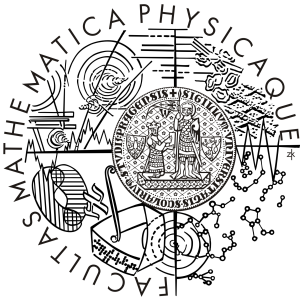
Univerzita Karlova v Praze
Matematicko-fyzikální fakulta

BAKALÁRSKA PRÁCA



Roman Cinkais

Steganografie a steganoanalýza

Katedra algebry

Vedúci bakalárskej práce: RNDr. David Stanovský, Ph.D
Študijný program: Matematické metody informační bezpečnosti

2007

Ďakujem RNDr. Davidovi Stanovskému, Ph.D. za odborné konzultácie a relevantné pripomienky k práci, vďaka čomu sa práca posunula na vyšší stupeň. Ďalej by som chcel poďakovať Ing. Jánovi Chabadovi za poskytnutie konzultácie v oblasti programovacieho jazyka Java a Ivanovi Štubňovi za pomoc pri písaní textu v TeXu.

Prehlasujem, že som svoju bakalársku prácu napísal samostatne a výhradne s použitím citovaných prameňov. Súhlasím so zapožičiavaním práce.

V Prahe dňa 13.7.2007 Roman Cinkais

Obsah

Názov práce: Steganografia a steganoanalýza
Autor: Roman Cinkais
Katedra: Katedra algebry
Vedoucí bakalářské práce: RNDr. David Stanovský, Ph.D
e-mail vedoucího: stanovsk@karlin.mff.cuni.cz

Abstrakt:
Steganografia je umenie ako ukryť alebo zakryť správu. Účel steganografie je kamuflovať(podviesť) komunikáciu - utajiť existenciu správy pre tretiu stranu. Na začiatok sa budem venovať technickému úvodu do steganografie pre tých, ktorým je táto oblasť vedy neznáma. Ďalej sa budem venovať historickému kontextu, ale hlavný dôraz budem klásť na digitálne aplikácie steganografie, najmä na ukrývanie informácie do obrázkov a audio súborov. Príklady softwaru používajúceho steganografiu alebo steganoanalýzu budem tak isto prezentovať.

Kľúčové slová: steganografia, steganoanlýza, ukrývanie

Title: Steganography and steganalysis
Author: Roman Cinkais
Department: Department of algebra
Supervisor: RNDr. David Stanovský, Ph.D
Supervisor's e-mail adress: stanovsk@karlin.mff.cuni.cz

Abstract:
Steganography is the art of covered or hidden writing. The purpose of steganography is covert communication-to hide the existence of a message from a third party. The beginnig is intended as a technical introduction to steganography for those unfamiliar with the field. Below this paper provides a historical context for steganography, but the emphasis is on digital applications, focusing on hiding information in image or audio files. Examples of software tools that employ steganography to hide data inside of other files as well as software to detect such hidden files will also be presented.

Keywords: steganography, steganalysis, hiding

1

PREHĽAD STEGANOGRAFIE

1.1. Úvod.

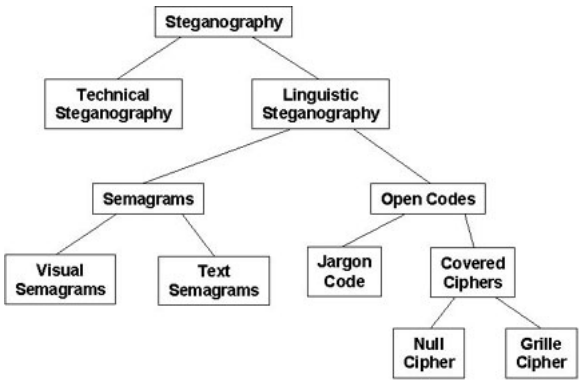
Steganografia je umenie ako ukryť alebo zakryť správu. Účel steganografie je kamuflovať(podviesť) komunikáciu - utajiť existenciu správy pre tretiu stranu. Tým sa líši od kryptografie. Niektorí autori však považujú steganografiu ako formu kryptografie odkedy je tajná komunikácia považovaná za tajné písance [**5**].

Aj keď termín steganografia sa začal používať na konci 15-teho storočia, použitie steganografie siaha až do dávnej minulosti. V staroveku boli správy skrývané na zadnú stranu voskových tabuliek (zaliali sa voskom a nebolo ich vidieť), na králičí žalúdok, alebo boli vytetované na hlavu otroka (a čakalo sa kým mu dorástli vlasy). Neviditelný atrament sa používa po stáročia - dnes už skôr pre zábavu ale takisto pre špionáže teroristov. Mikrobody a mikrofilmy, neoddeliteľná súčasť vojny a špionážnych filmov, sa začali používať až po vytvorení fotografií [**2**][**23**][**24**][**36**]).

Steganografia ukrýva nejakú správu, ale nie fakt, že medzi oboma partiami prebieha komunikácia. Steganografický proces všeobecne zahŕňa vloženie utajovanej správy na transportné médium nazývané nosič. Tajná správa je vložená (zabudovaná) do nosiča a vytvára takzvané steganografické médium. Steganografický kľúč môže byť použitý pre kódovanie skrývanej správy a/alebo pre vygenerovanie náhodnej steganografickej schémy. V skutočnosti:

steganografické médium = ukrývaná správa + nosič + steganografický kľúč

Obrázok 1.1 ukazuje obvyklú systematiku steganografických techník [**2**][**5**].



Obrázok 1.1. Klasifikácia steganografických techník (prispôsobené podľa [**5**]).

- **Technická steganografia (Technical steganography)** využíva vedecko-technické metódy na ukrytie správy, ako je napríklad použitie neviditeľného atramentu alebo mikrobodov a ostatných veľkosť redukujúcich metód.

- **Lingvistická (jazyková) steganografia (Linguistic steganography)** ukrýva správu do nosiča v nie veľmi zreteľnom spôsobe a je ďalej triedená na semagramy a otvorené kódy.

- **Semagramy (Semagrams)** ukrývajú správu pomocou symbolov a znakov. **Vizuálny (obrazový) semagram (Visual semagrams)** využíva nevinne vyzerajúce objekty alebo veci, s ktorými sa stretávame každý deň, ako napríklad čmárance alebo ukladanie vecí na stôl v určitom poradí alebo na webovú stránku, na to, aby sa správa dostala k druhej strane. **Textový semagram (Text semagrams)** ukrýva správu modifikovaním vzhľadu textu na nosiči, napríklad jemné úpravy vo veľkosti a typu písma, pridávanie extra medzier, alebo odlišné ozdobenie písma v dopise.

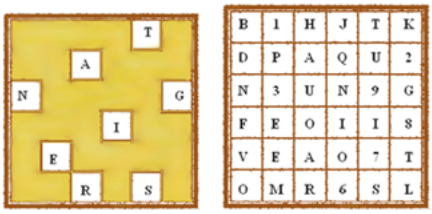
- **Otvorené kódy (Open codes)** ukrývajú správu na pravú správu nosiča tak, že to nič netušiacemu pozorovateľovi nepríde zreteľné. Takáto správa na nosiči sa niekedy nazýva vyložená alebo jasná komunikácia, zatiaľ čo ukrývaná správa je utajovaná komunikácia. Táto kategória sa ešte delí na žargónové kódy a skryté šifry.

- **Žargónové kódy (Jargon codes)**, ako napovedá názov, používajú jazyk, ktorý ovláda len istá skupina ľudí a je nezrozumiteľný pre ostatných. Žargónové kódy zahrňujú warchalking (symboly používané na indikovanie prítomnosti a typu signálu bezdrôtovej siete [Warchalking 2003]). iné terminológie, alebo prostú komunikáciu, ktorá prevádza špeciálny zmysel nejakého faktu, ktorý je známy len konkrétnej osobe. Podmnožinou žargónových kódov sú **pokynové kódy (Cue codes)**, kde určité dopredu dohodnuté frázy plnia svoj zmysel.

- **Skryté alebo ukryté šifry (Covered ciphers)** ukrývajú správu otvorenú na nosič tak, aby ju bolo možné obnoviť len niekým, kto pozná tajomstvo, ako to bolo ukrývané. **Zamrežová šifra (Grille cipher)** využíva vzor (šablonu), ktorý je používaný na pokrytie správy nosiča. **Nulová šifra (Null cipher)** ukrýva správu na základe nejakej preddefinovanej množine pravidiel, ako napríklad "čítaj každé piate slovo" alebo "čítaj tretie písmeno v každom slove".

Zväčšovaním množstva dát ukladaného na počítač a posielaním jeho obsahu po sieti nie je prekvapujúce, že steganografia vstupuje do digitálneho veku. Steganografia na počítači a na sieti umožnuje ukrývať nejaký typ binárnych súborov do iného binárneho súboru. Obrázok a audio súbor sú dnes najviac používané nosiče.

Steganografia poskytuje niektoré veľmi užitočné a zaujimavé funkcie v digitálnom svete, z čoho je najviac používaný digitálny watermarking. V takejto aplikácii môže autor vložit ukrývanú správu do súboru, takže neskôr môže pomocou toho



Obrázok 1.2. Grille cipher.

potvrdiť vlastníctvo daného súboru. Napríklad maliar by mohol poslať prostredníctvom internetu svoje originálne dielo. Ak niekto ukradne tento súbor a bude tvrdiť, že obraz je jeho, maliar môže neskôr bez problémov dokázať vlastníctvo, pretože on jediný je schopný obnoviť watermark [**2**][**4**][**25**]. Aj keď je watermarking konceptuálne podobný steganografii, väčšinou má rozdielne technické smery.

Steganografia podporuje množstvo nelegálnych aplikácií, najviac známe je napríklad ukrývanie ilegálnych nahrávok, finančných podvodov, priemyslových špiónáži, a komunikácie medzi členmi nejakej teroristickej alebo zločinnej organizácie [**18**]).

1.2. Nulová šifra.

Historicky sú nulové šifry spôsobom, ako ukryť správu do inej bez použitia komplikovaného algoritmu. Ukážeme si príklad jednu z najjednoduchších nulových šifier:

PRESIDENT'S EMBARGO RULING SHOULD HAVE IMMEDIATE NOTICE. GRAVE SITUATION AFFECTING INTERNATIONAL LAW. STATEMENT FORESHADOWS RUIN OF MANY NEUTRALS. YELLOW JOURNALS UNIFYING NATIONAL EXCITEMENT IMMENSELY.

APPARENTLY NEUTRAL'S PROTEST IS THOROUGHLY DISCOUNTED AND IGNORED. ISMAN HARD HIT. BLOCKADE ISSUE AFFECTS PRETEXT FOR EMBARGO ON BYPRODUCTS, EJECTING SUETS AND VEGETABLE OILS.

Nemecká ambasáda vo Washingtone, DC, poslala túto správu v telegrame do centrály v Berlíne počas prvej svetovej vojny (Kahn 1996). Keď prečítame prvé písmeno z každého slova v prvej správe a druhé písmeno z každého slova v druhej správe, dostaneme nasledujúci skrytý text:

PERSHING SAILS FROM N.Y. JUNE 1

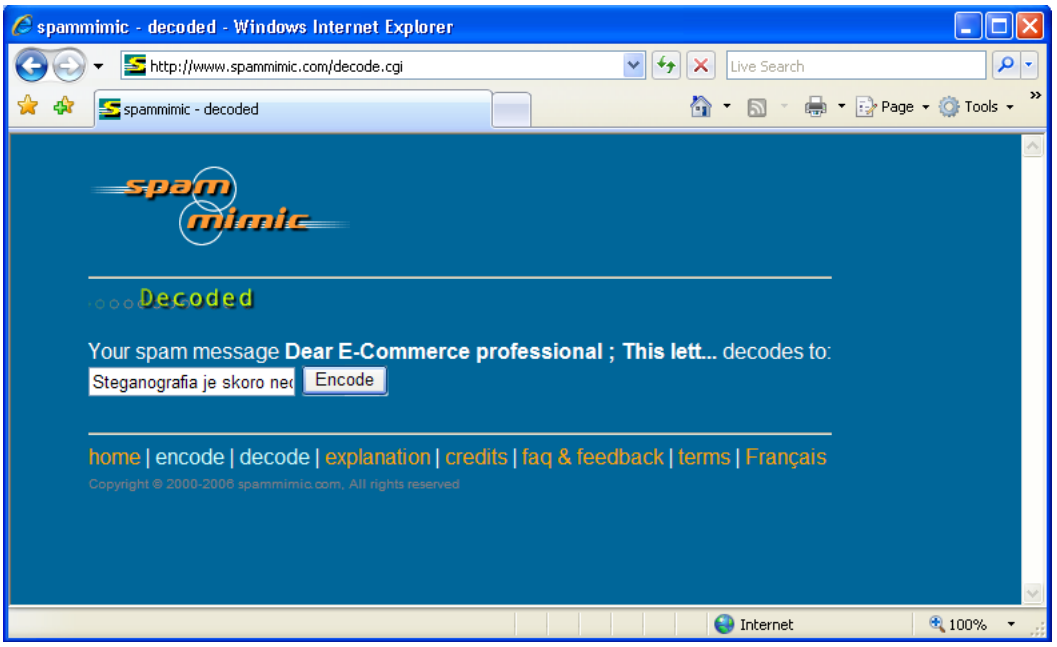
Na internete je spam potenciálnym nosičom pre ukrývanú správu. Skúste zvážiť nasledujúci text:

Dear E-Commerce professional ; This letter was specially selected to be sent to you . This is a one time mailing there is no need to request removal if you won't want any more . This mail is being sent in compliance with Senate bill 1916 , Title 6 ; Section 304 . Do NOT confuse us with Internet scam artists ! Why work for somebody else when you can become rich as few as 94 months ! Have you ever noticed most everyone has a cellphone and nobody is getting any younger ! Well, now is your chance to capitalize on this . WE will help YOU use credit cards on your website & use credit cards on your website ! You are guaranteed to succeed because we take all the risk ! But don't believe us . Prof Jones of Wisconsin tried us and says "I was skeptical but it worked for me" . We are a BBB member in good standing ! DO NOT DELAY - order today . Sign up a friend and you get half off ! Thanks ! Dear Salaryman , This letter was specially selected to be sent to you ! We will comply with all removal requests . This mail is being sent in compliance with Senate bill 1618 ; Title 4 , Section 302 ! Do NOT confuse us with Internet scam artists ! Why work for somebody else when you can become rich within 82 weeks ! Have you ever noticed nearly every commercial on television has a .com on in it & people love convenience . Well, now is your chance to capitalize on this ! We will help you use credit cards on your website & SELL MORE ! You can begin at absolutely no cost to you . But don't believe us . Mrs Ames of Iowa tried us and says "Now I'm rich, Rich, RICH" . We assure you that we operate within all applicable laws . Do not delay - order today . Sign up a friend and you get half off ! Thanks . Dear Business person , This letter was specially selected to be sent to you ! We will comply with all removal requests . This mail is being sent in compliance with Senate bill 2616 ; Title 8 ; Section 306 ! Do NOT confuse us with Internet scam artists ! Why work for somebody else when you can become rich inside 39 weeks . Have you ever noticed most everyone has a cellphone and people love convenience . Well, now is your chance to capitalize on this . WE will help YOU SELL MORE and deliver goods right to the customer's doorstep . The best thing about our system is that it is absolutely risk free for you . But don't believe us ! Mrs Simpson who resides in Wisconsin tried us and says "I've been poor and I've been rich - rich is better" ! We are a BBB member in good standing ! We BESEECH you - act now ! Sign up a friend and your friend will be rich too . Thanks ! Dear Friend ; This letter was specially selected to be sent to you . We will comply with all removal requests ! This mail is being sent in compliance with Senate bill 1622 ; Title 3 ; Section 303 ! This is not multi-level marketing . Why work for somebody else when you can become rich inside 79 days . Have you ever noticed most everyone has a cellphone and society seems to be moving faster and faster . Well, now is your chance to capitalize on this . We will help you process your orders within seconds & deliver goods right to the customer's doorstep . The best thing about our system is that it is absolutely risk free for you . But don't believe us . Ms Simpson of Mississippi tried us and says "Now I'm rich many more things are possible" . We assure you that we operate within all applicable laws ! Do not delay - order today ! Sign up a friend and your friend will be rich too ! Cheers .

Táto správa vyzerá ako typický spam, ktorý je väčšinou ignorovaný a vyradený z e-mailovej schránky. Správa bola vytvorená cez spam mimic. Je to webová stránka, ktorá konvertuje krátku textovú správu do textového bloku vyzerajúceho ako typický spam prostredníctvom idey gramaticky založenej mimiky [**35**][**36**]. Tretia strana nezistí nič všimaním si rozostupu medzier alebo gramatických chýb. Jedničky a nuly sú kódované voľbou slov. Ukrytá správa v spame hore je:

Steganografia je skoro neodhaliteľná.

Na ukrytie správy do digitálneho súboru používajúc nulové šifry nepotrebujeme žiadne špeciálne nástroje. Obrázok alebo text môže byť ukrytý pod iným obrázkom napríklad v súbore aplikácie PowerPoint. Správa môže byť ukrytá vo vlastnostiach súboru typu Word, v komentároch na webovej stránke, alebo v ďalších rôznych formátových vlastnostiach, ktoré sú ignorované prehliadačom [**3**].



Obrázok 1.3. Webová aplikácia spam mimic.

Správa môže byť grafický uložená v dokumente nastavením farby písma na farbu pozadia a umiestnením nejakého obrázka na pozadie. Adresát potom získa správu ďalšou zmenou farby textu [**33**]. To všetko sú rozhodne slabé mechanizmy, ale takisto môžu byť veľmi efektívne.

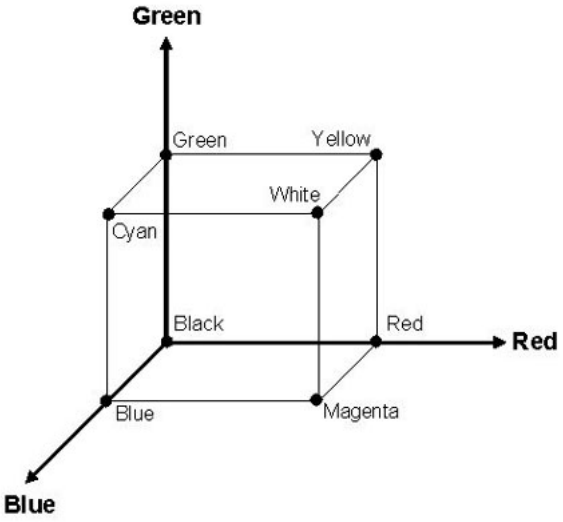
1.3. Digitálny obrázok a audio.

Mnoho súčasných digitálnych steganografických techník využíva grafické obrázky alebo audio súbory ako nosič média. Je poučné sa pozrieť ako funkuje kódovanie obrázkov a audio súborov predtým, ako budeme hovoriť o tom, akým spôsobom pracuje steganografia a steganoanalýza s týmito nosičmi.

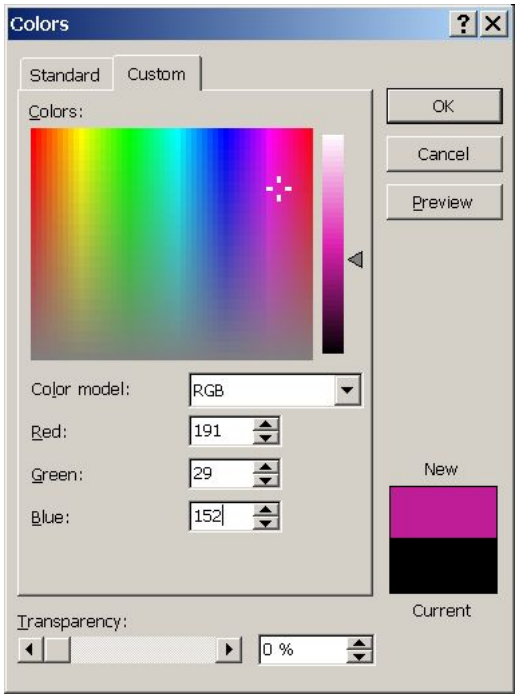
Obrázok 1.4 znázorňuje rozloženie **RGB** farieb, kde každú farbu reprezentuje nejaká intenzita z každej farebnej komponenty - červená (red), zelená (green), modrá (blue). Absencia všetkých farieb dáva farbu čiernu, znázornené ako prienik všetkých farieb v nule. Mix 100 percent z každej farby dáva farbu bielu. Ostatné farby získame podobne.

Obrázok 1.5 ukazuje intenzitu RGB pri nejakej náhodnej farbe. Každá komponenta je určená jedným bajtom, takže hodnoty pre každú farbu sú v škále od 0 do 255 . Na obrázku je konkrétny odtieň (fialová farba) označený takto: červený stupeň 191 (hex BF), zelený stupeň 29 (hex 1D), modrý stupeň 152 (hex 92). Teda fialová farba by bola kódovaná 24 bitmi ako 0xBF1D98. Táto 24-bitová kódovacia schéma podporuje 16,777,216 (2^{24}) unikátnych farieb [**6**][**21**].

Dnes už väčšina aplikácii, ktoré pracujú s digitálnymi obrázkami podporuje 24-bitové farby (24-bit true color), kde každý element obrázka (pixel) je kódovaný do 24 bitov zahrňujúcich tri RGB bajty ako sme si ukázali vyššie. Ostatné aplikácie používajú kódovanie farieb do 8 bitov na každý pixel. Tieto schémy takisto používajú 24-bitové farby, ale pri tom využívajú paletu, ktorá označuje aké farby sú používané v obrázku. Každý pixel je kódovaný v 8 bitoch, kde hodnota ukazuje



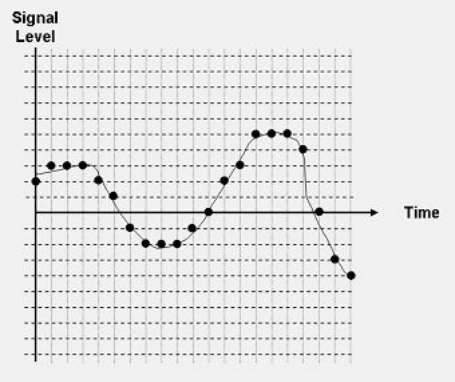
Obrázok 1.4. Schéma RGB.



Obrázok 1.5. Ukážka RGB stupňov vo vybranej farbe.

na hodnotu v 24 bitoch na palete. Z tohto dôvodu táto metóda podporuje len 256 (2^8) farieb. Voľba kódovania farieb má prirodzene vplyv na veľkosť obrázka (nie rozmer ale data uložené na disku). 640 x 480 pixelový obrázok, ktorý používa 8-bitové farby môže zaberať približne 307 KB (640 x 480 = 307,200 bajtov), zatiaľ čo 1400 x 1050 pixelový obrázok používajúci 24-bitové farby potrebuje 4.4 MB (1400 x 1050 x 3 = 4,410,000 bajtov).

Farebné palety a 8-bitové farby obvykle používali formáty obrázkov **Graphics Interchange Format (GIF) a Bitmap (BMP)**, ale dnes to už nemusí byť pravda. Obidva formáty môžu využívať aj viacbitovú reprezentáciu pixelov. GIF



Obrázok 1.6. Jednoduchá modulácia pulzov (signal level = stupeň signálu).

a BMP sú označované ako formáty s bezstratovou kompresiou, pretože obraz získaný po kódovaní a kompresii je bit po bitu identický originálu [**21**].

