autorských práv k fotografii automatický a nie je potrebná ich registrácia, prináša to so sebou aj nevýhody, pretože bez registrácie nie je jasne a jednoducho preukázateľné, kto má k tej ktorej fotografii autorské práva. Tento stav následne nahráva plagiátorom. Autor fotografie preto na preukázanie svojich práv k fotografii musí využiť všetky prostriedky, právne aj technické, aby jeho autorstvo k fotografii bolo zjavné a preukázateľné. Jednou zo základných vecí, ktorú by mal každý autor fotografie urobiť, je realizovať svoje základné právo a fotografiu označiť svojim menom alebo pseudonymom. Označenie na fotografii možno urobiť vložením mena autora priamo na fotografiu, alebo pod fotografiu, pričom k menu možno dodať aj znak © (copyright, copyrightová doložka) a dátum vytvorenia diela. Označenie autorstva možno dať tiež pod fotografiu, či vedľa nej. Na označenie fotografie menom autora v elektronickej podobe existujú aj viaceré technické spôsoby, ktoré by mali preventívne pôsobiť ako dôkaz autorstva: [1]

Uchovávať originálne fotografie s presným a pôvodným exifom (súborom informácií, ktoré sú priložené pri každom obrázku, ktorý fotoaparátom vyfotografujete). Exif môže niesť informácie o:

- autorovi
- dátume a čase vyhotovenia, prípadne zmeny obrázku
- údajoch o fotoaparáte a objektíve (značka, presný model)
- údajoch o expozícii (expozičné hodnoty času a clony ale aj ostatné nastavenia fotoaparátu)

Toto sú základné informácie, ktoré súbor s metadatami môže obsahovať. Výhodou je to, že si do Exifu v niektorých programoch môžete zapísať aj meno, či iné údaje o autorstve. V niektorých programoch si dokonca môžete zamknúť tieto informácie. Nevýhodou je však to, že veľa programov umožňuje meniť informácie v exife, dokonca aj také, ktoré sú zamknuté. V podstate každý softvér a digitálny zámok je napadnuteľný hackermi.

2. Zaobstarať si drahší (rádovo v stovkách eur) tzv. autorizačný softvér, ktorý ku každej fotografii pripája unikátny kód a registruje fotografie do databázy.

3. Do fotografií, ktoré chceme potenciálne predávať alebo nimi niečo dokázať, môžeme vsadiť vodoznak. Vodoznak (polo-priehľadný alebo priesvitný znak, ktorý dovoľuje

fotografiu prezrieť a zhodnotiť jej obsah a kvalitu, ale vzhľadom na to, že fotografiu prekrýva, nedovoľuje ju použiť na komerčné účely alebo inak neoprávnene použiť) sa však dá v rôznych softvéroch odstrániť, ale čím je zložitejší a zreteľnejší, tým je ťažšie odstrániteľný.

Všetky tieto spôsoby majú rad nevýhod. Sú všeobecne známe, resp ochraňujú autorstvo ľahko odstrániteľnými značkami, alebo sú relatívne nákladné.

Fotografi ktorí fotia na film majú preukazovanie autorstva jednoduchšie v tom, že disponujú negatívom, ktorý by mal preukázať, že ten, kto negatív vlastní, je aj autorom fotografií. V prípade digitálnej fotografie je dokazovanie pôvodu zložitejšie, o to viac ak je fotografia umiestnená na verejne dostupnom digitálnom úložisku alebo Internete.

Ak sú umiestnené fotografie on-line, nemôže si byť autor istý ničím čo ochráni jeho právo. Skripty „right-click“ môžeme obísť priamo zobrazením zdroja, rozbaľovacie obrázky je možné obísť rovnakým spôsobom, vodoznak môže byť odstránený (niekedy s ťažkosťami). Dokonca aj keď je fotografia vložená do objektu Flash, je možné ľahko vytvoriť kópiu obrazovky. [2]

V takom prípade musí autor hľadať alternatívny spôsob ochrany. Vhodnou alternatívou je umiestnenie informácie o autorovi priamo do fotografie (nie však notoricky známe metadáta).

2 Zakódovanie informácie o autorovi

Priamo do dát fotografie je možné umiestniť informáciu, ktorá nie je priamo viditeľná ale môže pomôcť pri dokazovaní autorských práv. Na jej umiestnenie sú použité priamo pixely ktoré zobrazujú fotografiu. Jedná sa teda o spôsob, ktorý je obdobou vodoznaku, avšak nie je priamo viditeľný (dokonca v mnohých prípadoch ľudským okom nerozoznateľný).

Princíp spočíva v kóde (alebo šifre) – jednoduchom hesle skladajúcom sa z niekoľkých znakov (meno, priezvisko, alebo iný identifikátor), ktoré je preložené pomocou ASCII tabuľky na čísla v dekadickej sústave, ktoré sú prevedené do binárneho tvaru, pozri Obr. 1.

Dec	Hx	Oct	Char	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr
0	0	000	NUL (null)	32	20	040		Space	64	40	100	@	@	96	60	140	`	`
1	1	001	SOH (start of heading)	33	21	041	!	!	65	41	101	A	A	97	61	141	a	a
2	2	002	STX (start of text)	34	22	042	"	"	66	42	102	B	B	98	62	142	b	b
3	3	003	ETX (end of text)	35	23	043	#	#	67	43	103	C	C	99	63	143	c	c
4	4	004	EOT (end of transmission)	36	24	044	$	$	68	44	104	D	D	100	64	144	d	d
5	5	005	ENQ (enquiry)	37	25	045	%	%	69	45	105	E	E	101	65	145	e	e
6	6	006	ACK (acknowledge)	38	26	046	&	&	70	46	106	F	F	102	66	146	f	f
7	7	007	BEL (bell)	39	27	047	'	'	71	47	107	G	G	103	67	147	g	g
8	8	010	BS (backspace)	40	28	050	(	(	72	48	110	H	H	104	68	150	h	h
9	9	011	TAB (horizontal tab)	41	29	051	)	)	73	49	111	I	I	105	69	151	i	i
10	A	012	LF (NL line feed, new line)	42	2A	052	*	*	74	4A	112	J	J	106	6A	152	j	j
11	B	013	VT (vertical tab)	43	2B	053	+	+	75	4B	113	K	K	107	6B	153	k	k
12	C	014	FF (NP form feed, new page)	44	2C	054	,	,	76	4C	114	L	L	108	6C	154	l	l
13	D	015	CR (carriage return)	45	2D	055	-	-	77	4D	115	M	M	109	6D	155	m	m
14	E	016	SO (shift out)	46	2E	056	.	.	78	4E	116	N	N	110	6E	156	n	n
15	F	017	SI (shift in)	47	2F	057	/	/	79	4F	117	O	O	111	6F	157	o	o
16	10	020	DLE (data link escape)	48	30	060	0	0	80	50	120	P	P	112	70	160	p	p
17	11	021	DC1 (device control 1)	49	31	061	1	1	81	51	121	Q	Q	113	71	161	q	q
18	12	022	DC2 (device control 2)	50	32	062	2	2	82	52	122	R	R	114	72	162	r	r
19	13	023	DC3 (device control 3)	51	33	063	3	3	83	53	123	S	S	115	73	163	s	s
20	14	024	DC4 (device control 4)	52	34	064	4	4	84	54	124	T	T	116	74	164	t	t
21	15	025	NAK (negative acknowledge)	53	35	065	5	5	85	55	125	U	U	117	75	165	u	u
22	16	026	SYN (synchronous idle)	54	36	066	6	6	86	56	126	V	V	118	76	166	v	v
23	17	027	ETB (end of trans. block)	55	37	067	7	7	87	57	127	W	W	119	77	167	w	w
24	18	030	CAN (cancel)	56	38	070	8	8	88	58	130	X	X	120	78	170	x	x
25	19	031	EM (end of medium)	57	39	071	9	9	89	59	131	Y	Y	121	79	171	y	y
26	1A	032	SUB (substitute)	58	3A	072	:	:	90	5A	132	Z	Z	122	7A	172	z	z
27	1B	033	ESC (escape)	59	3B	073	;	;	91	5B	133	[	[	123	7B	173	{	{
28	1C	034	FS (file separator)	60	3C	074	<	<	92	5C	134	\	\	124	7C	174			|
29	1D	035	GS (group separator)	61	3D	075	=	=	93	5D	135	]	]	125	7D	175	}	}
30	1E	036	RS (record separator)	62	3E	076	>	>	94	5E	136	^	^	126	7E	176	~	~
31	1F	037	US (unit separator)	63	3F	077	?	?	95	5F	137	_	_	127	7F	177	&#127;	DEL