Joint Photographic Experts Group (JPEG) formáty používajú individuálnu kosínusovu transformáciu radšej ako kódovanie bit po bite. V JPEG súbore je obraz rozdelený do 8 x 8 blokov pre každú samostatnú farebnú komponentu. Cieľom je nájsť bloky, kde množstvo zmien v hodnotách pixelov (energia, the energy) je nízka. Ak stupeň energie je príliš vysoký, blok je rozdelený na 8 x 8 podblokov, až kým energia nie je dostatočne nízka. Každý blok (alebo podblok) je zmenený na 64 individuálnych kosínusových transformáčných koeficientov, ktoré vytvárajú svietivosť (jasnosť (brightness), nejasnosť (darkness) a kontrast(contrast)) a farebnosť (color) tej konkrétnej časti obrázka. JPEG je formát so stratovou kompresiou, pretože obraz získaný z komprimovaného JPEG súboru je vizuálne skoro rovnaký, ale nie identický s originálom [**21**][**27**][**30**].

Audio kódovanie zahrňuje konvertovanie analogového signálu do bitového toku. Analogový zvuk - hlas a hudba - je reprezentovaný sínusovými vlnami v rozličných frekvenciách. Ľudské ucho dokáže vnímať frekvenciu v rozsahu od 20 do 20 000 Hz (cyklus/sekunda). Zvuk je analogový teda je to spojitý signál. Ukladanie zvuku digitálne vyžaduje aby spojitá zvuková vlna bola skonvertovaná do množiny vzorov, ktoré môžu byť reprezentované sekvenciou núl a jedničiek.

Analogovo-digitálna (analog-to-digital) konverzia je ukončená vytvorením vzoru z analogového signálu (pomocou mikrofónu alebo iného audio detektoru) a skonvertovaním tohto vzoru na stupeň napätia. Toto napätie je potom prevedené na numerickú hodnotu, ktorá používa schému nazývanú **modulácia pulzov (pulse code modulation)**. Prístroj, ktorý vykonáva túto konverziu je nazývaný kóder-dekóder (coder-decoder) alebo jodnoducho kodek (codec, väčšinou sa používa v zmysle PCM + kompression algorithm).

Modulácia pulzov obstaráva iba aproximáciu originálneho analogového signálu, ako znázorňuje obrázok 6. Ak je napríklad stupeň analogového zvuku zmeraný na 4.86 stupňa, bude to skonvertované na 5 pomocou modulácie pulzov. Toto sa nazýva **chyba hromadenia (quantization error)**. Rozdielne audio aplikácie majú definované iné čísla ako stupne modulácie pulzov, takže táto chyba je skoro nepostrehnuteľná pre ľudské ucho. Telefónna sieť konvertuje každý hlasový záznam do 8-bitovej hodnoty (0-255), zatiaľ čo hudobné aplikácie používajú hlavne 16-bitové hodnoty (0-65,535) [**17**][**31**].

Analogové signály musia byť vzorkované minimálne v dvakrát väčšej miere ako je frekvencia komponentu signálu, aby originál mohol byť korektne reprodukovaný zo vzorkov samostatne. V telefónnej sieti je ľudský hlas prenášaný s frekvenciou 0-4000 Hz (hoci len nejakých 400-3400 Hz je v skutočnosti používaných), a preto je hlas vzorkovaný 8000krát za sekundu (8 kHz, sample rate, frekvencia vzorkovania). Hudobne aplikácie predpokládajú celé spektrum ľudského ucha a používajú skoro vždy 44.1 sampling rate (samozrejme môžu používať aj iné vzorkovanie) [**17**][**31**].

Rýchlosť prenosu nekomprimovanej hudby môže byť ľahko vypočítaná z frekvencie vzorkovania (44.1 kHz), modulácie pulzov (16 bits), a z počtu zvukových kanálov (stereo má počet kanálov 2). Teda dostávame 1,411,200 bitov za sekundu. Tým by jedno-minutový audio súbor (nekomprimovaný) mohol zaberať 10.6 MB (1,411,200·60/8 = 10,584,000). Veľkosť audio súborov sa v skutočnosti zmenšuje pomocou rôznych kompresných techník. Jedna očividná metóda je redukovať počet kanálov na jeden, alebo redukovať frekvenciu vzorkovania, v niektorých prípadoch až na 11 kHz. Rôzne kodeky používajú vlastné kompresné schémy. Všetky tieto redukujúce spôsoby ale znižuju kvalitu zvuku.

Tabuľka 1.1. Niektoré bežné digitálne audio formáty [**17**].

Audio formát	**Prípona súboru**	**Kodek**
AIFF (Mac)	.aif, .aiff	Pulse code modulation (alebo iné)
AU (Sun/Next)	.au	ľ-law (alebo iné)
CD audio (CDDA)	n/a	Pulse code modulation
MP3	.mp3	MPEG Audio Layer III
Windows Media Audio	.wma	Microsoft proprietary
QuickTime	.qt	Apple Computer proprietary
RealAudio	.ra, .ram	Real Networks proprietary
WAV	.wav	Pulse code modulation (alebo iné)

1.4. Prehľad metód digitálnych nosičov.

Existuje veľa spôsobov ako môže byť správa utajená v digitálnom médiu. Digitálni forenzní analytici sú oboznámení skoro so všetkými spôsobmi [**6**]).

Informácie môžu byť skryté na hard disku na tajnej partícii. Tajnú partíciu nebude vidieť za normálnych okolností, aj keď konfigurácia disku a ostatné nástroje majú úplný prístup k tajnej partícii [**23**]. Táto teória je implementovaná v steganografickom systéme súborov ext2fs pre Linux. Skrytý systém súboru je obzvlášť zaujímavý, pretože chráni uživateľa od naviazanosti na istých informáciách na jeho hard disku (to znamená, že ma preddefinované isté práva, a k jeho súborom sa nikto nedostane, ak na to nemá právo). Táto forma možnej popierateľnosti umožňuje uživateľovi tvrdiť, že je vlastníkom niektorých informácií, alebo tvrdiť, že nejaká udalosť vôbec nenastala. Pod týmto systémom môžu uživatelia ukrývať súbory na disk, zaistiť diskrétnost obsahu súboru, a neporušiť neutajené súbory odstranením steganografického driveru [**1**][**3**][**26**].

Ďalší digitálny nosič môže byť sieťový protokol TCP/IP, ktorý v súčasnosti podporuje každý systém. Napríklad utajený Transmission Control Protocol vytvára tajné komunikáčné kanály použitím identifikačného poľa v Internet Protocol paketoch alebo sekvencie číselného poľa v segmentoch Transmission Control Protocol [**23**][**32**].

Existuje niekoľko charakteristík zvuku, ktoré môžu byť zmenené tak, aby boli pre človeka nevnímateľné (z hľadiska sluchu), a tieto nepatrné zmeny, ako je napríklad malý posun vo fázovaní, rečovej kadencii, a frekvencii, môžu prenášať ukryté informácie [**6**].

Audio a obrázkové (image) súbory avšak stále zostávajú najlepším a najviac používaním nosičom média na internete, pretože potenciálne súbory už existujú, veľmi jednoducho sa transportujú pomocou internetu, je možnosť vytvoriť ľubovoľné množstvo nových nosičov súborov, a človek má jednoduchý prístup k steganografickému softwaru, ktorý operuje s týmito nosičmi. Z tohto dôvodu sa budem v tomto dokumente zameriam na audio a image súbory.

Najviac používaná steganografická metóda v audio a image súboroch zahrňuje niektoré typy substitúcie najmenej významných bitov. Termín menej významný bit (least significant bit, LSB) pochádza z číselného významu bitov v bajte. Bit vysokého rádu alebo najviac významný bit je ten jeden s najväčšou aritmetickou hodnotou (napríklad 27=128), zatiaľ čo bit nízkeho rádu alebo najmenej významný bit je ten jeden s najnižšou aritmetickou hodnotou (napríklad 20=1).

Ako jednoduchý príklad substitúcie najmenej významného bitu si predstavte "ukrytie" písmena "G" do nasledujúcich 8 bitov nosiča súboru (najmenej významný bit je zvýraznený):

1001010*1* 0000110*1* 1100100*1* 1001011*0*
0000111*1* 1100101*1* 1001111*1* 0001000*0*

'G' je reprezentované v ASCII (American Standard Code for Information Interchange) kóde ako binárny reťazec 01000111. Týchto 8 bitov môžeme vložiť do najmenej významného bitu z každého z 8 bajtov nosiča nasledovne:

1001010*0* 0000110*1* 1100100*0* 1001011*0*
0000111*0* 1100101*1* 1001111*1* 0001000*1*

V tejto ukážke bola v skutočnosti len polovica najmenej významných bitov zmenená. To dáva zmysel práve vtedy, ak jedna množina núl a jedničiek je nahradená inou množinou núl a jedničiek.

Substitúcia najmenej významného bitu sa môže používať na prepisanie pravého RGB kódovania alebo na prepísanie palety ukazateľov v GIF a BMP súboroch, koeficientov v JPEG, stupňa modulácie pulzov v audio súboroch. Prepisaním najmenej významého bitu sa číselná hodnota len nepatrne zmení, čo si človek s najmenšou pravděpodobnosťou všimne.

Táto substitúcia je jednoduchá, bežná technika pre steganografiu. Avšak jej využitie nie je nevyhnuteľne a dá sa použit jednoduchší algoritmus ako napríklad metóda na zvuk. Iba naivný steganografický software by len prepisoval každý najmenej významný bit ukrytých dát. Skoro všetky programy používajú na výber bitu v nosiči, ktorý bude modifikovaný, istú náhodnosť. To je jeden z faktorov, ktorý robí detekciu steganografie ťažkou.

Ďalší spôsob ako ukryť informáciu do palety obrázka je zmeniť poradie farieb v palete alebo použiť radšej kódovanie najmenej významného bitu na palete farieb ako na data obrázku. Tieto metódy su potenciálne slabé. Veľa nástrojov pre grafické softwary usporadúvajú farby v palete podľa ich frekvencie, jasu, a ostatných parametrov, a náhodne usporadúvajú paletu na výstupe podľa štatistickej analýzy [**10**].

Novšie, viac komplikované steganografické metódy sa stále vyvíjajú. Rozšírené steganografické metody sú analogické rozšírenému rádiovému prenosu (vyvinuté v druhej svetovej vojne a súčasne používané v systémoch s datovou komunikáciou) kde je 'energia' signálu rozšírená cez široko-frekvenčné spektrum radšej ako na jedinú frekvenciu, v snahe zťažiť detekciu a úmyselné rušenie signálu. Rozšírená steganografia má takú istú funkciu - vyhnúť sa detekcii. Tieto metódy sa opierajú o fakt, že malé narušenie obrazu a zvukového súboru je najmenej zistiteľné v častiach s vyššou energiou na nosiči (napríklad vysoká intenzita vo zvukovom súbore alebo jasné farby v image súbore) [**36**].

1.5. Beztrátové grafické formáty.

1.5.1. BMP

.BMP ale aj **.DIB (device-independent bitmap)** je bitový grafický formát používaný v Microsoft grafickom systéme, a v súčasnosti pužívaný ako jednoduchý grafický formát pre platformu.

Obrázky BMP sú väčšinou ukladané s hĺbkou farieb 2 (1 bit), 16 (4 bity), 256 (8 bitov), 65,536 (16-bit), alebo 16.7 miliónov (24-bit) (to znamená koľko bitov je potreba na reprezentáciu každého pixelu). Osembitové obrázky môžu namiesto farieb používať aj šedú škálu. **Alfa kanál** (pre transparenciu) môže byť uložený v oddelenom súbore, kde je podobný ako obraz so šedou škálou. 32-bitová verzia s integrovaným alfa kanálom bola predstavená s príchodom Windows XP a je použitá napríklad v ich logu a v systémovej téme, a v konečnom dôsledku dáva veľkú podporu pre software zaoberajúci sa editovaním obrazu.

BMP nepatrí medzi úsporné formáty. Je tomu tak z nasledujúcich dôvodov:

(1) Neúspornosť začína už pri dátovej hlavičke súbora, ktorá obsahuje niekoľko rezervovaných, teda z praktického hľadiska zbytočných položiek, ktoré ani v minulosti a pravdepodobne ani v budúcnosti nebudú využité.
(2) Ďalší zdroj neúspornosti môžeme vidieť na príklade obrázka s farebnou paletou. Pre každé miesto vo farebnej palete sú rezervované 4 bajty namiesto dostačujúcich 3 bajtov. Posledný bajt však nie je možné použiť pre iné účely, teda ani pre alfa kanál (podľa platnej špecifikácie).
(3) Tretí a zďaleka najzávažnejší dôvod, prečo formát BMP je neúsporný, spočíva v použitom kompresnom algoritme. Zvolený postup kompresie je tak navrhnutý, že pre mnoho obrázkov dochádza skôr k nárastu veľkosti súboru

namiesto znižovania. Okrem toho je kompresia povolená len pre obrazy s farebnou paletou. Všetky riadky obrazu musia mať počet pixelov deliteľných 4.

Zaujímavý je takisto spôsob ukladania obrazových riadkov do súboru. Tie sa neukladajú smerom zhora nadol, ako je to prirodzené, ale presne naopak. Všetko sa tým pádom výrazne komplikuje. Dôvod, prečo je smer vykresľovania a ukladania v BMP opačný, spočíva v tom, že túto orientáciu používal operačný systém OS/2 (DOS a pod.).

Detailný popis formátu súborov typu BMP nájdete v appendixe 1 na priloženom DVD.

1.5.2. PNG

Grafický formát PNG (Portable Network Graphics - anglicky prenosná sieťová grafika; oficiálna výslovnosť skratky je "ping") je súborový formát určený pre ukladanie, prenos a zobrazovanie rastrových obrázkov. Obrázky sú pri použití PNG ukladané v komprimovanej podobe, pričom použitý komprimčný algoritmus je bezstratový.

Tento grafický frmát má mnoho vlastností, ktoré ho predurčujú pre spracovanie fotografií, prezentáciu obrázkov na webe atď. Medzi najvýznamnejšie vlastnosti patrí voliteľná bitová hĺbka (určuje maximálny počet farieb), ukladanie priehľadnosti pixelov (alfa kanál), prekladanie pixelov umožňujúce rýchle náhľady na obrázok, podpora farebných profilov a podobne. Na rozdiel od ďalších formátov s podobnými vlastnosťami (napríklad TIFF) je PNG veľmi jednoduchý formát, pri ktorom je presne známe, aké vlastnosti musí dodržať každý program, ktorý pracuje s PNG.

Veľa programátorov považuje formát PNG za jeden z najlepšie navrhnutých binárnych súborových formátov. Autori PNG při jeho návrhu uvažovali o niekoľkých variantách internej štruktúry tohoto formátu. Jednou z uvažovaných variant bol čiste textový popis obrazových dát v štýle formátov PBM, PGM a PPM (Portable BitMap, Portable GrayMap, Portable PixelMap), pričom by celý súbor bol pred svojim uložením na disk skomprimovaný programom zip alebo bzip2. Nakoniec sa od tohoto návrhu, ktorý bol v niekoľkých ohľadoch problematický, upustilo a prešlo sa na návrh čiste binárneho formátu, čo sa ukázalo ako krok správnym smerom. Tvorci PNG sa takisto poučili z mnohých chýb a nedostatkov do tej doby používaných binárnych formátov a navrhli konzistentnú internú štruktúru PNG, ktorá je na jednu stranu veľmi sofistikovaná a na druhú stranu pritom pomerne jednoduchá na implementáciu. Celý binárny súbor s uloženým obrázkom sa skladá z hlavičky, ktorá je nemenná, tj. neobsahuje ani číslo verzie. Za hlavičkou sa nachádza ľubovoľné množstvo takzvaných chunkov, čo sú pomenované bloky, z ktorých každý má svoju dĺžku, typ a kontrolný súčet CRC (Cyclic Redundancy Check/Cyclic Redundancy Code).

Detailný popis formátu súborov typu PNG nájdete v appendixe 2 na priloženom DVD.

1.6. Steganografia na bezstrátových grafických formátoch.

Každý text pozostáva z postupnosti jednotlivých znakov, ktoré sú jednoducho reprezentované pomocou jedného bajtu (ASCII kód).

Tabuľka 1.2. Príklad bitovej reprezentácie znakov.

časť textu:	H	i		a	l	l
ASCII kód:	72	105	32	97	108	108
binárny kód:	01001000	01101010	00100000	01100001	01101100	01101100

Tabuľka 1.3. Binárny operátor AND.

A	B	A AND B
0	0	0
0	1	0
1	0	0
1	1	1

Teda máme dva bitové toky. Jeden tok reprezentuje dáta v obrázku a druhý reprezentuje našu ukrývanú informáciu. Nemusí to byť len text, môže to byť čokoľvek, čo sa dá reprezentovať binárnym kódom (napríklad iný obraz).

Na vkladanie informácie použijeme metódu LSB. O tejto metóde sme si niečo povedali už v úvode. Jedná sa o veľmi jednoduchý algoritmus, ktorý nahradzuje najmenej významné bity v dátovom toku obrazu bitmi utajovanej správy. Vo všeobecnom prípade to nemusí byť len najmenej významný bit, ale môžu to byť napríklad aj posledné dva najmenej významné bity atď.

Na každý bajt z dátovej časti obrazu aplikujeme tzv. **masku 254 (1111 1110)**. Ak máme 'H', teda '0100 1001' a aplikujeme na to našu masku 1111 1110, jednoducho "zmažeme" jedničku na konci binárneho kódu písmena 'H'. To znamená, že sa aplikuje bitový operátor AND.

Napíšeme si celý algoritmus, ako prebieha vkladanie informácie do obrazu vo formáte BMP:

(1) "Hi" → binárny kód **010**01001 01101001
(2) časť dátovej časti BMP súbora

11000100 10011001 10011100

aplikujeme masku 254 (1111 1110)

11000100 10011000 10011100

substituujeme najmenej významne bity našou správou

*010*01001 01101001

(3) Po aplikovaní substitúcie dostanem výsledok

11000100 10011001 10011100

Obrázok 1.7. Príklad originálneho BMP (naľavo) a steganografického BMP (napravo).

Samozrejme, že do obrazu nemôžeme vkladať nekonečné množstvo bitov. Každý obraz má svoje obmedzenie na dĺžku vkladanej informácie, dané počtom farebných kanálov a hĺbkou farieb. Napríklad, ak máme obraz v truecolor, kde je každý pixel reprezentovaný troma kanálmi R, G, B, a má rozlíšenie 640 x 480, budeme mať k dispozícii 640x480x3 najmenej významných bitov na substitúciu.

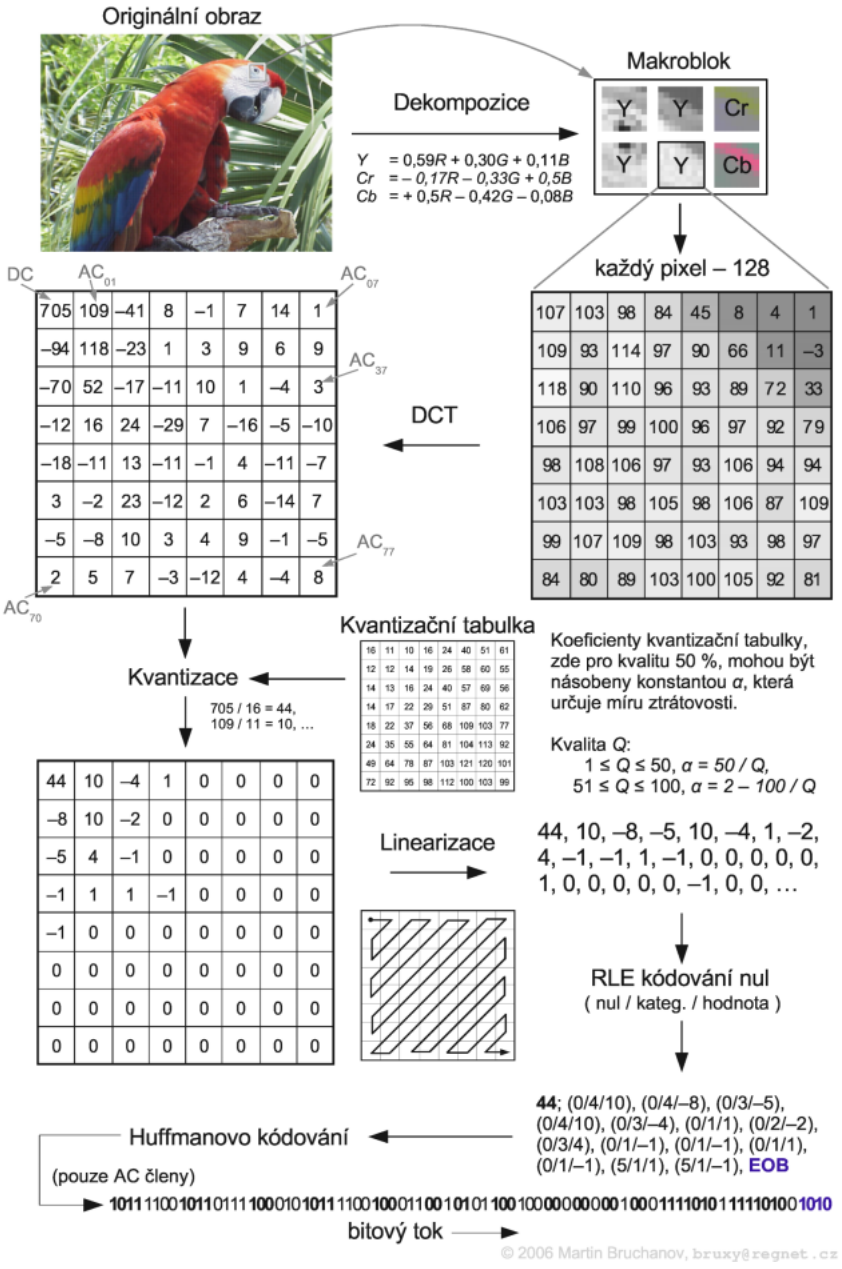
1.7. JPEG.

JPEG je štandardná metóda stratovej kompresie používaná na ukladanie digitálnych obrázkov vo fotorealistickej kvalite. Skratka JPEG je odvodená od **Joint Photographic Experts Group**. Je to názov spojených výborov ISO/CCIT, ktoré vytvorili tento štandard. Skupina bola zorganizovaná v roku 1986 a vydala štandard v roku 1992, ktorý bol schválený v roku 1994 ako ISO 10918-1. JPEG je podobný ako MPEG, Moving Picture Experts Group, ktorý vytvára kompresnú scgému pre pohyblivé obrazy.

JPEG umožňuje stratovú kompresiu obrazu (hoci existuje veľa obmien štandardu založených na JPEG, ktoré sú bezstratové). Formát súboru, ktorý používa túto kompresiu sa zvyčajne nazýva takisto JPEG; najviac vyskytujúca sa prípona takých typov súborov je .jpg, ale aj .jpeg, .jfif, .JPG, .JPE.

JPEG ako taký špecifikuje ako je obraz transformovaný na prúd bajtov, ale nie ako sú tieto bajty zapúzdrené v nejakom partikulárnom úložnom médiu. Neskorší štandard vytvorený skupinou **Independent JPEG Group**, nazývanou **JFIF** (JPEG File Interchange Format), špecifikuje, ako vytvoriť súbor z prúdu JPEG vhodný na ukladanie do počítača a prenos (napríklad po internete). V prirodzenom použití, ak niekto hovorí o "súbore JPEG", tak hovorí o súbore založenom na JFIF, alebo niekedy o Exif JPEG **(Exchangeable image file format)** súbore. Existujú samozrejme aj iné formáty založené na JPEG, ako je napríklad JNG **(JPEG Network Graphics)**, a takisto formát TIFF **(Tagged Image File Format)** môže niesť informácie založené na JPEG.

JPEG/JFIF je formát najviac používaný na ukladanie a prenos fotografií na WWW (World Wide Web). Pre tieto aplikácie sú preferované typy súborov ako GIF, ktorý má limit 256 rôznych farieb, čo je nedostatočné pre fotografický obraz, a PNG, ktorý produkuje oveľa väčší image súbor. Kompresný algoritmus nie je veľmi dobre situovaný pre kresby a textové a ikonové grafiky, preto sú GIF a PNG pred JPEG/JFIF preferované.



Obrázok 1.8. Celková schéma kódovania JPEG.

Veľa volieb v štandarde JPEG nie je používaných. Pozrieme sa na stručný popis jednej z viac obvyklých metód kódovania, ak je aplikovaná na vstup, kde je každý pixel reprezentovaný 24 bitami. Táto partikulárna voľba je metóda stratovej datovej kompresie.

Z obrázka 1.8 vidíme, ako prebieho kompresia JPEG obrázka:

(1) Dekompozícia na zložky Y, Cr, Cb.
(2) Každý blok Y, Cr a Cb sa rozdelí do blokov 8x8.
(3) Každý blok 8x8 obsahuje 64 bajtov, z každého elementu sa odčíta číslo 128.
(4) Na každý koeficient bloku sa aplikuje diskrétna kosínusová transformácia DCT.

(5) Pomocou kvantizačnej tabuľky prebehne kvantizácia koeficientov.

Detailný popis formátu súborov typu JPEG nájdete v appendixe 3 na priloženom DVD.

1.8. Steganografia a JPEG.

1.8.1. Kvázi-steganografická metóda

Ukážeme si jednu vtipnú metódu. Táto metóda nie je veľmi bezpečná, ale jej implementácia je veľmi jednoduchá a pre všedného človeka nie veľmi postrehnuteľná. Všetko, čo budeme na to potrebovať je Windows 2000 alebo vyšší a WinRAR.

(1) Vyberieme si JPEG, do ktorého chceme vložiť data (najlepšie je si všetko dať pod jeden adresár, t.j. data aj JPEG).
(2) Data, ktoré chceme ukryť, vložíme do nového RAR archívu.
(3) Otvoríme príkazový riadok (Command Prompt) a vojdeme do adresára, kde máme uložené naše potrebné súbory.
(4) Napíšeme príkaz **'copy /b [súbor_do_ktorého_ukrývame].jpg + [naše_ukrývane_data].rar [meno_výstupného_súboru].jpg'**.
(5) Výsledný JPEG je uložený v našom adresári.

Ak otvoríme výsledný JPEG tak sa nám objaví nezmenený obraz. Ak tento súbor otvoríme vo WinRAR-e tak sa nám otvorí ako balík a môžeme si vybrať ukryté súbory.

1.8.2. Sekvenčný postup

Derek Upham's JSteg bol prvý verejne dostupný steganografický systém pre JPEG images. Jeho ukrývajúci algoritmus sekvenčne nahradzoval LSB DCT koeficientov datami správy.

```
Algoritmus:
INPUT: message, cover image
OUTPUT: stego image
WHILE data left to embed DO
    get next DCT coefficient from cover image
    IF DCT != 0 and DCT != 1 THEN
        get next LSB from message
        replace DCT LSB with message LSB
    END IF
    insert DCT into stego image
END WHILE
```

Algoritmus nepotrebuje zdieľané tajomstvo; ako výsledok, hocikto, kto pozná steganografický system môže získať správu ukrytú pomocou JSteg.

1.8.3. Pseudonáhodný postup

OutGuess 1.0 je steganografický systém, ktorý vylepšuje vkládací krok použitím generátora pseudonáhodného čísla na výber DCT koeficientov náhodne. LSB

vybraného DCT koeficientu je nahradený zašifrovanou správou.

```
Algoritmus:
INPUT: message, shared secret, cover image
OUTPUT: stego image
initialize PRNG with shared secret
WHILE data left to embed DO
    get pseudo-random DCT coefficient from cover image
    IF DCT != 0 and DCT != 1 THEN
        get next LSB from message
        replace DCT LSB with message LSB
    END IF
    insert DCT into stego image
END WHILE
```

2

DETEKCIA STEGANOGRAFIE

2.1. Úvod.

Problém väzňa [**34**] je často používaný na priblíženie steganografie, hoci bol pôvodne používaný na vykreslenie kryptografie.

Problém sa týka dvoch väzňov, Alici a Boba, ktorý sú zatvorený v oddelených celách a chcú sa dohodnúť na nejakom tajnom pláne. Alica a Bob majú povolené vymieňať si správy medzi sebou, ale strážnik William si ich môže všetky prečítať. Alica a Bob vedia, že ak William odhalí ich tajný komunikačný kanál, tak už nebudú môcť spolu komunikovať.

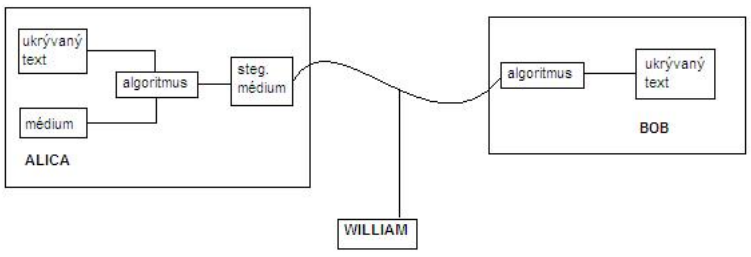
William môže zaujať pasívny, alebo aktívny postoj. V pasívnom postoji William preskúma správu a rozhodne sa, či správu posunie ďalej alebo nie. V aktívnom postoji môže William zmeniť správu, ak chce. Zlomyseľný strážnik by teda mohol meniť každú správu, aby predišiel tajnému kanálu, takže Alica a Bob musia použiť veľmi silnú steganografickú metódu [**19**][**16**].

To, ako bude strážnik reagovať, dosť závisí od zložitosti steganografického algoritmu a od Williamových vedomostí [**19**][**16**][**30**].

Na základe tohto modelu si priblížime steganoanalýzu, a podľa možností a vedomostí všetkých strán rozdelíme steganoanalýzu na základné útoky. Steganoanalýza, detekcia steganografie treťou stranou, je relativne mladá disciplína. Umenie a veda steganoanalýzy spočíva v detekovaní alebo odhalení ukrývanej informácie založenom na pozorovaní nejakého toku dát bez akéhokoľvek predpokladu o steganografickom algoritme [**19**]. Detekcia ukrytých dát nemusí byť postačujúca. Staganoanalysta chce vytiahnuť informácie skrytej správy a prípadne dosiahnuť toho, aby to adresát nemohol prečítať, alebo poslať miľnú informáciu [**20**]. Steganografická detekcia a extrakcia je úspešná vtedy ak sa to podarí dokázať.

Techniky steganoanalýzy môžu byť klasifikované podobne ako metódy v kryptoanalýze, podľa toho, ako veľa vieme o médiu [**6**][**22**]:

- Steganografické médium je jediná vec, ktorú máme k dispozícii pre analýzu **(Steganography-only attack)**.



Obrázok 2.1. Názorný priebeh komunikácie medzi Alicou a Bobom.

- Nosič a steganografické médium sú dostupné pre analýzu **(Known-carrier attack, nikedy sa označuje ako Known cover attack)**.
- Poznáme ukrytú správu **(Known-message attack)**.
- Máme steganografické médium a je nám známy algoritmus **(Chosen-steganography attack)**.
- Známa správa a steganografický algoritmus použijeme na vytvorenie média pre budúcu analýzu a porovnanie **(Chosen-message attack)**.
- Poznáme nosič, médium a algoritmus **(Known-steganography attack)**.

Steganografické metódy pre digitálne média môžu byť klasifikované ako metódy operujúce s oblasťou obrazu alebo s oblasťou transformácie. Nástroje, ktoré pracujú s oblasťou obrazu, ukrývajú správu do nosiča manipuláciou bitu po bitu, ako napríklad vkladanie najmenej významného bitu. Nástroje, ktoré pracujú s oblasťou transformácie, manipulujú so steganografickým algoritmom a s transformáciami zavedenými v ukrývaní informácie, ako napríklad individuálna kosínusova transformácia koeficientov v JPEG súboroch [**22**]).

Teda steganoanalýza hľadá algoritmus, ktorý bol použitý pre účely steganografie. Jeden jednoduchý postup je vizuálne preskúmať nosič a steganografické médium. Väčšina jednoduchších steganografických nástrojov pracuje v oblasti obrazu a volí bity správy v nosiči nezávisle od obsahu nosiča. Hoci je ľahšie ukryť správu do miesta s vyššou jasnosťou alebo hlasitým zvukom, program nemusí takéto miesta vyhľadávať. Teda vizuálne skúmanie môže byť úspešné a vyvolať podozrenie na steganografické médium.

Druhý postup spočíva vo vyhľadaní štrukturálnych zvláštností, ktoré nasvedčujú manipulacii. Vloženie najmenej významného bitu do paletového obrázka často spôsobuje veľké množstvo duplikátnych farieb, kde identické (alebo skoro identické) farby vznikajú na palete dvakrát a líšia sa len v najmenej významnom bite (LSB). Steganografické programy, ktoré ukrývajú informáciu jedine manipuláciou poradia farieb v palete, spôsobujú takisto štrukturálne zmeny. Štrukturálne zmeny často vytvárajú signatúru steganografického algoritmu, ktorý bol použitý [**20**][**36**].

Steganografické techniky všeobecne menia štatistiky nosiča a, samozrejme, dlhšia správa spôsobí väčšiu zmenu v nosiči ako kratšia [**8**][**10**][**12**][**28**]. Štatistická analýza je obyčajne používaná na detekciu ukrytej informácie, obvykle ak analysta nemá žiadné informácie [**20**]. Existuje veľké množstvo prác ohľadom štatistickej steganoanalýzy.

Štatistická analýza image a audio súborov môže ukázať, či štatistické vlastnosti súborov sa odkloňujú od očakávaného výsledku, normy [**8**][**28**][**29**]. Tieto takzvané jednoúrovňové (first-order) štatistiky - priemery, odchýlky, chi-kvadrát testy - môžu odmerať množstvo redundantných informácií a/alebo deformáciu v médiu. Hoci tieto merania nám môžu poskytnúť akúsi predikciu či obsah bol modifikovaný alebo vyzerá podozrivo, určite nie sú definitívne [**36**].

Štatistická steganoanalýza je niekedy zbytočná, pretože niektoré steganografické algoritmy usilujú o ochranu súborov nosiča pred first-order štatistikou, aby sa pomocou nej nedali detekovať. Zašifrovanie ukrývanej správy zťažuje detekciu, pretože šifrované dáta majú všeobecne vyšší stupeň náhodnosti, a výskyt jedničky a nuly na nejakom mieste je rovnako pravdepodobný [**8**][**29**].

Obnova ukrytej informácie (chceme zistiť ukrývanú správu) pridáva ďalšiu vrstvu zložitosti v porovnaní s detekciou prítomnosti ukrytej informácie. Obnovenie ukrytej správy vyžaduje vedomosti alebo odhad na dĺžku správy, eventuálne šifrovací kľúč a znalosť šifrovacieho algoritmu [**16**].

Špecifické typové algoritmy na súbory nosiča môžu urobiť steganoanalýzu priamočiaru. Obzvlášť JPEG súborom sa venuje veľká pozornosť, pretože existujú rôzne spôsoby ako operovať s týmito typmi súborov. JPEG je prostý nosič média, ak použijeme jednoduché vloženie LSB, pretože modifikácia súboru spôsobená JPEG kompresiou uľahčuje úlohu detekcie ukrytej informácie [**10**]. Existuje niekoľko algoritmov, ktoré ukrývajú informáciu do JPEG súboru a všetky pracujú rozdielne. JSteg postupne vkladá ukrývanú informáciu do LSB, JP Hide&Seek používa náhodný proces na výber LSB, F5 požíva priestorové šifrovanie založené na Hammingových kódoch, a OutGuess chráni pred first-order štatistikou [**8**][**13**][**14**][**15**][**29**][**30**].

Pokročilejšie štatistické testy používajú viacúrovňové (higher-order) štatistiky, lineárne analýzy, Markovove náhodné polia, vlnové štatistiky atď. na image a audio súbory [**8**][**9**][**12**][**28**]. Výsledky takýchto testov môžete vidieť v rôznych steganografických nástrojoch na detekciu.

Väčšina steganoanalýz je dnes založená na signatúrach, podobne ako antivírové programy a nástroje na detekciu narušenia systému (intrusion detection system, IDS). Steganoanalystické systémy založené na odchýlke sa ešte len rozvíjajú. Hoci predošlé systémy sú presné a robustné, nastávajúce budú flexibilnejšie a budú schopné rýchlo odpovedať na nové steganografické techniky. Jedna forma takzvanej "slepej steganografickej detekcie" rozoznáva medzi čistým a steganografickým obrazom založenom na štatistickom vlnovom rozklade, alebo skúma priestor, orientáciu a škálu v podmnožine väčšieho image súboru [**8**][**20**].

Nástroje, ktoré dokážu detekovať a klasifikovať steganografiu sú stále v plienkach, ale začínajú sa vyskytovať ako software-ové nástroje, niektoré z nich sú S-Tools, JP Hide and Seek, Gargoyle.

2.2. Vizuálna analýza.

Najjednoduchšia, avšak často nespoľahlivá, metóda analyzovania podozrivých obrázkov je vizuálne analyzovanie a hľadanie anomálií alebo iných znakov, ktoré by mohli vzniknúť pri vkladaní dát. Veľa steganografických metód, vrátane metód založených na LSB a DCT, zanechávajú znateľné zmeny v homogénnych oblastiach obrázku.

2.3. Known-carrier attack.

V tomto útoku máme k dispozícii steganografické médium a nosič. Môžeme skúmať súvislosti medzi obidvoma médiami a vytvoriť tak spoľahlivý algoritmus na detekciu výskytu ukrytej informácie. Ale väčšinou nemáme k dispozícii obidve média. Analýzou štatistických vlastností nosiča a steganografického média vytvoríme podmienky pre detekciu. Sústredime sa na dve základné metódy, a to sú analýza histogramu a rozdiel štvorcov (Histogram Analysis, Sum-Squared Difference).

OBRÁZOK 2.2. Príklad obrázku s anomáliami spôsobenými steganografiou.

2.3.1. Analýza histogramu

Pomocou analýzy histogramov budeme skúmať rozdiely medzi našimi dvoma obrazmi.

DEFINÍCIA. Histogram digitálneho obrazu so šedou škálou v rozsahu $[0, L-1]$ je diskrétna funkcia $p(r_k) = \frac{n_k}{n}$, kde r_k je k-ty stupeň šedej farby, n_k je počet pixelov s touto farbou, n je celkový počet pixelov, a $k = 0, 1, 2, \ldots, L-1$.

Teda funkcia $p(r_k)$ nám dáva pravdepodobnosť výskytu farby r_k. Graf tejto funkcie pre všetky rôzne k poskytuje globálny popis obrazu.

2.3.2. Rozdiel štvorcov

Rozdiel štvorcov je jednoduchá metóda na porovnávanie dvoch obrázkov a hľadanie rozdielov medzi nimi. V tomto prípade jednoducho porovnávame hodnoty farieb každého pixelu v obidvoch správach. Rozdiel je potom suma všetkých štvorcov rozdielov.

DEFINÍCIA. Nech x_i, y_i je hodnota i-teho pixelu v obraze x, y. Potom rozdiel štvorcov je $\sum_i (x_i - y_i)^2$, kde i prebieha všetky pixely v obraze.

Táto hodnota nám dáva poznatok o tom, ako veľmi bol obrázok zmenený. Takisto môžeme vidieť, kde bol obrázok zmenený, a tým pádom, kde je ukrytá správa. Potom musíme prísť na to, či správa bola vložená pomocou LSB algoritmu, alebo pomocou niečoho iného.

2.4. Párová analýza. (Raw Quick Pair Analysis).

Veľký počet steganografických metód pre bezstrátové obrázky používa manipuláciu LSB. Teda najmenej významné bity sú menené na dosiahnutie požadovaného výsledku. Táto metóda je populárna, pretože v skutočnosti sa zmení len približne polovica bitov v obrázku. LSB manipulácia tým pádom po sebe nezanechá značné stopy.

Vytvoríme test na detekciu výskytu vloženej správy v truecolor obrázkoch. Hodnota každého pixelu je v truecolor reprezentovaná hodnotami R, G, B. Každá z týchto hodnôt je reprezentovaná bajtom. Nech počet unikátnych farieb je U.

Definícia. Povieme, že dve farby (R_1, G_1, B_1) a (R_2, G_2, B_2) formujú skoro pár ak $|R_1 - R_2| \leq 1$, $|G_1 - G_2| \leq 1$, $|B_1 - B_2| \leq 1$. Ekvivalentne $(R_1 - R_2)^2 + (G_1 - G_2)^2 + (B_1 - B_2)^2 \leq 3$.

Počet všetkých farebných párov je:

$$\binom{U}{2} \geq P,$$

kde P je počet skoro párov.

Uvažme pomer R medzi skoro pármi a všetkými pármi:

$$R = \left(\frac{P}{\binom{U}{2}} \right).$$

Pomer R nám dáva relatívny počet skoro párov v obrázku.

Popíšeme algoritmus na detekciu steganografie, teda nejaký Steganography-only attack:

- Ako vstup máme nejaký digitálny obrázok.
- Na začiatku potrebujeme vypočítať počet unikátnych farieb a počet skoro párov v nich. Potom vypočítame pomer R.
- Náhodne vyberieme pixely a vykonáme substitúciu LSB našej zvolenej testovacej správy do nosiča.
- Po získaní stego-obrázku vypočítame počet unikátnych farieb a počet skoro párov. Vypočítame z týchto hodnôt ich pomer. Označme tento počet unikátnych farieb U' a tento pomer R'.

Po prebehnutí algoritmu vidíme, že počet skoro párov je oveľa nižší pre správu, ktorá neobsahovala žiadnu informáciu pred začiatkom.

Zaujímavé je pozorovanie správania sa obrazov vzhľadom k tomuto testu. Ak obraz už v sebe obsahoval nejakú informáciu, tak potom nezistíme markantnú zmenu v porovnaní pomerov, ktoré získame pred a po vložení ďalšej správy. Vidíme, že $R \equiv R'$. Ak obraz neobsahoval informáciu, potom sa budú pomery významne líšiť, teda $R' > R$.

Z pozorovania musíme určiť hranicu Th, pomocou ktorej budeme s určitou pravdepodobnosťou rozlišovať obrazy ako obyčajné alebo ako stego. Potrebujeme minimalizoať dva druhy chýb, a to, že detekujeme správu, kde nemá byť, a naopak. Hranica môže byť vypočítana použitím vzorca:

$$Th = \frac{\mu\sigma(s) + \mu(s)\sigma}{\sigma + \sigma(s)},$$

kde μ, σ sú priemerná a štandardná odchýlka pomeru R'/R pre nejakú databázu obyčajných obrazov. $\mu(s)$, $\sigma(s)$ sú priemerná a štandardná odchýlka pomeru R'/R pre nejakú databázu stego-obrazov.

Obrázok, ktorý bude mať pomer pod touto hranicou, tak je s veľkou pravdepodobnosťou stego. Ak je pomer nad hranicou, potom to s veľkou pravdepodobnosťou dokazuje, že v sebe nemá žiadnu ukrytú informáciu.

Ako získať túto hranicu Th sa čitateľ môže dozvedieť v [**11**]. Takisto v [**11**] je ukázané, že RQP útok funguje spoľahlivo len vtedy, ak počet unikátnych farieb v nosiči je menší ako 30 percent z celkového počtu pixelov toho istého nosiča.

Výsledok dokonca bude výrazne nespoľahlivý, ak počet unikátnych farieb presiahne 50 precent z celkového počtu pixelov. Ďalšou nevýhodou tohto útoku je, že ho nemôžeme aplikovať na obrázky so šedou škálou farieb, funguje len pre RGB obrázky.

Otázkou ale stále zostáva, či tento algoritmus spoľahlivo funguje pre rôzne dĺžky správ.

2.5. Chi-kvadrát útok.

2.5.1. Chi-kvadrát test dobrej zhody

Chi-kvadrát testy sú založené na porovnaní rozdielnosti medzi nameranými početnosťami a početnosťami ideálnymi. Rozdiel je meraný pomocou normovaného kvadratického kritéria, ktoré má chi=kvadrát rozdelenie (odtiaľ ch-kvadrát testy). Pre test sa používajú absolutné početnosti O výskytu sledovaného znaku, tzv. *pozorované* (observed) početnosti a absolútne početnosti E, ktoré presne odpovedajú H_0 (nulová hypotéza), tzv. *teoretické* alebo *očakávané* početnosti (expected).

Pre namerané početnosti O_i, $i = 1, 2, \ldots, n$ a teoretické početnosti E_i, $i = 1, 2, \ldots, n$ má štatistika chi-kvadrát tvar:

$$\chi^2 = \sum_{i=1}^{n} \frac{(O_i - E_i)^2}{E_i}.$$

Štatistika meria vzdialenosť medzi pozorovanými a teoretickými početnosťami (je nezáporná). Ak sú početnosti rovnaké, rovná sa nule. Čím viac sú početnosti odlišné, tým je hodnota štatistiky väčšia. Nulová hypotéza testu je zhoda početností, alternatívna hypotéza je nezhoda. Test je vždy pravostranný s kritickým oborom

$$W = (\chi^2_\alpha, \infty)$$

a p-hodnotou

$$p_v = P(\chi^2 > \chi^2_r).$$

Pre testovanie hypotézy o hodnotách pravdepodobností $p_1, \ldots, p_k$, s ktorými nastávajú jednotlivé výsledky náhodného pokusu (o k možných výsledkoch), na základe pozorovaných početností $O_1, \ldots, O_k$ výsledkov pri n nezávislých pokusoch,

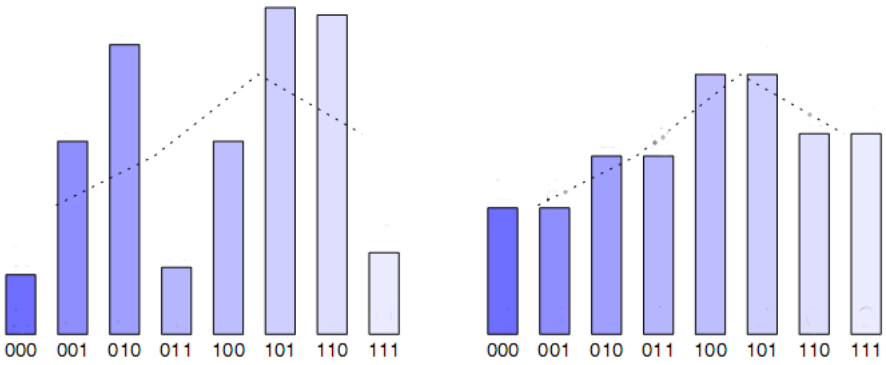
výsledok č.	1	...	k
pozorované početnosti	O_1	...	O_k
očakávané početnosti	np_1	...	np_k

kde testujeme nulovú hypotézu

$$H_0 : p_1 = p_1^0, \ldots, p_k = p_k^0$$

proti

$$H_1 : p_j \neq p_j^0$$



Obrázok 2.3. Príklad transformácie hodnôt bajtov (PoVs).

aspoň pre jedno j (to znamená, že H_0 neplatí), kde $p_1^0, \ldots, p_k^0 \in (0,1)$, $\sum_j p_j^0 = 1$, sú dané čísla, sa používa test založený na štatistike chi-kvadrát, kde $E_j = np_j^0$.

Za predpokladu, že $E_j > 5$ pre všetky $j = 1, \ldots, k$, zamietame hypotézu H_0 približne na hladine významnosti α, ak

$$\chi^2 > \chi^2_{1-\alpha}(k-1),$$

kde $\chi^2_{1-\alpha}(k-1)$ je $(1-\alpha)$-kvantil rozdelenia χ^2_{k-1}.