Source: www.LookupTables.com

Obrázok 1: Obr. 1: ASCII Tabuľka [3]

Majme identifikátor „ALABAMAZZ“, ktorý pomocou ASCII tabuľky preložíme tak ako ukazuje obrázok 2 (na automatizáciu prekladu bolo použité prostredie Matlab).

```
>> double('ALABAMAZZ')

ans =

    65    76    65    66    65    77    65    90    90
```

Obrázok 2: Dekadické kódy znakov identifikátora podľa ASCII tabuľky

Každý znak je vyjadrený číselnou reprezentáciou. Následne skonvertujeme čísla dekadickej sústavy do binárneho tvaru ako ukazuje obrázok 3.

```
>> str=double('ALABAMAZZ');
>> dec2bin(str)

ans =

1000001
1001100
1000001
1000010
1000001
1001101
1000001
1011010
1011010
```

Obrázok 3: Binárne kódy dekadickej reprezentácie znakov identifikátora podľa ASCII tabuľky

Takáto binárna postupnosť je následne zakódovaná do jednotlivých bodov fotografie.

3 Aplikácia steganografie a jej vplyv na zmenu kvalitu fotografie

Na umiestnenie steganografickej infiltrácie sa v rastrovej grafike používa posledný bit každého pixelu obrázka, tzv LSB – Last Significant Bit. LSB sa používa preto, pretože jeho vplyv na zmenu kvality je najmenší, v mnohých prípadoch aj zanedbateľný. Ak je použité štandardné vyhotovenie v kvalite True Color (24 bitová grafika), je pre každý pixel k dispozícii 24 bitov, teda pri farebnom modely napr. RGB pre každú farebnú zložku pripadá 8 bitová informácia, čo je 256 odtieňov. Celkovo je teda k dispozícii pre každý pixel 256^3 možností, čo je cca 16.7 milióna farieb. Ak použijeme LSB, zostane k dispozícii pre každý pixel 128^3 možností, čo je cca 2.1 milióna farieb. Teda ľudským zrakom nepozorovateľná zmena kvality.

Na obrázku 4 je ukážka fotografie, na ktorú bola aplikovaná steganografická infiltrácia. Postupne smerom do pravej strany sa zvyšuje masívnosť steganografockej infiltrácie od 1 až po hĺbku posledných 4 bitov. Ľudským okom sa pri infiltrácii v LSB nedá na bežných zobrazovacích zariadeniach rozoznať zmena kvality a to ani pri detailnejšom zobrazení. Ak je však infiltrácia rozšírená do ďalších bitov v poradí od najmenšieho dochádza postupne k pozorovateľnej zmene kvality. Na obrázku 4 je v druhej časti zľava steganografická infiltrácia aplikovaná na dva posledné bity, celkovo je teda k dispozícii pre každý pixel 64^3 možností, čo je cca 262,144 farieb.

Steganografická infiltrácia aplikovaná na tri posledné bity, celkovo je teda k dispozícii pre každý pixel 32^3 možností, čo je cca 32,768 farieb. Steganografická infiltrácia aplikovaná na štyri posledné bity, celkovo je k dispozícii pre každý pixel len 16^3 možností, čo je cca 4,096 farieb. Zmena kvality je jasne vidieť na odtieňoch šedej v oblasti rúk.

Obrázok 4: Porovnanie steganografickej infiltrácie pri rôznych bitových hĺbkach z ľava od 1 až po 4 bit, pôvodná fotografia [4]

Steganografická infiltrácia je aplikovaná do fotografie pomocou skriptu zostrojeného pre prostredie Matlab, ktorého ukážka hlavnej časti kódu je na obrázku č.5. Premenná „bit“ uvádza ktorý bit sa nastavuje a premenná Color v ktorej farebnej zložke (Red, Green alebo Blue v skratkách R, G a B). Keďže identifikátor, ktorý implementujeme do steganografickej infiltrácie pozostáva z deviatich znakov a každý znak je pritom identifikovaný v ASCII tabuľke 7 bitmi, celkotá dĺžka potrebná na umiestnenie steganografickej infiltrácie je 63 bitov. Ak teda umiestnime infiltráciu do prvého bitu každej farebnej zložky, na jeden výskyt budeme potrebovať 21 pixelov (pre každý pixel 3 bity vo farebných zložkách RGB).