Ak nie je podmienka $E_j > 5$ splnená pre každé j, je možné najprv niektoré výsledky (tj. početnosti a pravdepodobnosti) zlúčiť.

Pri platnosti H_0 sú E_j očakávanými početnosťami a štatistika chi-kvadrát má asymptoticky pre n $\to \infty$ rozdelenie χ^2_{k-1}. Kritický obor je tvorený hodnotami χ^2 blízkymi ∞. Viac o štatistických testoch v [**7**].

2.5.2. PoVs a Chi-kvadrát útok

Definícia. Frekvenciou farby r_k rozumieme počet všetkých pixelov v obrázku s touto hodnotou. Histogram nám teda ukazuje všetky frekvencie farieb vyskytujúcich sa v obrázku.

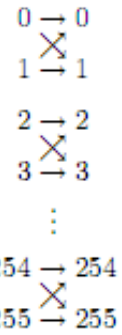
Definícia. Distribúciou budeme nazývať rozloženie frekvencií v poradí za sebou pri konkrétnom obrázku. Distribúcia má takisto istú súvislosť s histogramom.

Prepisovanie LSB transformuje hodnoty na hodnoty, ktoré sa líšia len v LSB. Tieto párové hodnoty sa nazývajú PoV (pairs of values). Ak bity, použité na prepísanie LSB, sú rovnomerne rozložené, frekvencie obidvoch hodnôt každej PoV sú rovnaké. Na obrázku 2.3 je znázornený príklad vloženia rovnomerne rozdelenej správy do obrázku, kde je vidieť zmena histogramu.

Označme x, y frekvencie PoV v originálnom obrázku. Podobne označme x', y' frekvencie toho istého PoV po prebehnutí steganografického algoritmu. S predpokladom, že bity, použité na prepísanie LSB, sú rovnomerne rozdelené, dostávame

$$x' = \frac{x}{2} + \frac{y}{2},$$
$$y' = \frac{x}{2} + \frac{y}{2},$$

čo súhlasí s obrázkom 2.3.



Obrázok 2.4. Príklad transformácie hodnôt bajtu (možné PoV).

Príklad. Pixel, ktorý má hodnotu 100 v originálnom obrázku, získa buď hodnotu 101, alebo ostane s hodnotou 100 v steganografickom obrázku. Podobne, pixel, ktorý má hodnotu 101 v originálnom obrázku, získa buď hodnotu 100, alebo ostane s hodnotou 101. Teda dvojica $\{100, 101\}$ je PoV. Vo všeobecnom prípade, v 8-bitovej škále, $\{2k, 2k+1 | 0 \leq k \leq 127\}$ formuje PoVs.

Idea štatistických útokov je porovnať teoreticky očakávané frekvencie distribúcií v steganogramoch s nejakou testovacou distribúciou pri sledovaní na nejakom nosiči. Kritický bod v tomto prípade je, ako získať teoreticky očakávanú frekvenciu distribúcie (napríklad frekvenciu výskytu môžeme sledovať až po aplikovaní steganografických zmien). Táto frekvencia nesmie byť odvodená z nejakého náhodného príkladu, pretože tento náhodný príklad už môže byť zmenený steganografickými operáciami. Taktiež vo väčšine prípadov nemáme k dispozícii originálny obrázok, aby sme ho mohli porovnávať a odvodiť očakávanú frekvenciu. V originále je očakávaná frekvencia aritmetický priemer dvoch frekvencii v PoV. Pretože vkládacia funkcia prepisuje LSB, nemení sa suma týchto frekvencií. Počet nepárnych hodnôt frekvencie je prenesený na korešpondujúce párne hodnoty frekvencie v každých PoV a naopak. Ak suma ostáva konštantná, potom aritmetický priemer je rovnaký pre PoV v obidvoch prípadoch (originálny nosič a každé korešpondujúce steganografické médium). Tento fakt nám pomáha získať teoreticky očakávanú frekvenciu rozloženia z náhodného vzoru. Teda nepotrebujeme originálny nosič pre tento útok.

Stupeň podobnosti získanej distribúcie a teoreticky očakávanej je kritérium pravdepodobnosti, že bola prevedná nejaká steganografická operácia. Stupeň podobnosti je determinovaný použitím Chi-kvadrát testu [**7**]. Tento test operuje na zmapovaných záznamoch v kategóriách. Uskutočňuje to v nasledujúcich krokoch:

(1) Predpokladajme, že máme k kategórií, a že máme nejaký náhodný vzor pozorovania. Každé pozorovanie musí spadať práve do jednej z kategórií. Kategórie sú buď všetky paletové farby, všetky frekvencie farieb, DCT koeficienty atd (záleži od typu obrázka). Bez újmy na obecnosti, sústredime sa na nepárne hodnoty PoV média, na ktoré útočime. Ich minimálna teoreticky očakávaná frekvencia musí byť väčšia ako 4, môžeme unifikovať kategórie kvôli platnosti tejto podmienky.

(2) Teoreticky očakávaná frekvencia v kategórii i po vložení rovnomerne rozloženej správy je:

$$n_i^* = \frac{|\{farba|indexfarby \in \{2i, 2i+1\}\}|}{2}$$

(3) Nameraná frekvencia výskytu v našom náhodnom vzore je:

$$n_i = |\{farba|indexfarby = 2i\}|$$

(4) χ^2 hodnota je daná ako:

$$\chi^2_{k-1} = \sum_{i=1}^{k} \frac{(n_i - n_i^*)^2}{n_i^*},$$

s $k-1$ stupňami voľnosti.

(5) p je pravdepodobnosť tejto hodnoty pri podmienke, že distribúcie n_i a n_i^* sú rovnaké. Je vypočítaná integráciou hustoty rozloženia:

$$p = 1 - \frac{1}{2^{\frac{k-1}{2}}\Gamma(\frac{k-1}{2})} \int_0^{\chi^2_{k-1}} e^{-\frac{x}{2}} x^{\frac{k-1}{2}-1} dx,$$

kde Γ je Eulerova Gamma funkcia. Teda ak nezamietneme hypotézu H_0, tak výsledna pravdepodobnosť sa bude blížiť k nule (to znamená, že tvrdíme, že teoreticky očakávana a pozorovaná distribúcia sú skoro rovnaké a pravdepodobnosť ukrytej správy je minimálna).

Príklad. Predpokladajme obrázok v šedej škále (tj. 8-bit pp). Nech X, Y sú také vektory, že $x_k = frekvencia(2k)$ a $y_k = frekvencia(2k+1)$, $0 \leq k \leq 127$. Teoreticky očakávaná frekvencia (teda frekvencia, ktorá by mala byť nameraná v obrázku, ktorý skúmame, ak hypotéza platí) je $z_k = \frac{x_k + y_k}{2}$. Predpokladajme, že máme 128 kategórií (pretože $\frac{256 \text{ odtieňov}}{2}$). Bez újmy na všeobecnosti sa môžeme sústrediť na párne hodnoty PoV, takže nameraná frekvencia výskytu v kategórii k je x_k. Kedykoľvek, ak súčet frekvencií $2k$ a $2k+1$ je menší alebo rovný ako 4, počet kategórií je o jednu menší. Vypočítame χ^2 štatistiku s $k-1$ stupňami voľnosti:

$$\chi^2_{k-1} = \sum_{i=0}^{127} \frac{(x_i - z_i)^2}{z_i}, \ kde \ z_i = \frac{x_i + y_i}{2}.$$

Predopkladáme, že pre stego-obrázok bude hodnota χ^2_{k-1} relativne malá, pretože x_i by mala byť blízko z_i, a pre originál naopak. Vypočítame pravdepodobnosť p, pomocou ktorej si to overíme.

3

ANALÝZA STEGANOANALÝZ

3.1. Úvod.

V tejto kapitole si ukážeme, ako spoľahlivo detekujú jednotlive steganoanalýzy zmenu digitálnych obrázkov. Ukážeme si to na aplikácii steganografického algoritmu na nejakých vybraných obrázkoch. Obrázky zvolíme tak, aby sa od seba markantne líšili, a tým pádom by sme videli rozdiely medzi rôznymi rozloženiami farieb. Budeme sledovať znaky, ktoré tieto algoritmy vytvoria a aplikujeme steganoanalýzu. Pokúsime sa vyvodiť dôsledky a navrhnúť algoritmus, ktorý bude odolný proti známej steganoanayze. Uvidíme, či je vôbec možné takýto algoritmus zostrojiť.

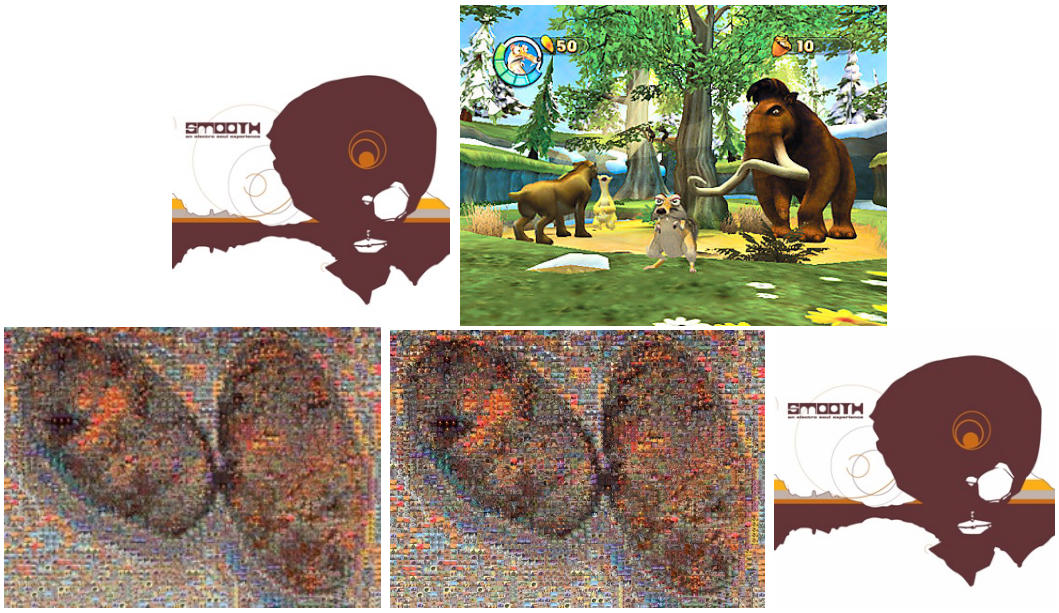
Pre tieto účely som zostavil menšiu databázu obrázkov, ktoré som stiahol náhodne z internetu, a predpokladám, že ešte na žiadny z nich nebol aplikovaný steganografický algoritmus. Tvoria ju obrázky:

- **Husté (dense)** - obrázky s bohatým rozložením farieb.
- **Hladké (smooth)** - obrázky s veľkými homogénnymi časťami.
- **Náhodné** - obrázky s náhodným rozložením farieb.
- **Husté steganografické** - husté obrázky, ktoré sú v plnej miere modifikované steganografiou.
- **Hladké steganografické** - hladké obrázky, ktoré sú v plnej miere modifikované steganografiou.

Celá databáza je rozdelená na jednotlivé druhy obrázkov a každá ich obsahuje práve 60. Databázu môžete nájsť na priloženom DVD.

Pre steganografický algoritmus, pomocou ktorého budeme testovať obrázky, budeme uvažovať nasledujúce predpoklady:

- Vkládací algoritmus bude vkládať najviac jeden bit na pixel. Teda niektoré pixely nemusia obsahovať vložený bit.
- Vkládací algoritmus bude vkládať bity postupne, začínajúc v prvom pixely obrázka, prejde prvý riadok, a pokračuje na druhom riadku, atd. Tento postup bude aplikovať až do vyčerpania bitov, ktoré sa majú vložiť (samozrejme predpokladáme, že počet bitov nie je väčší ako počet pixelov v obrázku). Toto nám potom dovoľuje jednoducho testovať vkladanie rôznych dĺžok správ.
- Každá správa bude generována náhodne s dĺžkou, ktorá nám bude vyhovovať. Týmto predídeme tomu, že bz správa mohla mať nejaké špecifické vlastnosti.
- Počet bitov správy nie je väčší ako počet pixelov v obrázku. To je v súlade s tým, že každý pixel môže obsahovať najviac jeden vložený bit.
- Správa je náhodná distribúcia núl a jedničiek. Ak sa správa pred vložením šifruje, tak šifrovaná postupnosť túto vlastnosť splňuje.



OBRÁZOK 3.1. Obrázky v poradí od prvého: hladký, náhodný, hustý, hustý steganografický, hladký steganografický.

Náš algoritmus teda bude vyerať nasledovne:

`Algoritmus:`
`VSTUP: originálny RGB image, počet percent zo všetkých pixelov, ktoré budeme modifikovať`
`VÝSTUP: RGB stegoimage`

(1) `Vypočíta počet pixelov, ktoré budú použité.`
(2) `Pre každý pixel od začiatku, až po posledný v poradí (podľa percenta):`
- `Zvoľ nasledujúce 3 hodnoty pre vkladanie náhodne (teda 0 alebo 1).`
- `Do zložiek R, G, B vlož postupne tieto hodnoty.`

Klasický zmysluplný text sa chová veľmi podobne ako náš náhodný text, preto namiesto neho bude uvažovať algoritmus popísaný vyššie.

3.2. Analýza histogramov.

Pre jednoduchšie znázornenie výsledkov testov som vybral z každej kategórie obrázkov jedného reprezentanta. Budeme sledovať, ako sa bude postupne meniť histogram obrázka vzhľadom k modifikovanej časti našim algoritmom. Vybrané obrázky sú znázornené na obrázku 3.1.

Pozrime sa najprv na histogramy hustého obrázka, viz obrázok 6.13. Všimnime si, že od histogramu originálu sa histogramy ostatných stegoobrazov zreteľne nelíšia. Algoritmus svojou modifikáciou nevytvoril žiadne markantné zmeny, ktoré by sme mohli nejakým spôsobom detekovať. Z toho, a ešte z ďalších histogramov (obrázky 6.14, 6.15, 6.16, 6.17), vidíme, že metóda, ktorá sa spolieha na zmenu histogramov nie je spoľahlivá, teda nedetekuje spoľahlivo aplikovanú steganografiu.

3.3. Raw Quick Pair Analysis

Pre analýzu tejto metódy nám veľmi dobre poslúži naša databáza obrázkov. Podľa párovej analýzy potrebujeme poznať počet všetkých párov pixelov a počet všetkých skoro párov pixelov. Na základe týchto hodnôt a štatistických údajov vytvoríme hranicu detekovateľnosti, podľa ktorej rozhodujeme o obsahu obrázka. Tento test je detailne popísaný v [**11**], preto sa ním nebudeme zaoberať (čitateľ si výsledky môže sám overiť a prečítať). Výsledky tohto testu nájdete aj na priloženom DVD.

Namiesto toho sa pozrieme na to, ako sa tento test bude tváriť, ak miesto unikátnych farieb vezmeme do úvahy počet všetkých pixelov (to znamená, že vezmeme do úvahy všetky farby, aj tie duplicitné). Vtedy by malo byť logické, že ak nosič bude hladký, tak po aplikovaní steganografického algoritmu sa počet skoro párov výrazne zvýši. Na výsledky použijeme hranicu Th (viz. kapitola 2.4.) a vyvodíme dôsledky.

Z každej kategórie obrázkov si preto vytvoríme tabuľku, ktorá bude obsahovať počet párov originálu U, počet skoro párov originálu P, počet skoro párov stegoobrazu P', pomer R v originály, pomer R' v stegoobraze, a nakoniec pomer R'/R. Všetky takéto tabuľky môžete nájsť v prílohe.

Z pomeru R'/R vidíme, ako veľmi sa obrázok modifikoval po aplikovaní steganografického algoritmu. Vypočítame priemernú a štandardnú odchýlku pomeru R'/R, a pozrieme sa, ako spoľahlivo detekuje hranica Th z párovej analýzy steganografiu.

Definícia. Štandardná odchýlka σ náhodnej veličiny je druhá odmocnina rozptylu σ^2. Pre množinu o veľkosti n je štandardná odchýlka definovaná ako

$$\sigma = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(x_i - \bar{x})^2},$$

kde $\bar{x}$ je priemer distribúcie.

Definícia. Priemern8 odchýlka μ je priemer absolutných odchýlok nejakej množiny dát. Pre množinu o veľkosti n je priemerná odchýlka definovaná ako

$$\mu = \frac{1}{n}\sum_{i=1}^{n}|x_i - \bar{x}|,$$

kde $\bar{x}$ je priemer distribúcie.

Vypočítame priemernú a štandardnú odchýlku v databázi originálnych obrázkov a v databázi stegoobrazov, pričom ako priemer nám poslúži pomer $R'/R = 1$ (pretože tento pomer znamená rovnosť skoro párov originálu a stegoobrazu).

V tabuľkách 3.1, 3.2, 3.3, 3.4, 3.5 vidíme štandardnú a priemernú odchýlku našej databáze. Povšimnime si, že pri modifikácii väčšej časti obrázka sa zväčšujú obidve odchýlky. Je to logické, pretože pri väčsej modifikácii vzniká väčší počet skoro párov. Ďalej si všimnime, že pri steganografických obrázkoch vzniká o mnoho menšia odchýlka.

Vypočítame si ešte štandardnú a priemernú odchýlku pre celú databázu bez ohľadu na modfifikovanú časť (tabuľka 3.6).

Teraz máme všetko potrebné, aby sme mohli určiť hranicu Th, podľa ktorej budeme rozhodovať o obsahu obrázka. Pripomeňme si vzorec pre Th zo sekcie

2.4.

$$Th = \frac{\mu\sigma(s) + \mu(s)\sigma}{\sigma + \sigma(s)}$$

Tabuľka 3.1. Štandardná a priemerná odchýlka pomerov R'/R v hustých obrázkoch

Počet modifikovanej časti	Štandardná odchýlka σ	Priemerná odchýlka μ
Husté 10%	0.043097292526979705	0.027395211806213574
Husté 20%	0.07052970859011455	0.04499947685568192
Husté 30%	0.0814805452879241	0.05649939235375368
Husté 40%	0.08992856669210865	0.06611786784596561
Husté 50%	0.10032357578625782	0.07630969104584129
Husté 60%	0.11025623905521804	0.08486458895482746
Husté 70%	0.1203524369037646	0.09429540432262472
Husté 80%	0.1298274828553952	0.10240987806244502
Husté 90%	0.14311261436663084	0.11400694086266261
Husté 100%	0.1582464933629212	0.12674337110594233

Tabuľka 3.2. Štandardná a priemerná odchýlka pomerov R'/R v hladkých obrázkoch

Počet modifikovanej časti	Štandardná odchýlka σ	Priemerná odchýlka μ
Hladké 10%	0.023950100623032544	0.01307333989731167
Hladké 20%	0.04721643576062525	0.026518016605265208
Hladké 30%	0.06635688191852339	0.03745530980518836
Hladké 40%	0.08568358702446262	0.04829439093804338
Hladké 50%	0.10061988973716936	0.0575648194794436
Hladké 60%	0.11334579687639354	0.06562044053348276
Hladké 70%	0.12524886285631592	0.07356947090738929
Hladké 80%	0.1349088195189631	0.0814764831720063
Hladké 90%	0.14567563182907325	0.0886103354779694
Hladké 100%	0.15514409094237433	0.0953589082762764

Tabuľka 3.3. Štandardná a priemerná odchýlka pomerov R'/R v hustých steganografických obrázkoch

Počet modifikovanej časti	Štandardná odchýlka σ	Priemerná odchýlka μ
Hladké 10%	0.0014539752742113534	9.517453903865069E-4
Hladké 20%	0.0018431054646685715	0.0012029528831695225
Hladké 30%	0.002118153501526036	0.001310519081833909
Hladké 40%	0.0024200999899777796	0.001449799608842215
Hladké 50%	0.00213389096898709	0.0014865469723542306
Hladké 60%	0.002234575985816496	0.0015519451190709318
Hladké 70%	0.002534766144468748	0.001635328508700959
Hladké 80%	0.0021655690545439865	0.0014786854003666489
Hladké 90%	0.0024541413307943402	0.0018915271614632894
Hladké 100%	0.0025262335042059796	0.0017350996598309814

Podľa našich výpočtov je teda hranica $Th = 0.00795978530842668$.

Vraťme sa k našim obrázkom (3.1) a pozrime sa ako detekuje hranica Th ich obsah (tabuľka 3.7).

Ako vidíme, táto metóda zase nedetekovala steganografické obrázky, a ak hranicu Th porovnáme s ostatnými pomermi z tabuliek v prílohe, tak zistíme, že veľmi málo sa trafíme do správneho výsledku.

3.4. Chi-kvadrát analýza.

Idea chi-kvadrát útoku je porovnať teoreticky očakávané frekvencie distribúcií v steganogramoch s nejakou testovacou distribúciou pri sledovaní na nejakom nosiči.

TABUĽKA 3.4. Štandardná a priemerná odchýlka pomerov R'/R v hladkých steganografických obrázkoch

Počet modifikovanej časti	Štandardná odchýlka σ	Priemerná odchýlka μ
Hladké 10%	0.0028107804456110595	5.562380865551698E-4
Hladké 20%	0.005338602559605551	9.541430246835995E-4
Hladké 30%	0.007914867489556639	0.0013256713964568108
Hladké 40%	0.010378762596292892	0.0017094606186948843
Hladké 50%	0.012903739084695548	0.002265739022240547
Hladké 60%	0.014937272941745074	0.0026252241302479086
Hladké 70%	0.017255217862400838	0.003023101755975817
Hladké 80%	0.019393936794359863	0.003311583983484324
Hladké 90%	0.0215090872391052	0.0038330892074389805
Hladké 100%	0.023639673965248693	0.004180012331143319

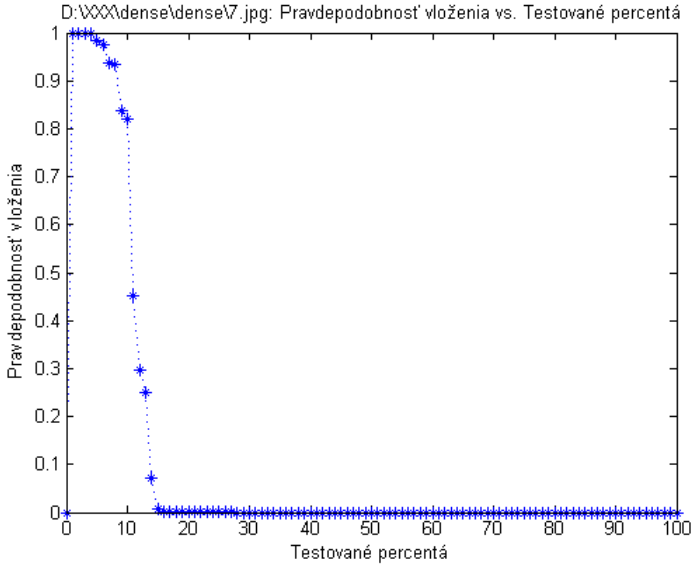
TABUĽKA 3.5. Štandardná a priemerná odchýlka pomerov R'/R v náhodných obrázkoch

Počet modifikovanej časti	Štandardná odchýlka σ	Priemerná odchýlka μ
Hladké 10%	0.04176829539016264	0.02549160123154269
Hladké 20%	0.06542109745048598	0.041183495111586026
Hladké 30%	0.08431037159421788	0.052943470396883505
Hladké 40%	0.10144940473249196	0.06470429094469389
Hladké 50%	0.11553443006511799	0.07459429264517528
Hladké 60%	0.12623134518481197	0.08234465623265645
Hladké 70%	0.1371310065258015	0.09046296021599808
Hladké 80%	0.15159336104935828	0.10218670762542408
Hladké 90%	0.1700386319640291	0.11612430715224879
Hladké 100%	0.18703964609692983	0.12998410519937498

TABUĽKA 3.6. Štandardná a priemerná odchýlka pomerov R'/R v celej databázi obrázkov.

Typ obrázkov	Štandardná odchýlka σ	Priemerná odchýlka μ
Originály	0.11485213127149983	0.07204010750213057
Steganografické	0.010818171544483387	0.0019239206671470292

Podľa algorimtu v sekcii 2.5.2. vytvoríme test a aplikujeme ho zase na naše obrázky 3.1. Budeme sledovať zmenu v grafoch. Na obrázkoch 3.2, 3.3, 3.4 vidíme grafy chi-kvadrát testu s rôznymi modifikovanými časťami. Prvý obrázok vyzerá podľa očakávaní, ale na začiatku to nevyzerá veľmi dôveryhodne. Ostatné dva obrázky už vyzerajú tak, ako by sú v skutočnosti modifikované. V tomto prípade teda chi-kvadrát test nepochybil.



Obrázok 3.2. Originál hustého obrázka a jeho graf chi-kvadrát testu.

Bohužiaľ tento príklad nie je pravidlom a v ostatných prípadoch nám chi-kvadrát test tak veľmi nepomôže. V prílohe sú ďalšie grafy chi-kvadrát testu pre hladký, náhodný a steganografický obrázok. Môžeme si všimnúť, že pri steganografickom obrázku sa už graf chi-kvadrát testu nemení, ani v závislosti na počtu modifikovaných pixelov. Je to preto, lebo náš algoritmus náhodne generuje správy takej dĺžky, akej požadujeme, a teda prepísanie náhodnej správy náhodnou správou nevytvorí žiadny rozdiel.

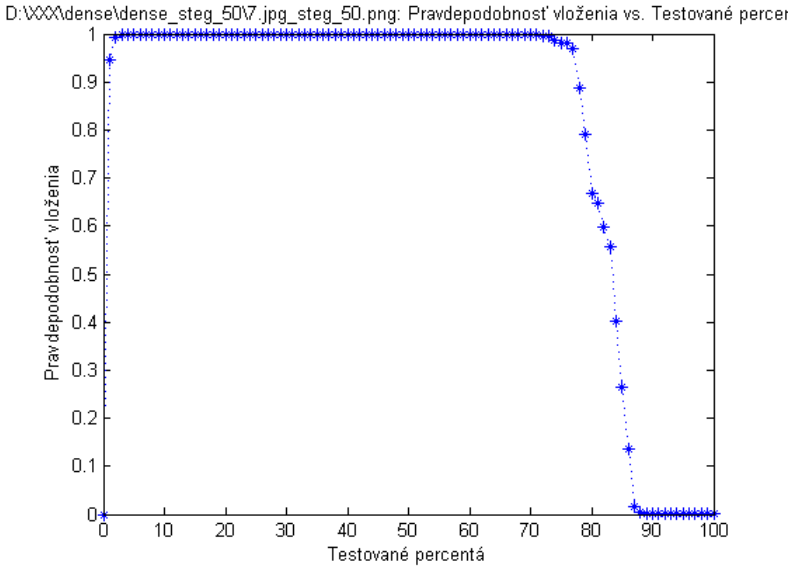
Chi-kvadrát útok je efektívny na algoritmy steganografie, ktoré jednoducho modifikujú LSBs každého pixelu. Toto je tiež užitočné, pretože aj keď takýmto spôsobom modifikujeme celý obrázok, tak voľným okom nebudeme vidieť rozdiel. Preto bol v našom prípade chi-kvadrát útok úspešný, použili sme jednoduchú modifikáciu LSBs pixelov, ktorá vytvára PoVs. Avšak tento útok nám nedá veľmi dôveryhodné výsledky ak použijeme hustý obrázok s dobrým rozložením farieb. Naopak veľmi dobre detekuje hladké obrázky. Náš algoritmus vytvára rovnomerne

Tabuľka 3.7. Detekcia steganografie v obrázkoch podľa hranice Th.

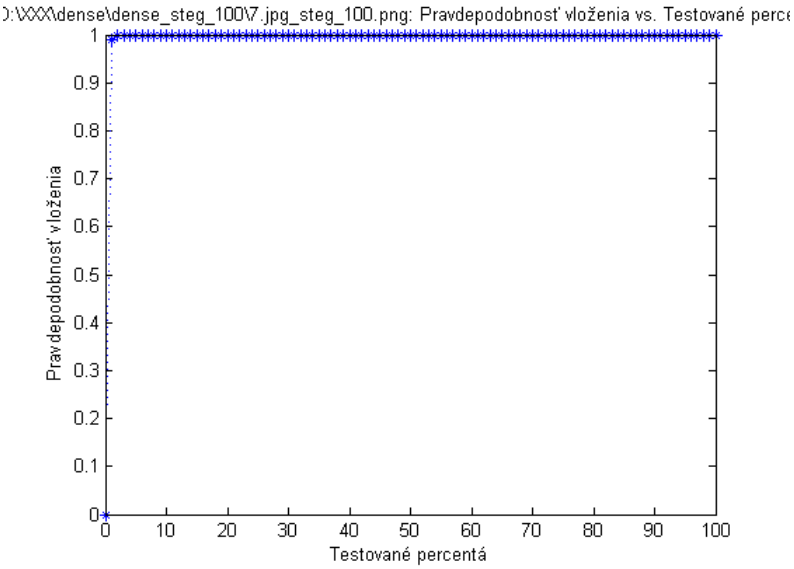
Obrázok	Pomer R	Výsledok
Hustý	0.01003165975125268	non stego
Hladký	0.72803250985717	non stego
Náhodný	0.32408258666567846	non stego
Hustý steganografický	0.010494489830505705	non stego
Hladký steganografický	0.7280153317237966	non stego

rozloženie správy a to je ďalší faktor, prečo je pri týchto steganografických obrázkoch test úspešný. Je totiž stavaný na presne takéto situácie. Ak by sme vytvorili algorimus, ktorý by už nevytváral rovnomerné rozloženie správy a dokonca by to nerobil spôsobom jednoduchej mdifikácie LSBs, potom by na to bol chi-kvadrát útok príliš krátky.

Aby sme si potvrdili to, čo hovoríme v predchádzajúcom odstavci, skúsime vytvoriť algoritmus, ktorý chi-kvadrát test nedetekuje. Bude nám pri tom záležať na týchto veciach:



Obrázok 3.3. Steganografický hustý obrázok s 50% modifikovanou časťou a jeho graf chi-kvadrát testu.



Obrázok 3.4. Steganografický hustý obrázok s 100% modifikovanou časťou a jeho graf chi-kvadrát testu.

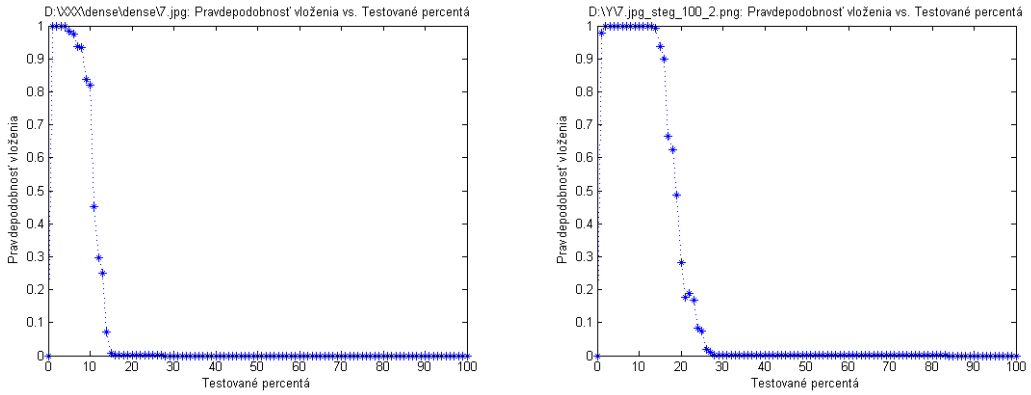
- **Voľba obrázka** - budeme vyberať obrázky, ktoré sú štatisticky husté podľa celého obrázka. Videli sme totiž, že pre takéto obrázky nie je chi-kvadrát test veľmi spoľahlivý. Je veľmi dobre zdokumentovaný fakt, že husté obrázky sú najlepšou voľbou pre steganografiu všeobecne.
- **Voľba pixelov pre vkladanie** - dá sa očakávať, že ak je $|x_k - z_k|$ z príkladu zo sekcie 2.5.2. dosť veľké číslo dokonca aj pre malý počet PoVs, potom je číslo χ^2_{n-1} veľké, a teda pravdepodobnosť p vloženia je blízko nule. Túto ideu môžeme aplikovať na algoritmus.
- **Vyhýbanie sa PoVs** - jedna zo slabostí chi-kvadrát testu je to, že je efektívny len na spomínané algoritmy, ktoré jednoducho modifikuju LSBs a vytvárajú teda PoVs.

Pre tieto naše účely nám postačí modifikovať algoritmus, ktorý sme použili pre naše testy, takýmto spôsobom:

`Algoritmus:`
`VSTUP: originálny RGB image, počet percent`
`zo všetkých pixelov, ktoré budeme modifikovať`
`VÝSTUP: RGB stegoimage`

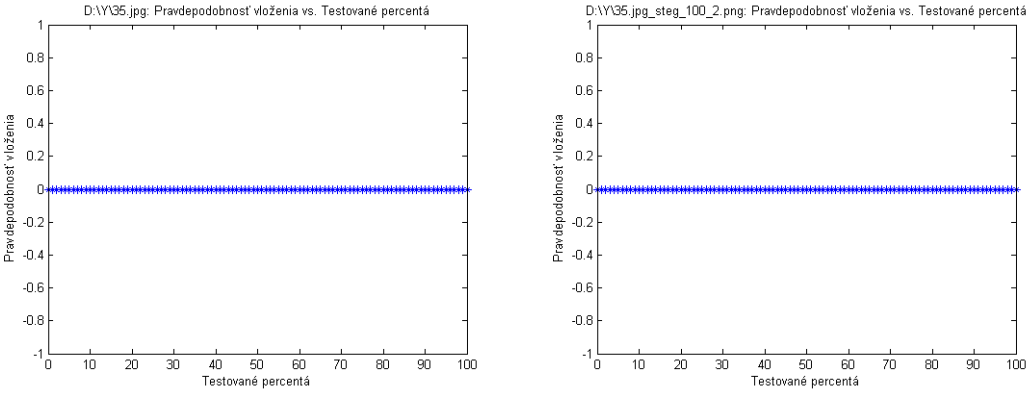
(1) `Vypočíta počet pixelov, ktoré budú použité.`
(2) `Pre každý` **`tretí`** `pixel od začiatku, až po posledný v poradí (podľa percenta):`
   - `Zvoľ nasledujúce 3 hodnoty pre vkladanie náhodne (teda 0 alebo 1).`
   - `Do zložiek R, G, B vlož postupne tieto hodnoty.`

Pozrime sa teraz, ako vyzerajú grafy našich obrázkov aplikovaním tohto trochu modifikovaného steganografického algoritmu.

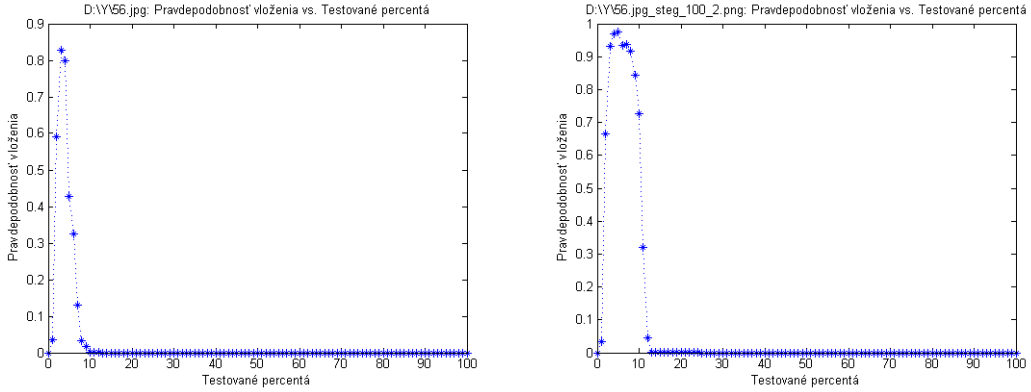


Obrázok 3.5. Originál hustého obrázka (vľavo) a jeho steganogram (100%) použitím druhého steganografického algoritmu (vpravo) a ich graf chi-kvadrát testu.

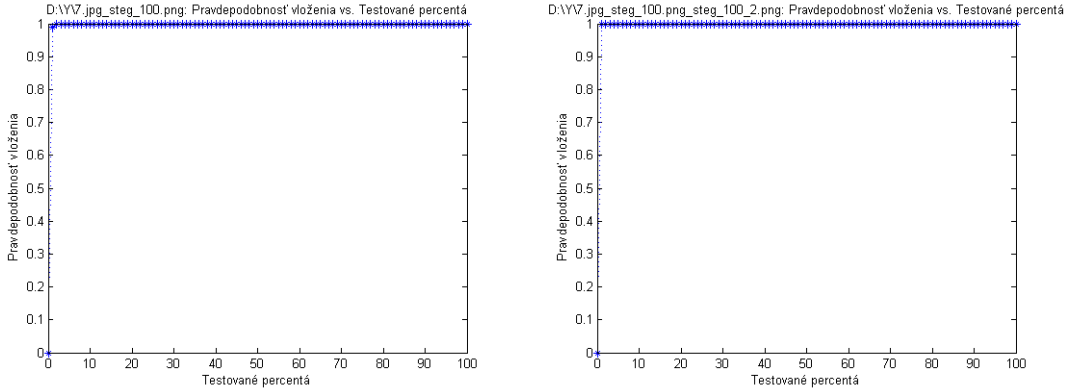
Použili sme algoritmus, v ktorom sme namiesto každého pixelu modifikovali každý tretí pixel. V dôsledku toho sme sa vyhli vytváraniu veľkého množstva PoVs a tým pádom už chi-kvadrát test nie je spoľahlivý (viz obrázky 3.5, 3.6, 3.7, 3.8, 3.9). Výsledky sú znázornené aj na iných, ako hustých obrázkoch. Nevyužili sme



Obrázok 3.6. Originál hladkého obrázka (vľavo) a jeho steganogram (100%) použitím druhého steganografického algoritmu (vpravo) a ich graf chi-kvadrát testu.

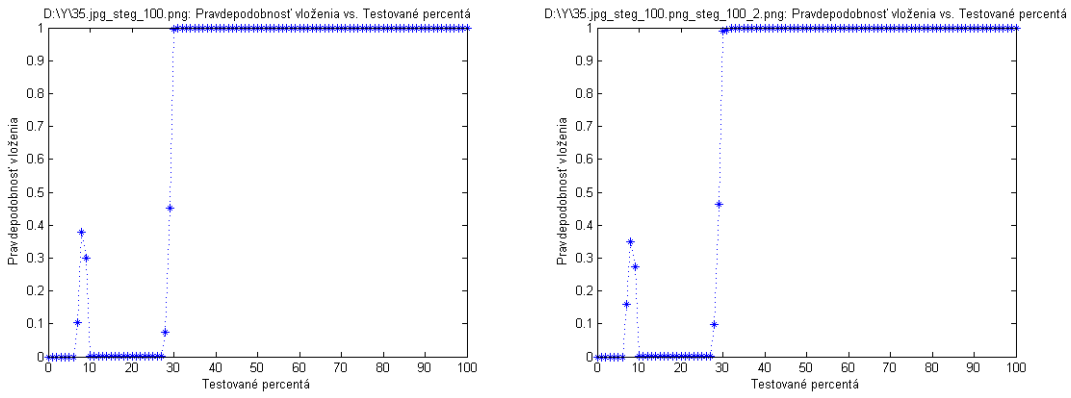


Obrázok 3.7. Originál náhodného obrázka (vľavo) a jeho steganogram (100%) použitím druhého steganografického algoritmu (vpravo) a ich graf chi-kvadrát testu.



Obrázok 3.8. Originál hustého steganografického obrázka (vľavo) a jeho steganogram (100%) použitím druhého steganografického algoritmu (vpravo) a ich graf chi-kvadrát testu.

všetky možnosti, ako sa vyhnúť detekcii chi-kvadrát útoku, ale aj malou triviálnou zmenou sme dokázali tento test "oklamať" (v grafoch sú len malé zmeny).



Obrázok 3.9. Originál hladkého steganografického obrázka (vľavo) a jeho steganogram (100%) použitím druhého steganografického algoritmu (vpravo) a ich graf chi-kvadrát testu.

4 ZÁVER

Steganografia je veľmi pekný nástroj pre utajenie komunikácie. Dovoľuje nám veľké množstvo možností. V digitálnom svete sa tieto možnosti ešte viac rozrastajú a každá steganografia môže vyzerať úplne inak. Videli sme, ako fungujú rôzne steganografické nástroje. Ich rozmanitosť je prakticky nekonečná.

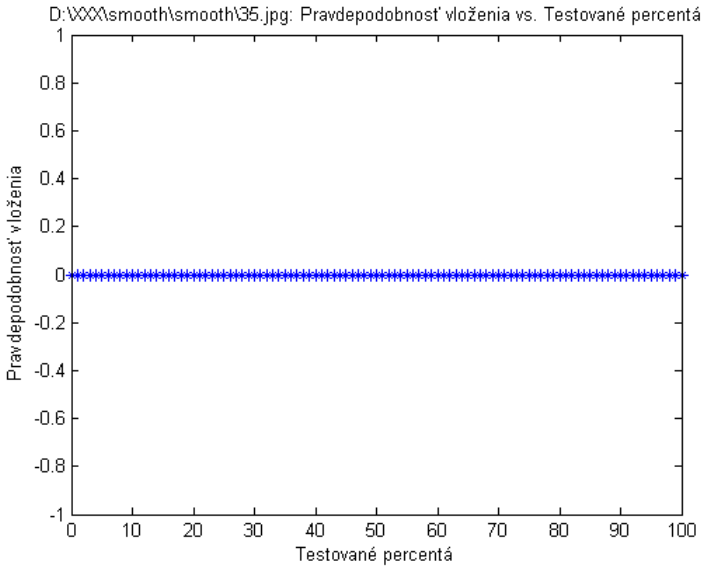
Steganoanalýza začala vznikať paralelne so steganografiou. Ľudia sú zvedavý a majú potrebu zisťovať, o čom sa bavia ostatní. Začali vznikať rôzne steganoanalýzy digitálnych obrázkov, ktoré boli schopné odhaliť steganografiu. Ale ako to tak býva, nič nie je dokonalé, a hlavným problém steganoanalýzy je, že každá z nich funguje len na jeden konkrétny steganografický algoritmus. Stačí algoritmus pozmeniť v konkrétnom smere, a steganoanalýza už bude krátka.

5
OBSAH DVD

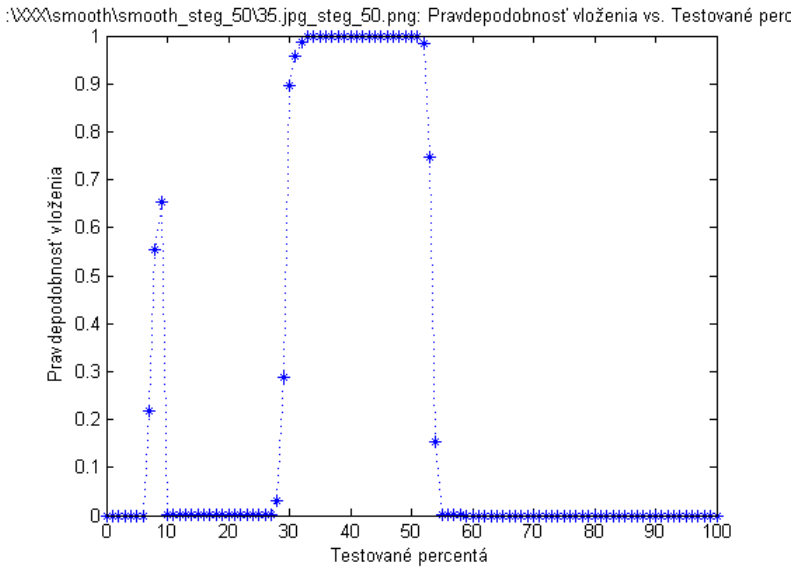
Na priloženom DVD nájdete:

- Bakalársku prácu vo formáte PDF
- Prílohu detailnejších informácií o digitálnych nosičoch typu BMP, PNG, JPEG vo formáte DOC
- Prílohu tabuliek RQP testu vo formáte PDF
- Vlastnú aplikáciu "Stegais" pre využitie steganografie a steganoanalýzy
- Databázu obrázkov
- Databázu histogramov testovaných obrázkov
- Databázu detailných súborov pre RQP test
- Databázu testov Chi-kvadrát
- Zdrojové kódy programov, testov a analýz (amatérske kódy)

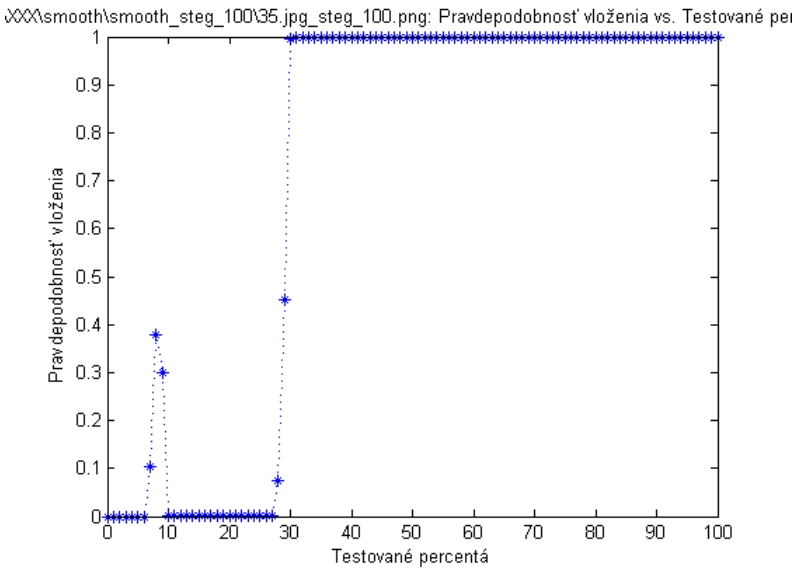
6
PRÍLOHA



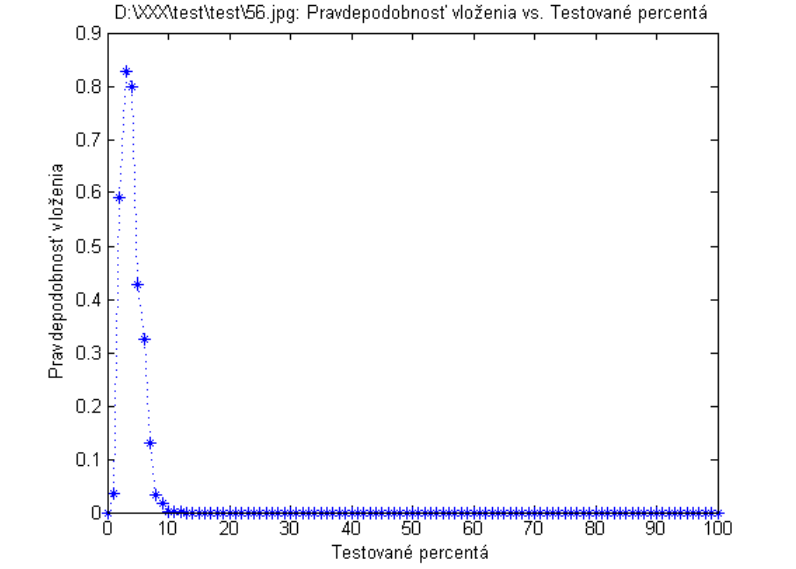
Obrázok 6.1. Originál hladkého obrázka a jeho graf chi-kvadrát testu.