Takto aplikovaná ochrana fotografie je bezpečná, voľným okom nerozpoznateľná a ťažko odstrániteľná, pretože sa môže nachádzať len v jednej časti fotografie, alebo na viacerých miestach, prípadne, môže byť masovo implementovaná v každom pixely v celej fotografii.

Preukázať, že infiltrácia sa nachádza vo fotografii vyžaduje špeciálne prístupy steganalýzy a prehľadanie veľkého množstva dát. [5]

```
% Premenná bit uvádza ktorý bit sa nastavuje a premenná Color v ktorej
farebnej zložke
bit=7;
R=1;G=2;B=3;
Color=R;
% Hodnotu n-tého bitu v R zložke z RGB nastaví na code bit v 21 pixeloch
(63:3)
b=0;
  for i=1:mn(1)
    for j=1:mn(2)
      % Hodnotu RGB zvysi o code bit v 21 pixeloch (63:3)
      if b<63
        b=b+1;
      else
        b=1;
      end;

          Color_b=dec2bin(X(i,j,Color));

          sRGB=size(Color_b);

                                                              if sRGB(2)<bit
              if code(b)==dec2bin(1)
                  for k=Color:Color
                      X(i,j,k)=2^(bit-1);
                  end;
              end;
          else
              if code(b)~=Color_b(sRGB(2)-bit+1)
                  for k=Color:Color
                      %Optimalizacia hodnoty upravy LSB
                      X(i,j,k)=X(i,j,k)+2^(bit-1);
                  end;
              end;
          end;

    end;
  end;
```

Obrázok 5: Hlavný algoritmus vloženia steganografickej infiltrácie pre prostredie Matlab

4 Zhodnotenie

V článku sme ukázali akým spôsobom vkladáme steganografickú infiltráciu priamo do fotografie, popísali sme jej automatizovanú verziu pomocou prostredia Matlab, pričom uvádzame aj hlavný algoritmus. Do fotografie vložený Identifikátor „ALABAMAZZ“ čo nemení viditeľným spôsobom jej kvalitu a je ľudským okom bežne nerozoznateľný až do hĺbky 3 bitov, je ale merateľný a následne rekonštruovateľný. V bitovej hĺbke 4 bity bola pozorovateľná zhoršená úroveň kvality v oblasti rúk, kde je na relatívne veľkej ploche plynulé tieňovanie. Prostredie Matlab sme zvolili pretože je veľmi vhodné na implementáciu aj zložitejších matematických algoritmov, čo nám do budúcna umožňuje napríklad šifrovanie steganografickej infiltrácie identifikátora autora kvôli vyššej bezpečnosti a ťažšiemu odstráneniu identifikátora z fotografického diela.

Zoznam bibliografických odkazov

(1) BABIAKOVÁ, K.: *Praktické rady ako chrániť autorské práva.* [online] [cit. 2.03.2016], Dostupné na: http://www.ephoto.sk/photopointy/photopointy-cz/vysocina/prakticke-rady-ako-chranit-autorske-prava/

(2) KIRNIN, J.: *How to Protect Your Digital Photos from Being Copied.* [online] [cit. 2.03.2016], Dostupné na: http://webdesign.about.com/od/graphics/a/aa102406.htm

(3) ASCII Tabuľka, [online] [cit. 2.03.2016], Dostupné na: http://www.asciitable.com/

(4) Главная причина неудач стартапов - преждевременное масштабирование [online] [cit. 2.03.2016], Dostupné na: http://www.garagebiz.ru/view/glavnaya_prichina_neudach_startapov_-_prezhdevremennoe_masshtabirovanie/startapi

(5) TRNKA, A.: *Analýza neštruktúrovaných textových dát*. In: Anna Zaušková, Rudolf Rybanský (eds.): Marketing Identity 2014, Trnava, 2014, s. 108 – 114, ISBN 978-80-8105-668-0

Adresa autora:

Robert Halenár, Ing. PhD.
Univerzita sv. Cyrila a Metoda v Trnave
Fakulta masmediálnej komunikácie
Nám. J. Herdu 2
917 00 Trnava
Slovak republic
robert.halenar@ucm.sk