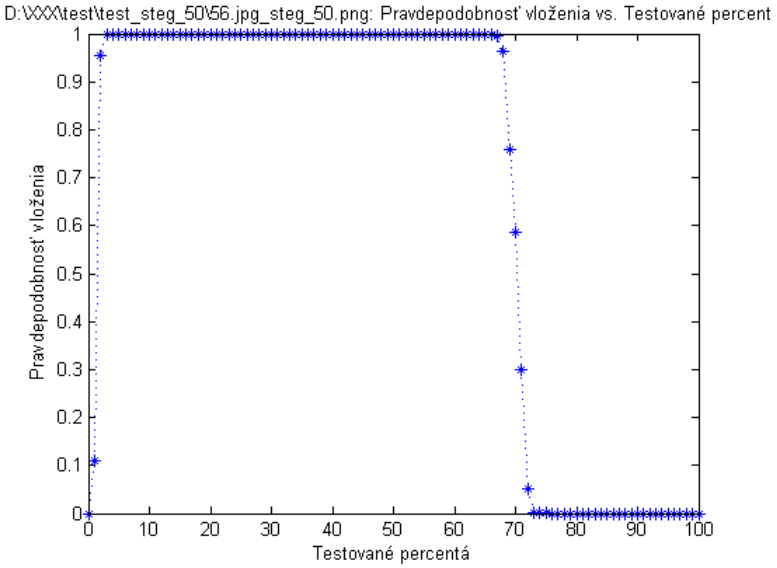
Obrázok 6.2. Steganografický hladký obrázok s 50% modifikovanou časťou a jeho graf chi-kvadrát testu.



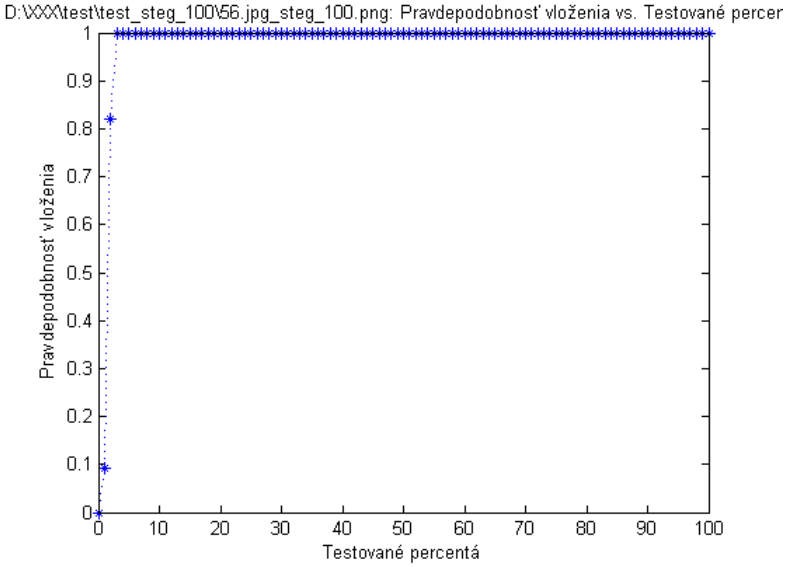
Obrázok 6.3. Steganografický hustý obrázok s 100% modifikovanou časťou a jeho graf chi-kvadrát testu.



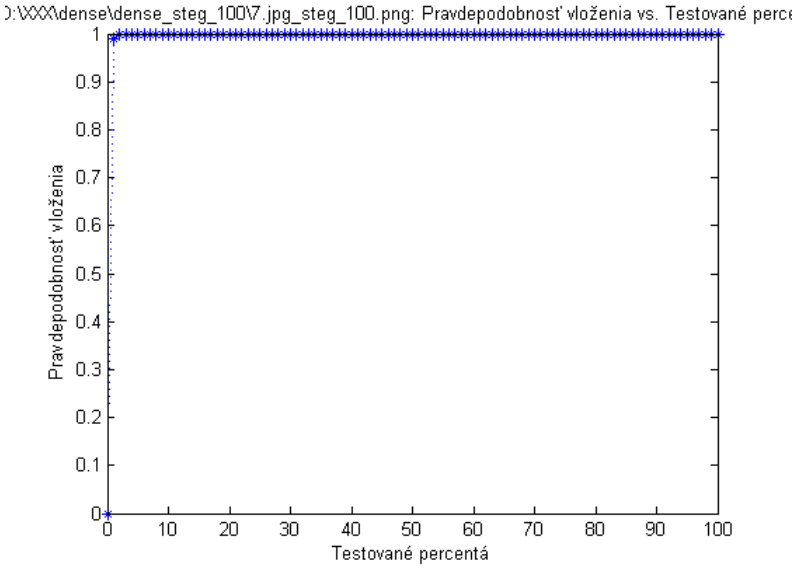
Obrázok 6.4. Originál náhodného obrázka a jeho graf chi-kvadrát testu.



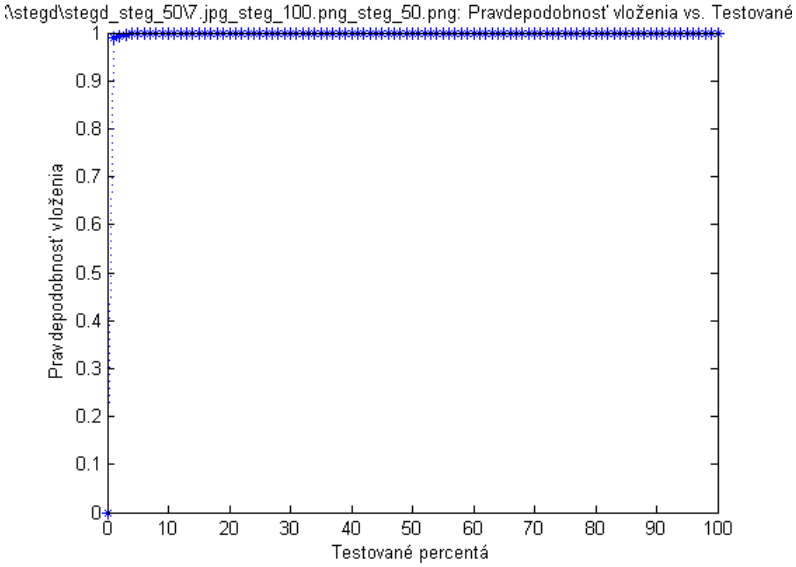
Obrázok 6.5. Steganografický náhodný obrázok s 50% modifikovanou časťou a jeho graf chi-kvadrát testu.



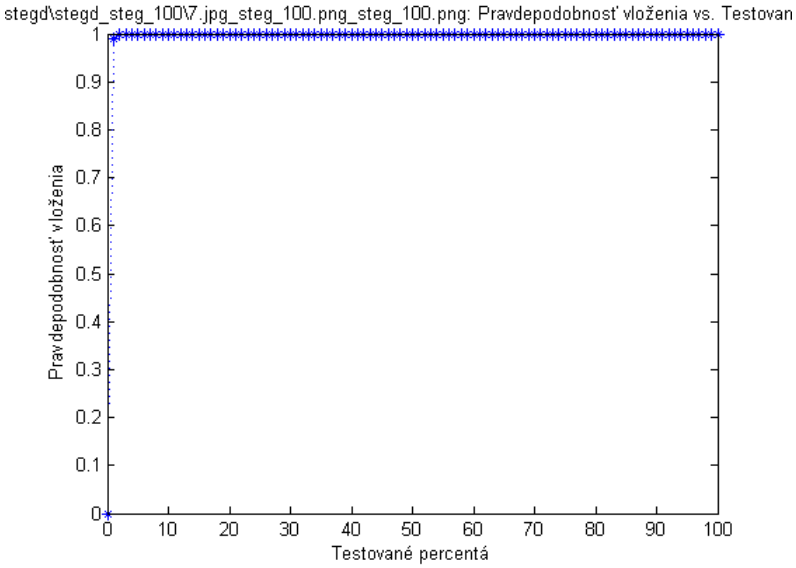
Obrázok 6.6. Steganografický náhodný obrázok s 100% modifikovanou časťou a jeho graf chi-kvadrát testu.



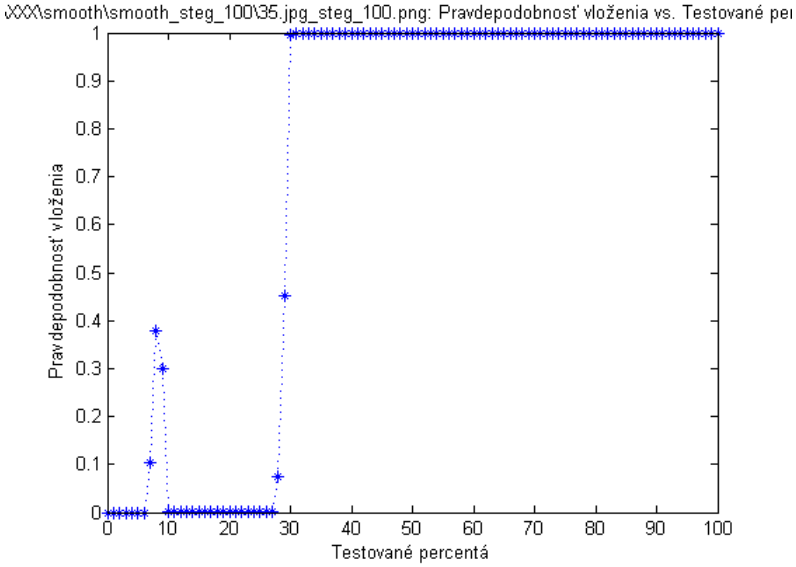
Obrázok 6.7. Originál hustého steganografického obrázka a jeho graf chi-kvadrát testu.



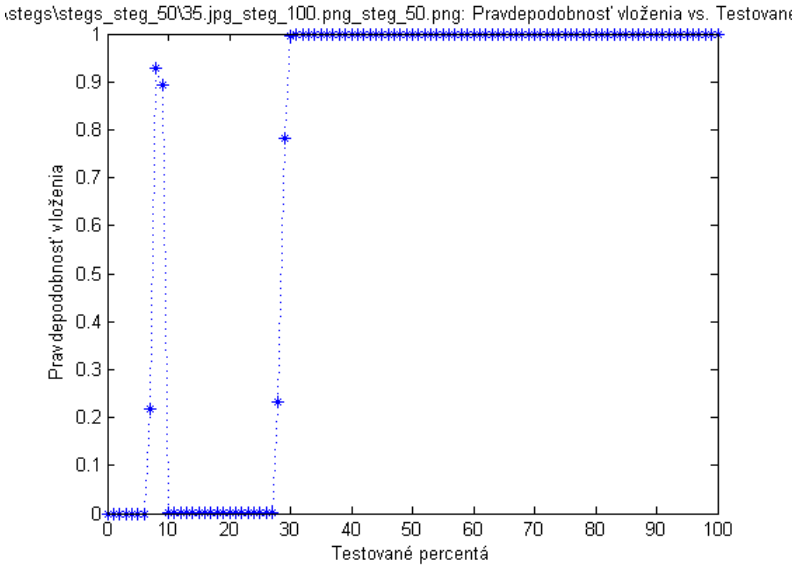
Obrázok 6.8. Steganografický hustý steganografický obrázok s 50% modifikovanou časťou a jeho graf chi-kvadrát testu.



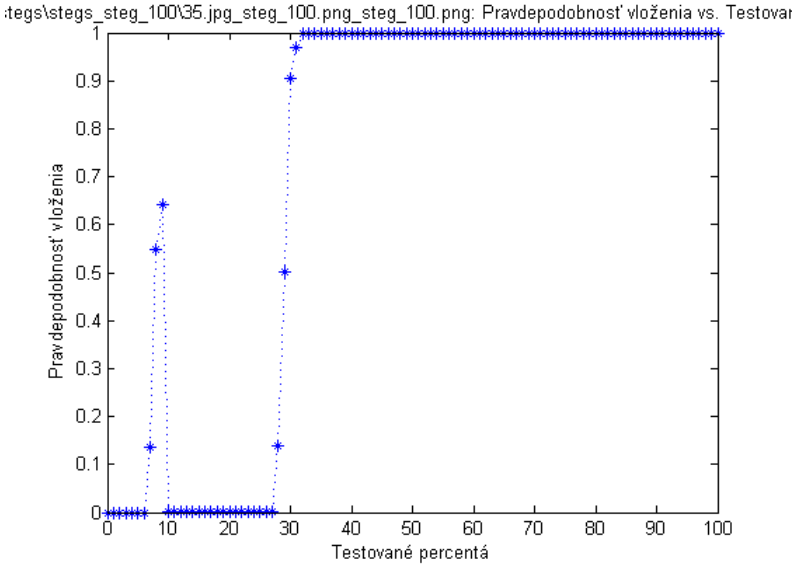
Obrázok 6.9. Steganografický hustý steganografický obrázok s 100% modifikovanou časťou a jeho graf chi-kvadrát testu.



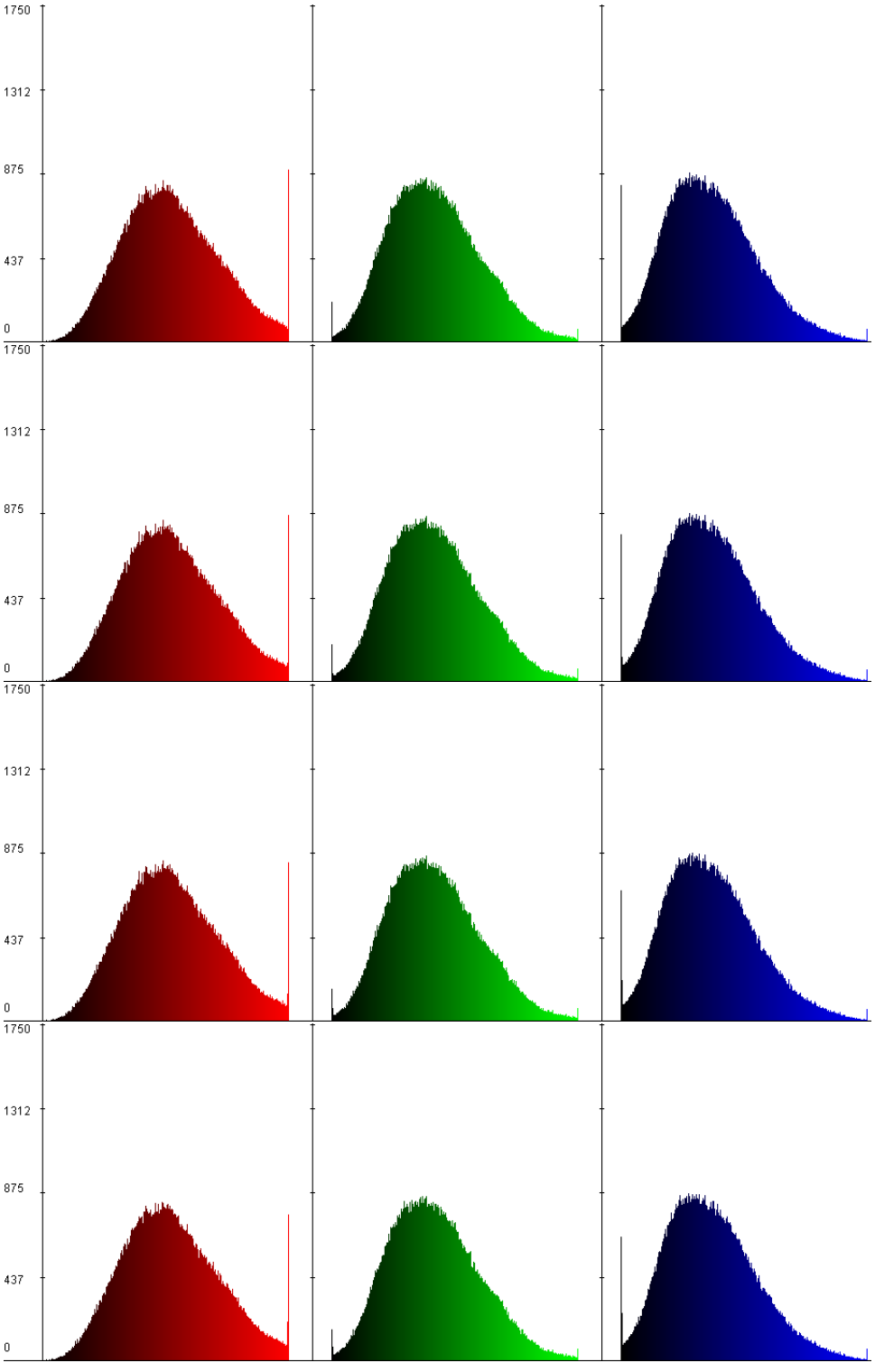
Obrázok 6.10. Originál hladkého steganografického obrázka a jeho graf chi-kvadrát testu.

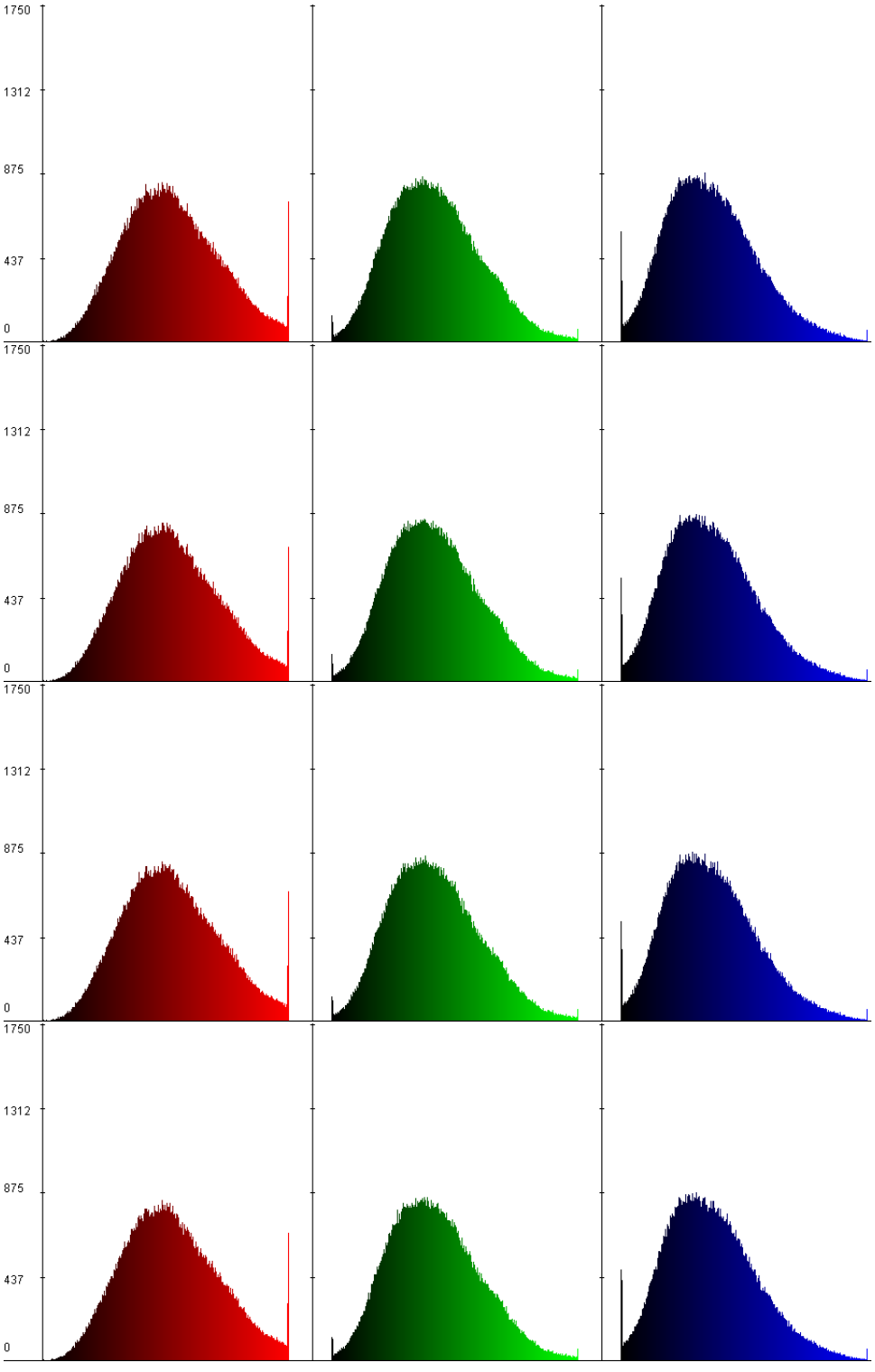


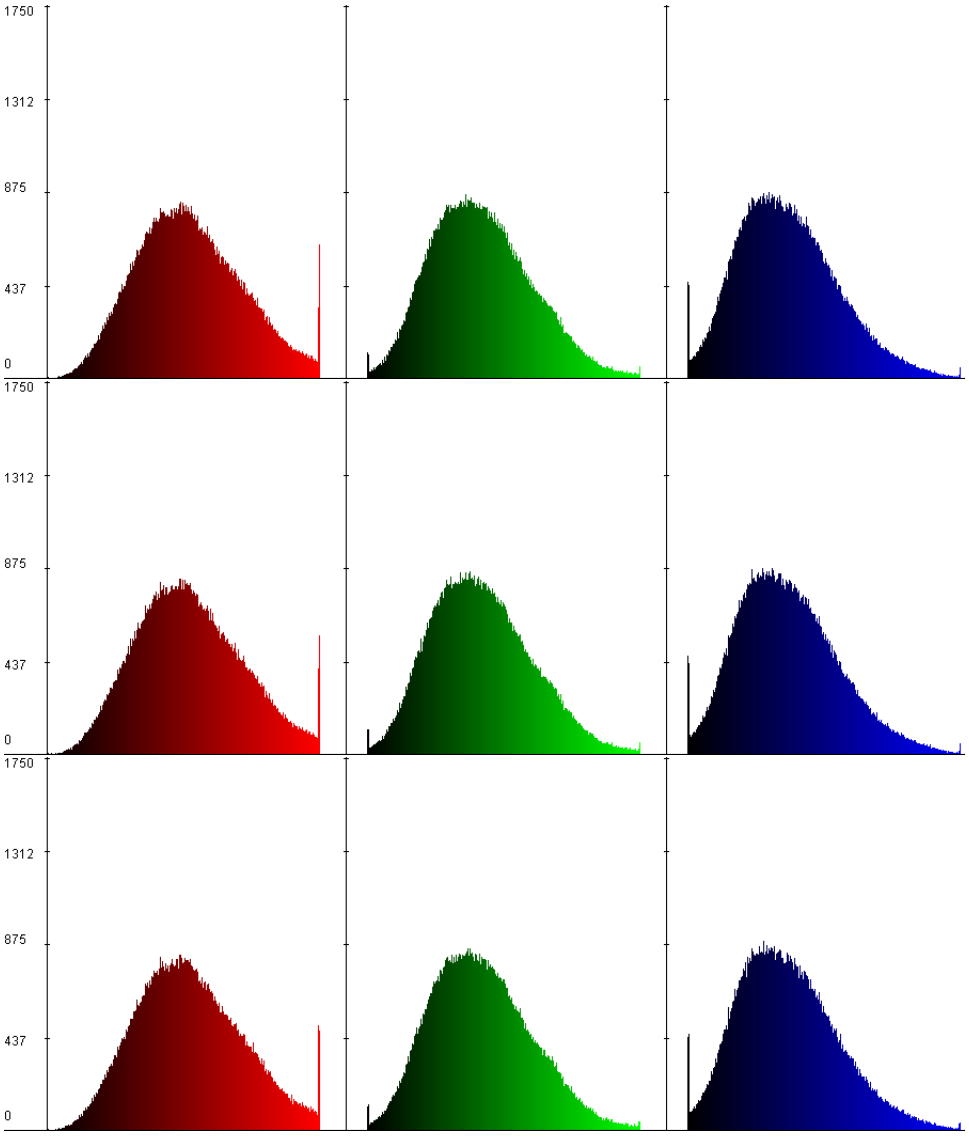
Obrázok 6.11. Steganografický hladký steganografický obrázok s 50% modifikovanou časťou a jeho graf chi-kvadrát testu.



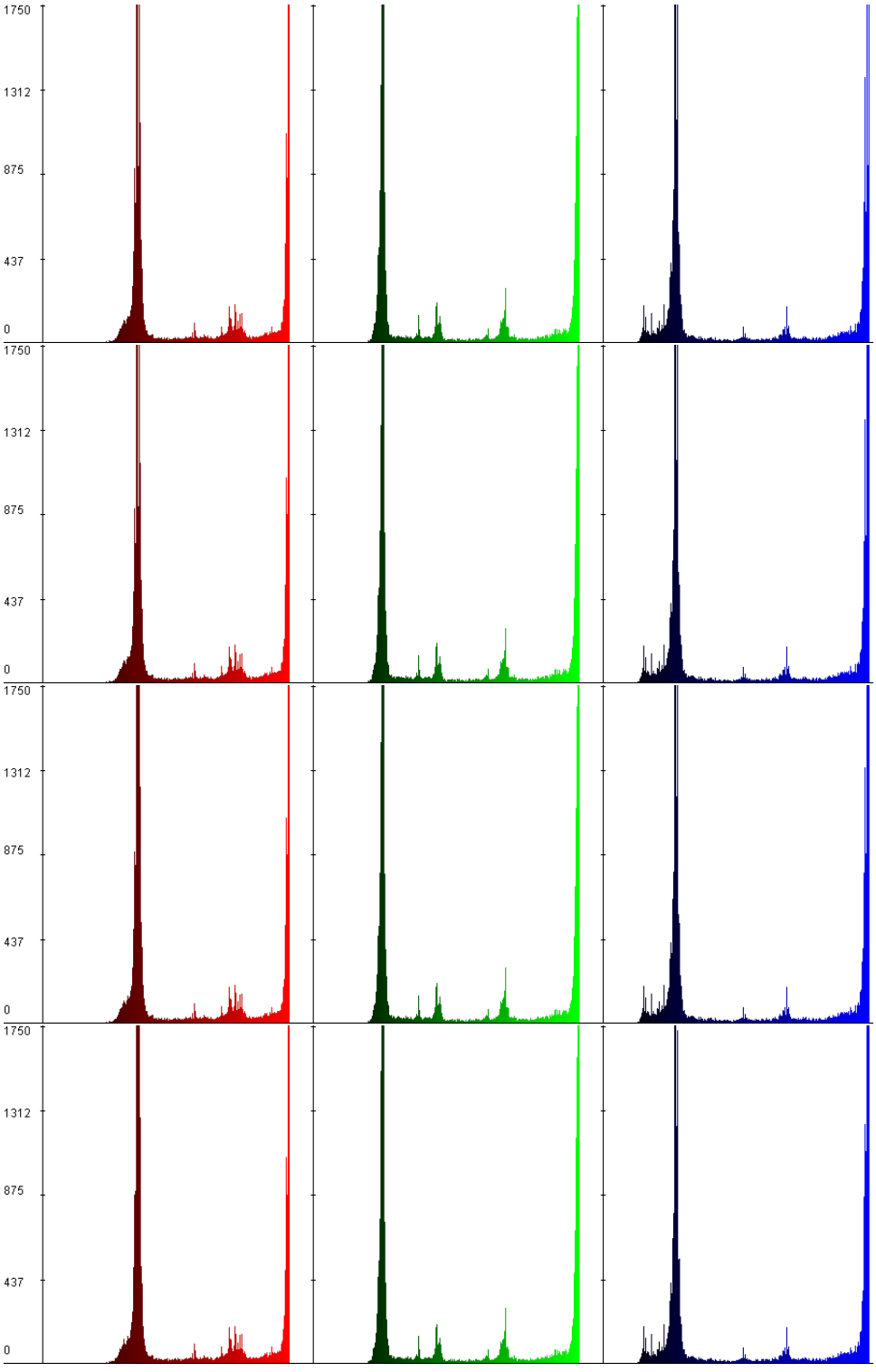
Obrázok 6.12. Steganografický hladký steganografický obrázok s 100% modifikovanou časťou a jeho graf chi-kvadrát testu.

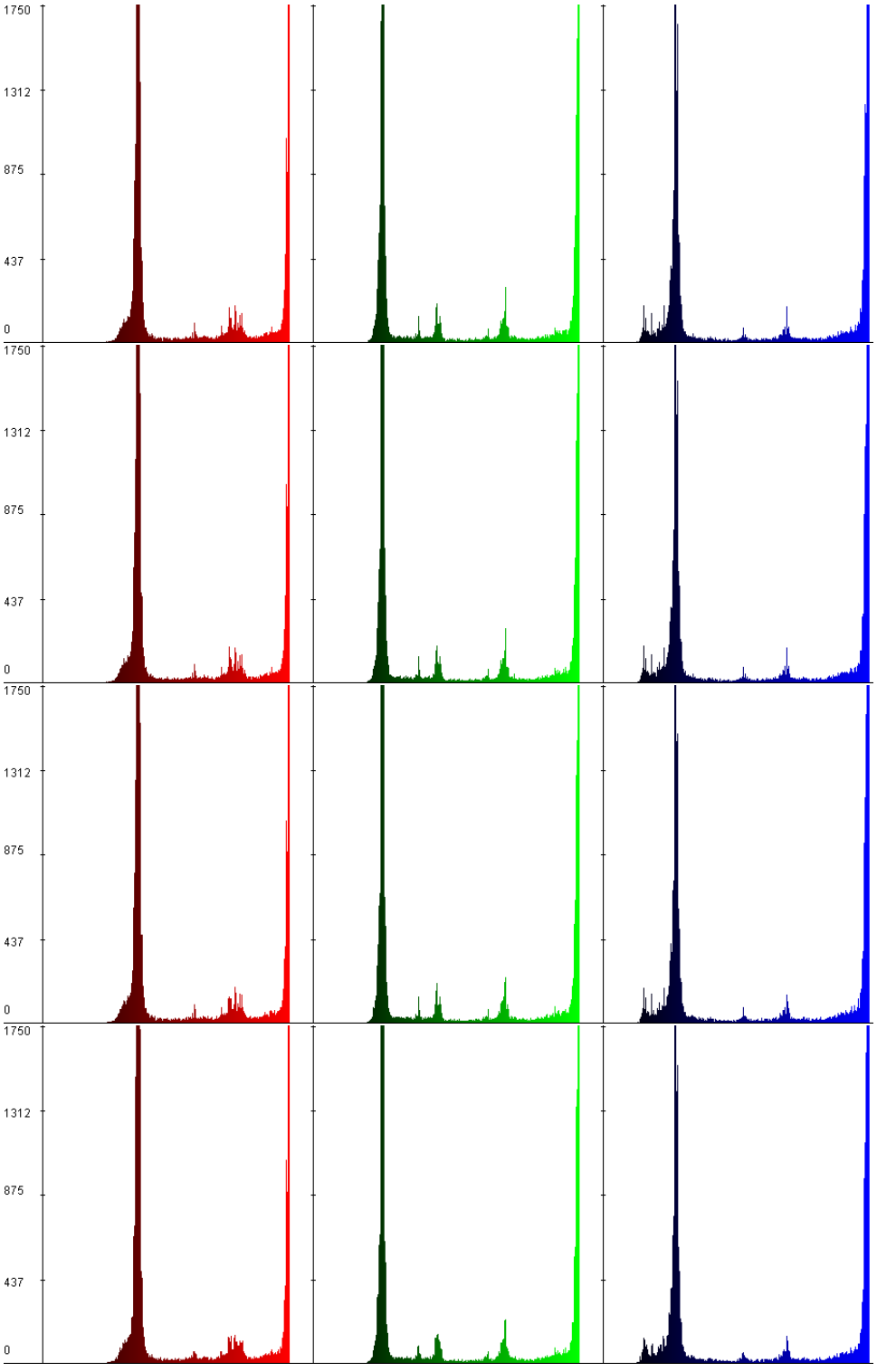

1750
1312
875
437
0
1750
1312
875
437
0
1750
1312
875
437
0
1750
1312
875
437
0

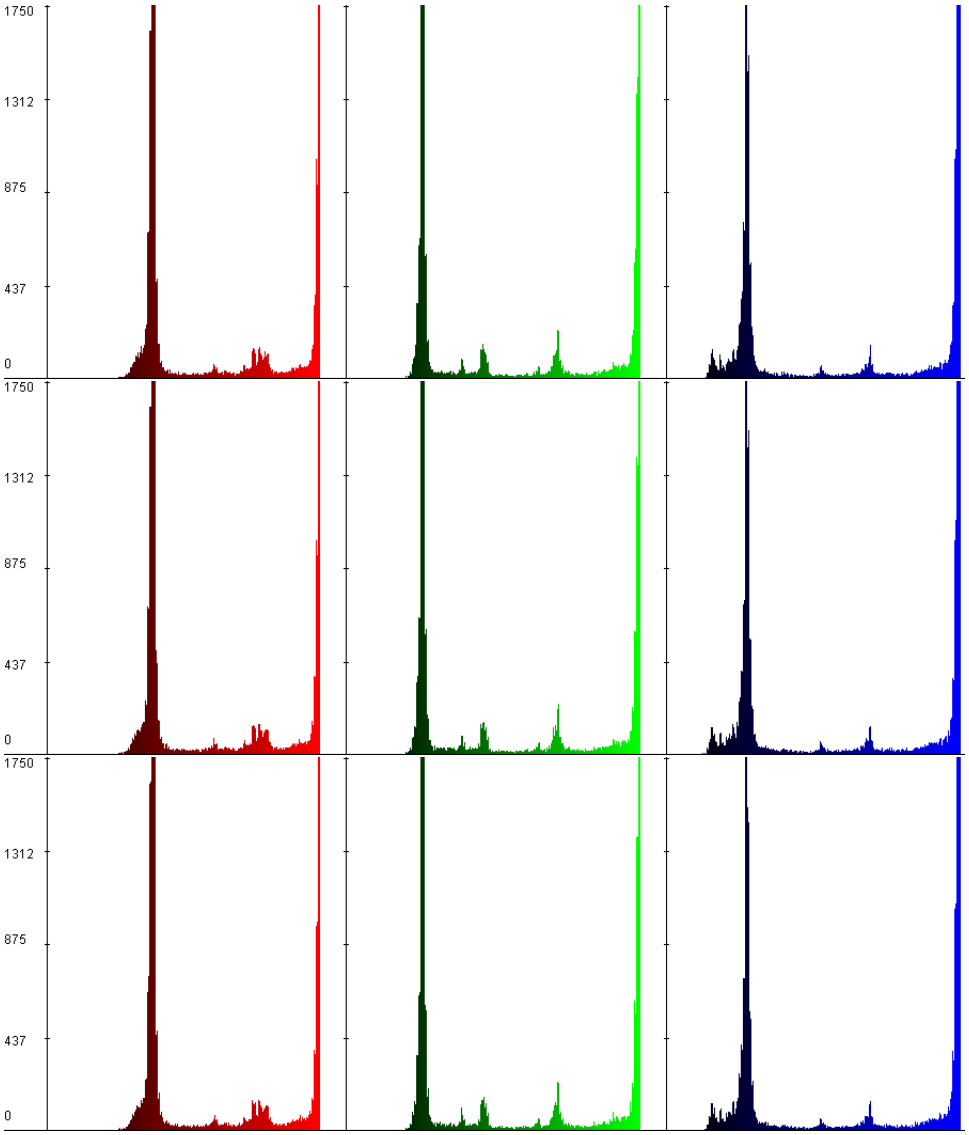

1750
1312
875
437
0
1750
1312
875
437
0
1750
1312
875
437
0
1750
1312
875
437
0



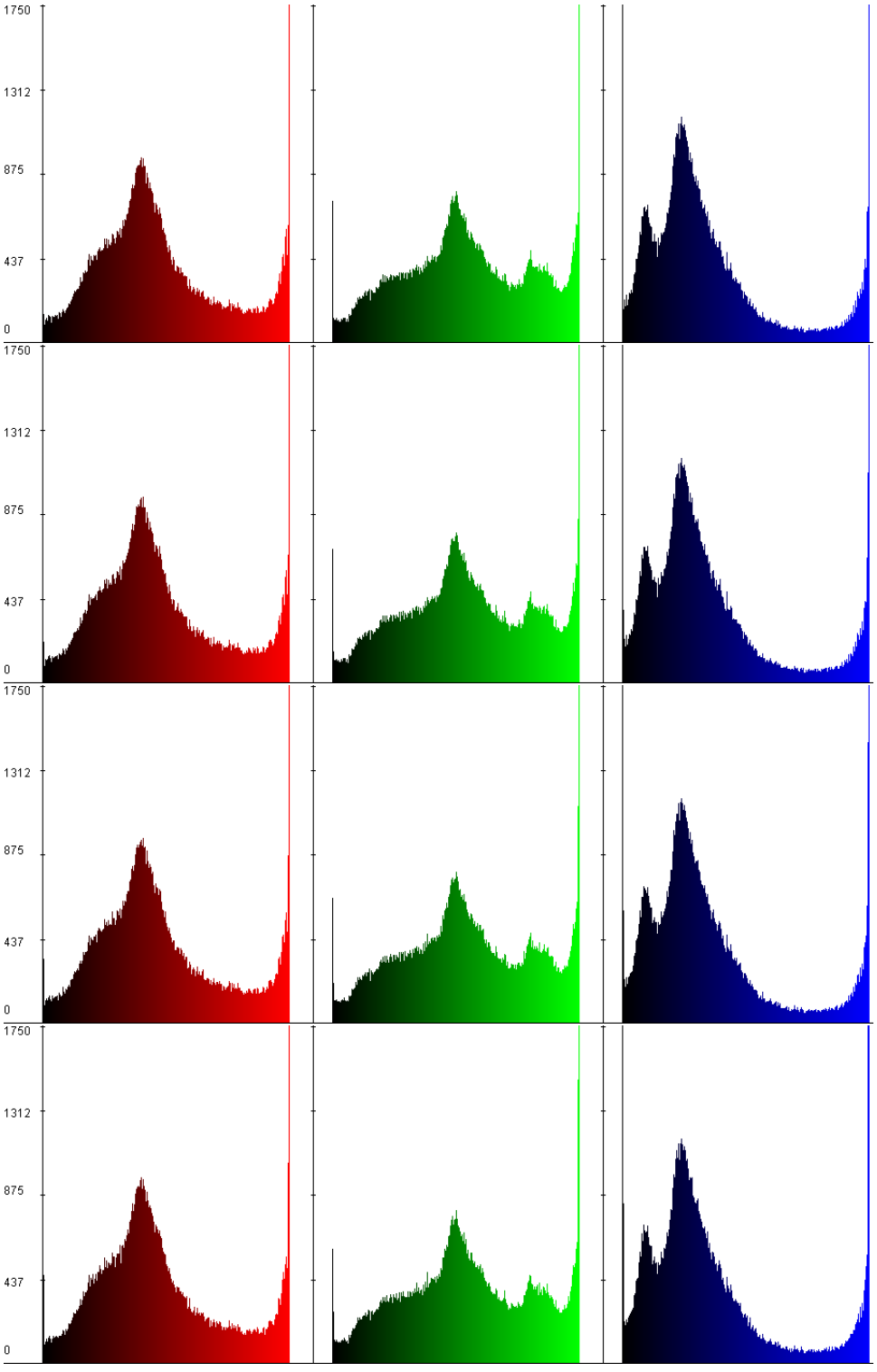
Obrázok 6.13. Histogramy hustého obrázka. Postupne: histogram originálu, histogram so zmenenými 10 percentami obrázka, ... , histogram so zmenenými 100 percentami obrázka.

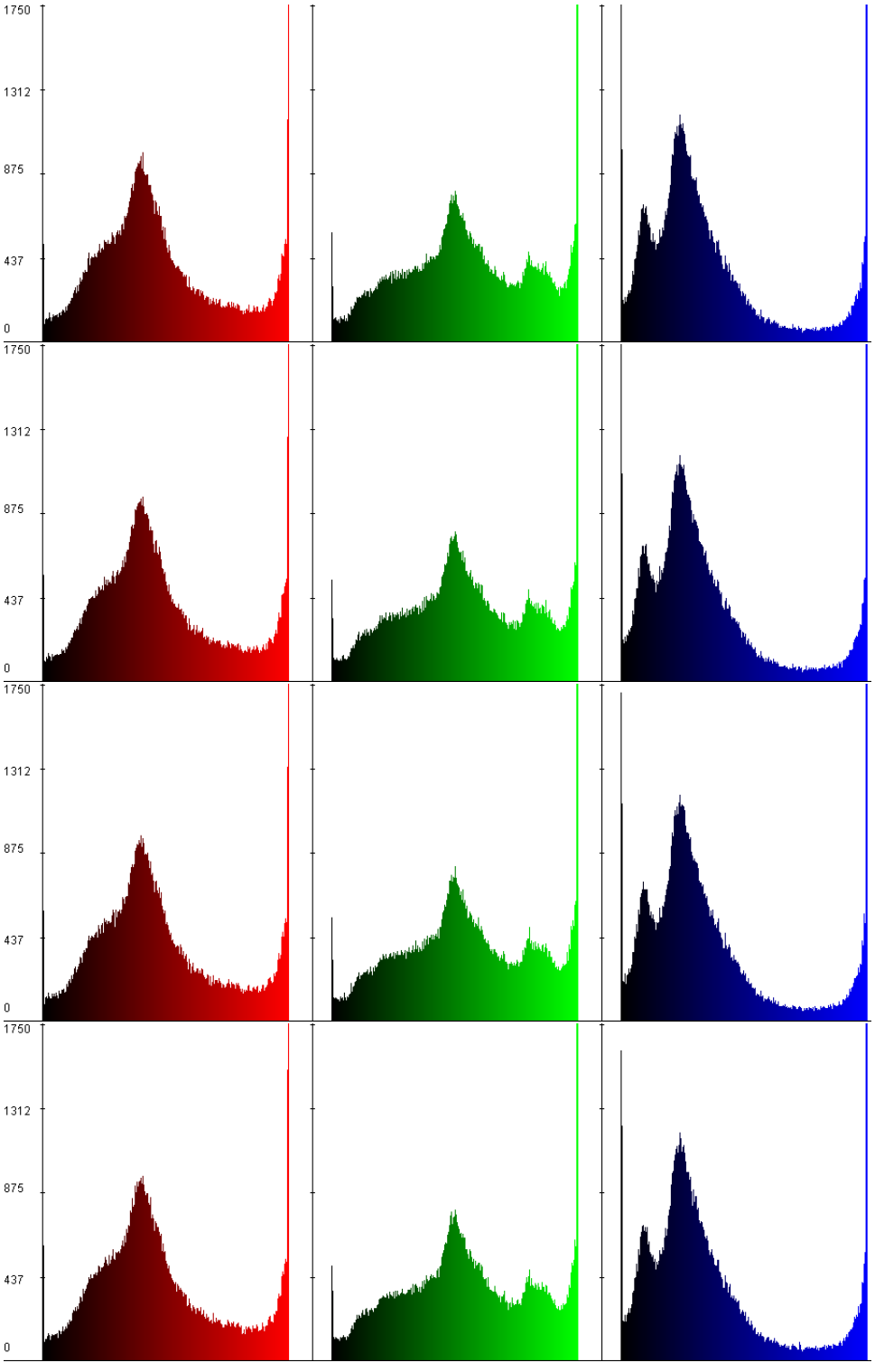

1750
1312
875
437
0
1750
1312
875
437
0
1750
1312
875
437
0
1750
1312
875
437
0

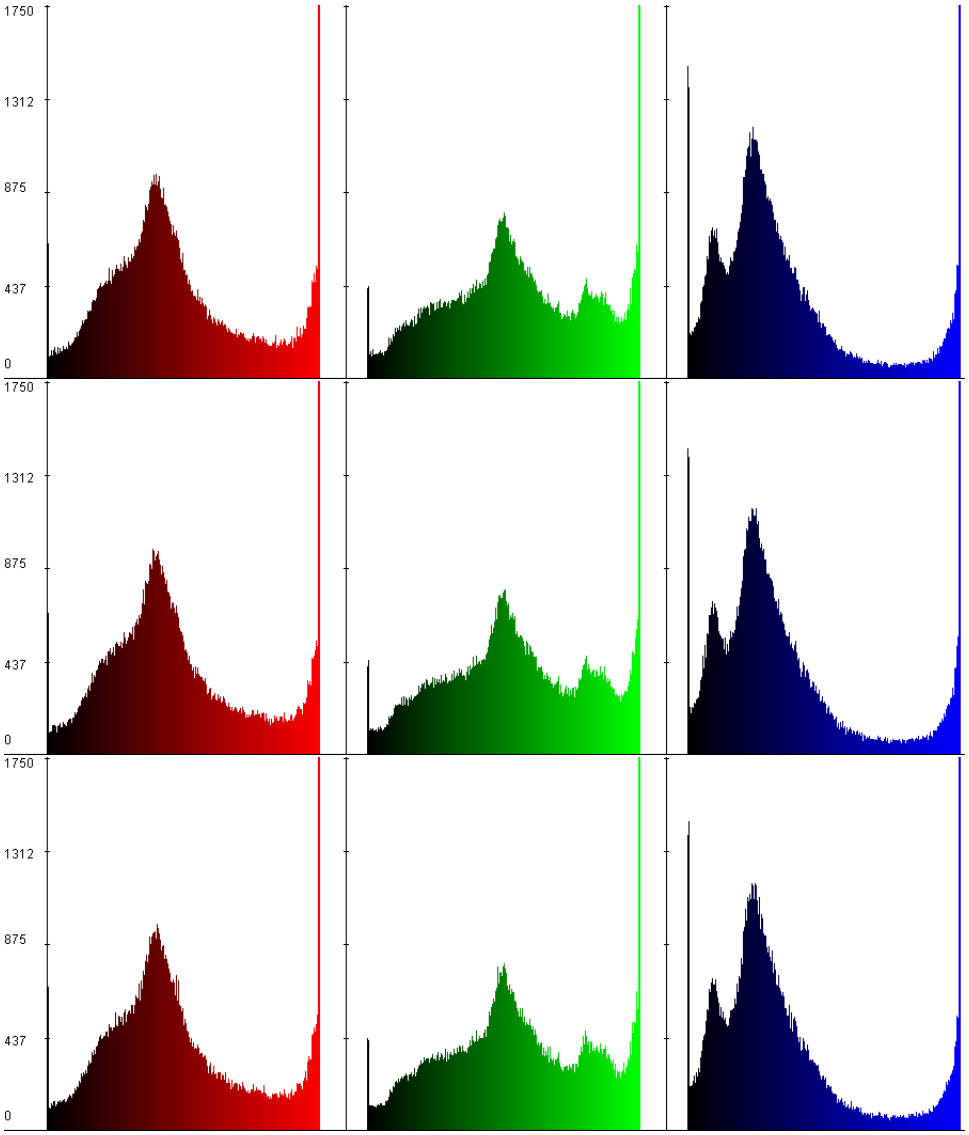

1750
1312
875
437
0
1750
1312
875
437
0
1750
1312
875
437
0
1750
1312
875
437
0



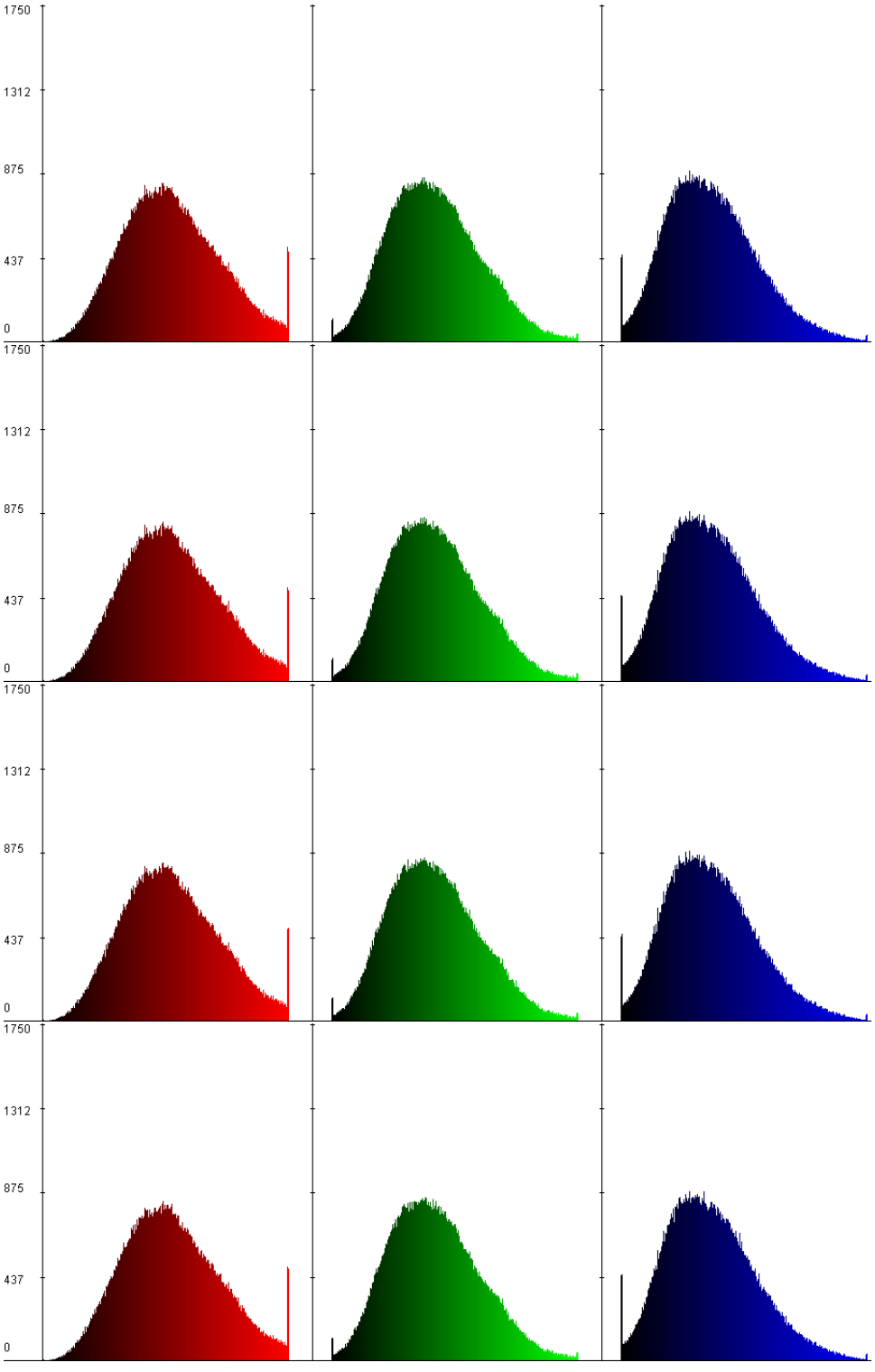
Obrázok 6.14. Histogramy hladkého obrázka. Postupne: histogram originálu, histogram so zmenenými 10 percentami obrázka, ... , histogram so zmenenými 100 percentami obrázka.

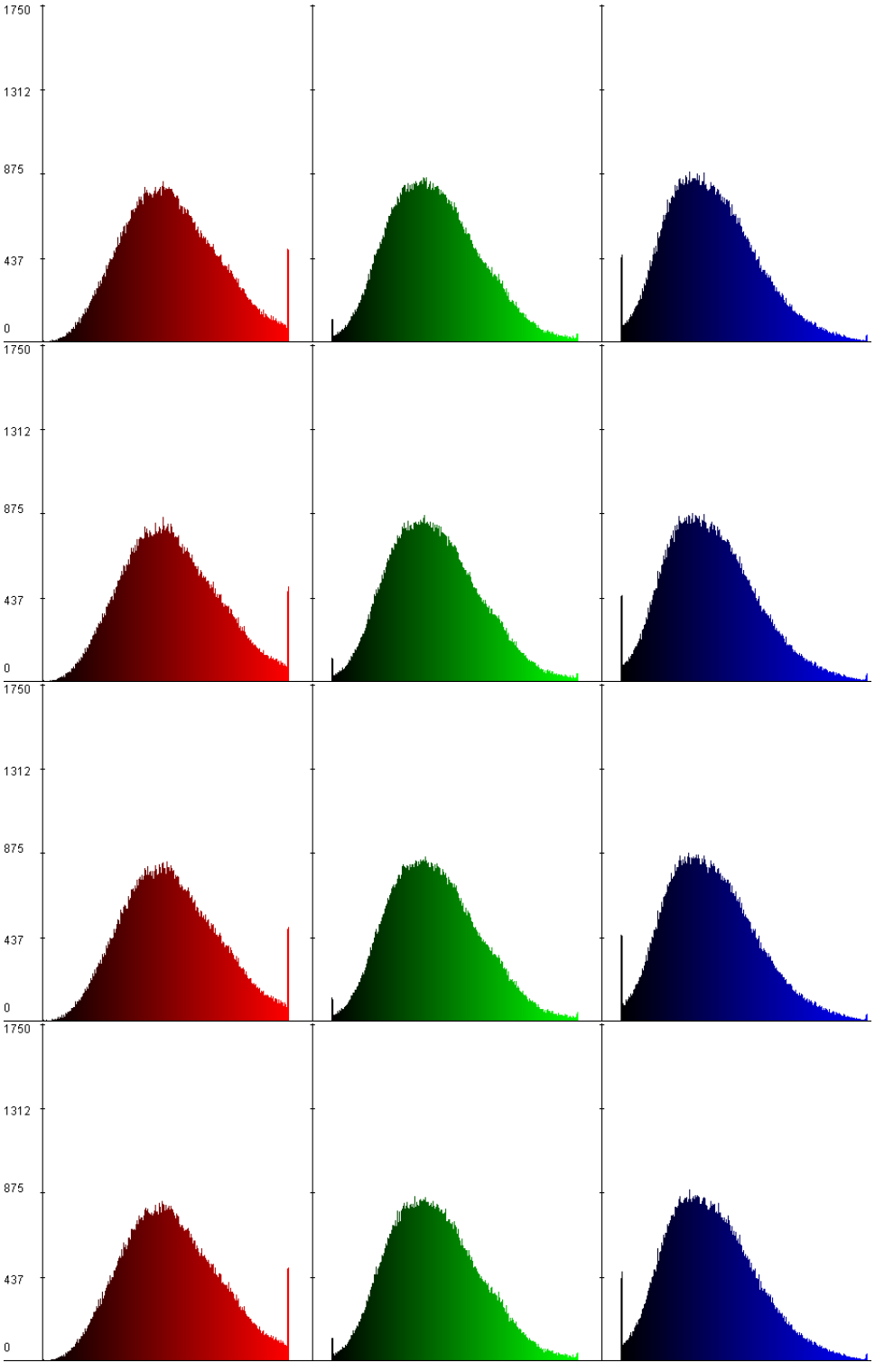

1750
1312
875
437
0
1750
1312
875
437
0
1750
1312
875
437
0
1750
1312
875
437
0

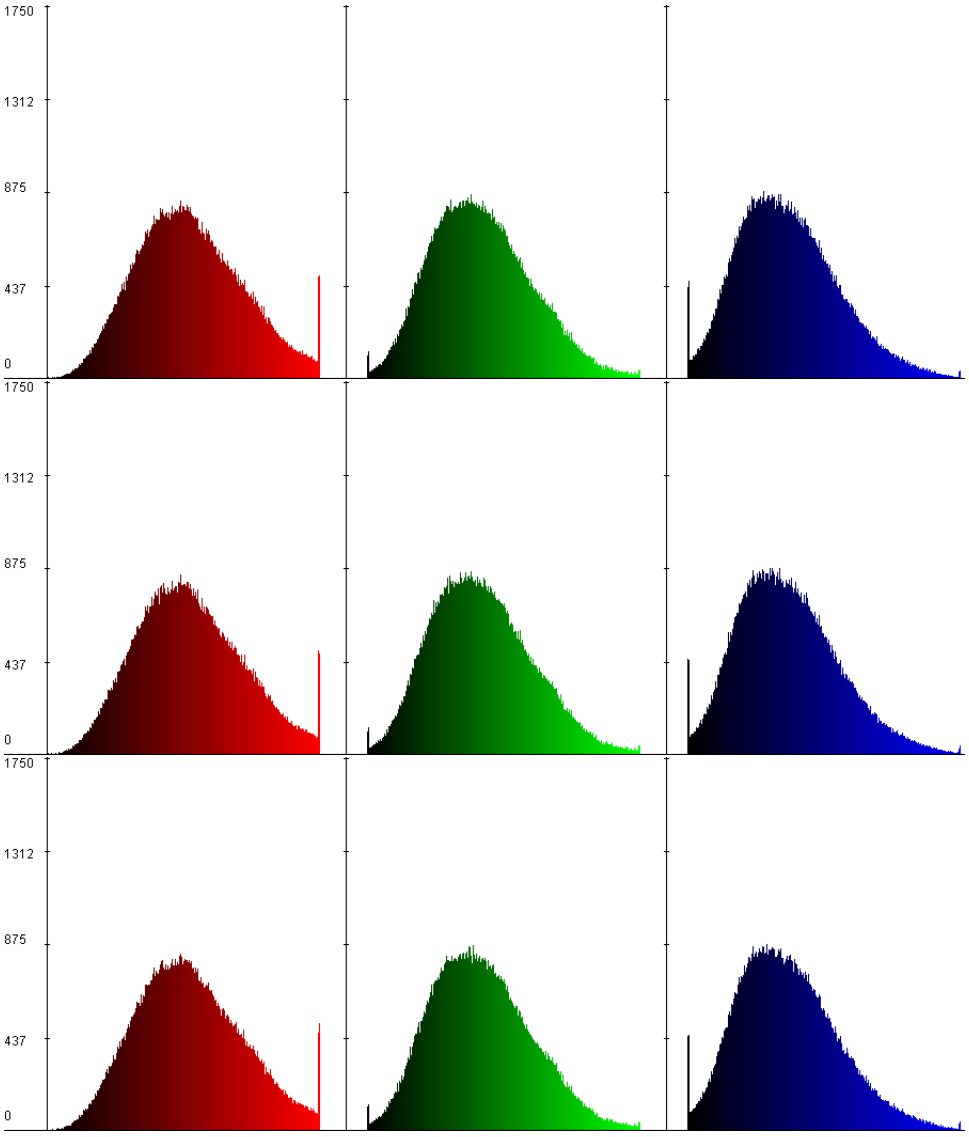

1750
1312
875
437
0
1750
1312
875
437
0
1750
1312
875
437
0
1750
1312
875
437
0



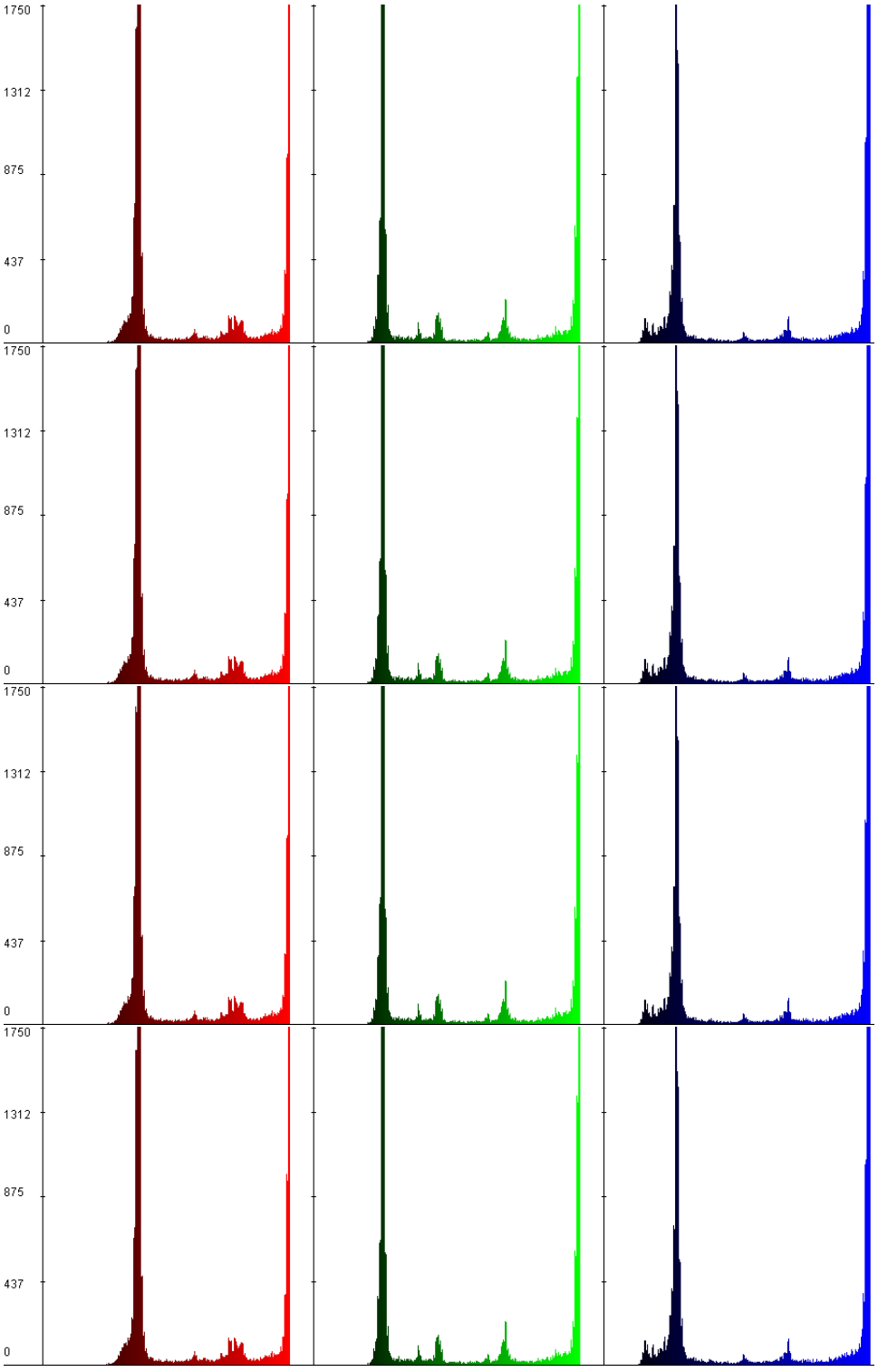
Obrázok 6.15. Histogramy náhodného obrázka. Postupne: histogram originálu, histogram so zmenenými 10 percentami obrázka, ... , histogram so zmenenými 100 percentami obrázka.

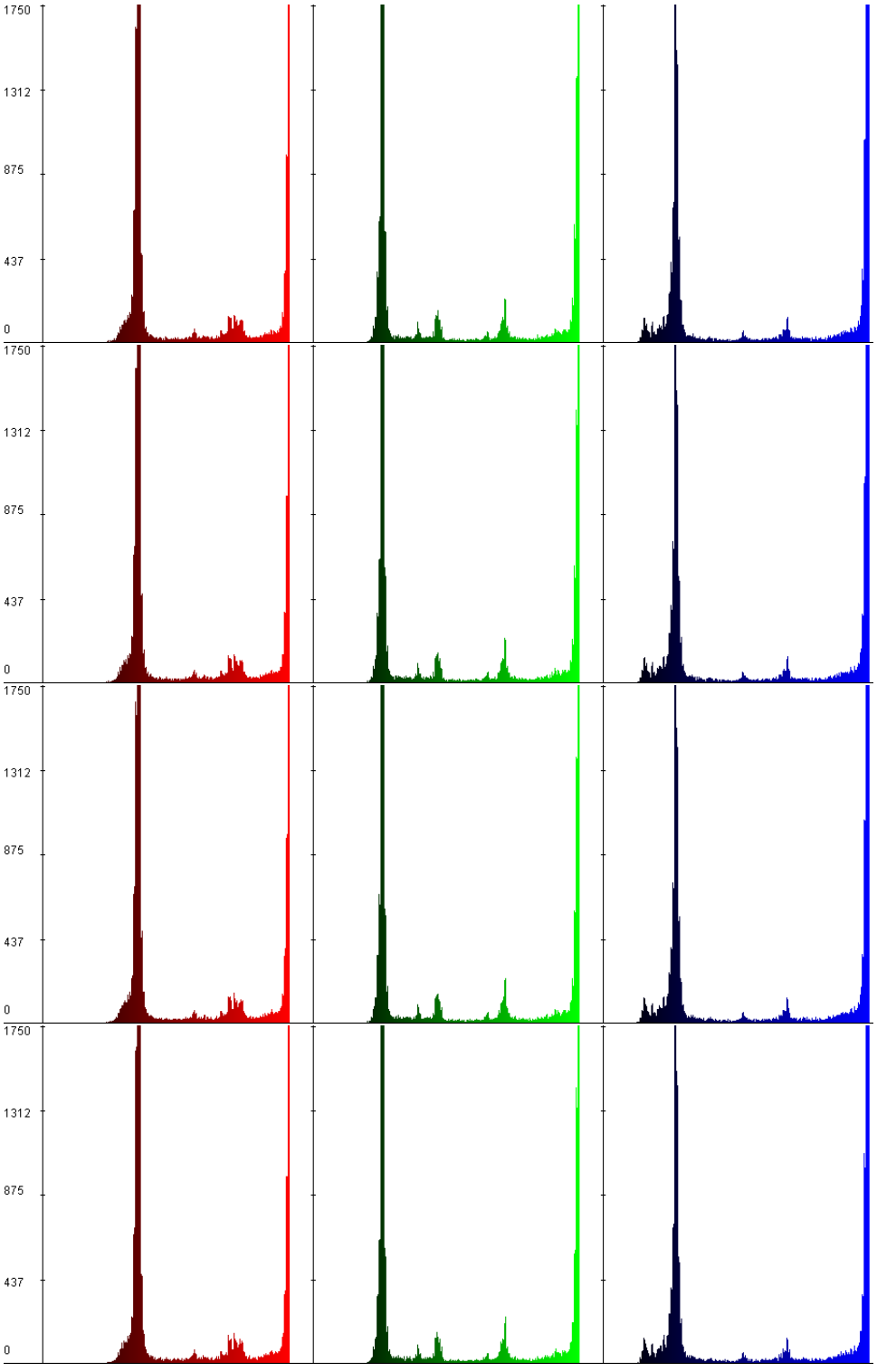

1750
1312
875
437
0
1750
1312
875
437
0
1750
1312
875
437
0
1750
1312
875
437
0

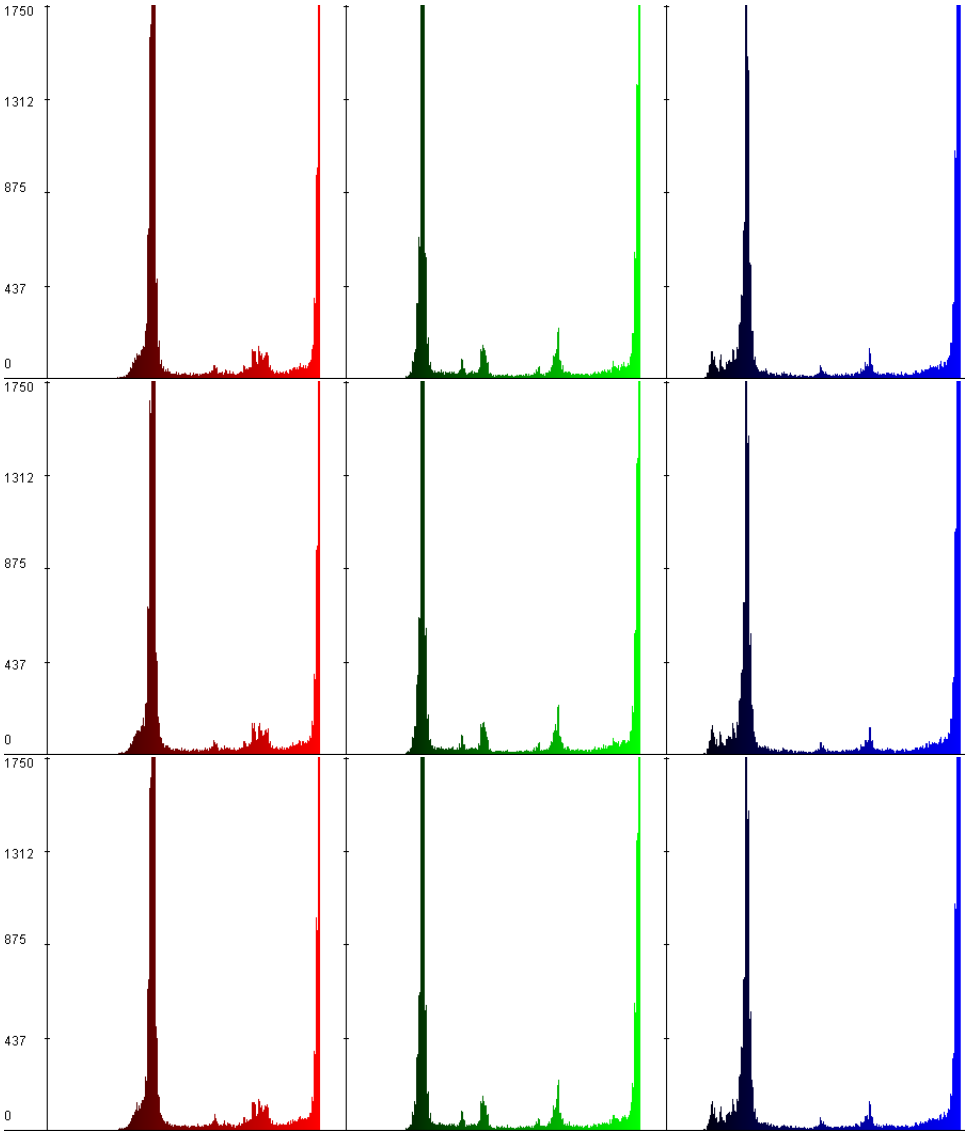

1750
1312
875
437
0
1750
1312
875
437
0
1750
1312
875
437
0
1750
1312
875
437
0



Obrázok 6.16. Histogramy hustého steganografického obrázka. Postupne: histogram originálu, histogram so zmenenými 10 percentami obrázka, ... , histogram so zmenenými 100 percentami obrázka.


1750
1312
875
437
0
1750
1312
875
437
0
1750
1312
875
437
0
1750
1312
875
437
0


1750
1312
875
437
0
1750
1312
875
437
0
1750
1312
875
437
0
1750
1312
875
437
0



Obrázok 6.17. Histogramy hladkého steganografického obrázka. Postupne: histogram originálu, histogram so zmenenými 10 percentami obrázka, ... , histogram so zmenenými 100 percentami obrázka.

TABUĽKA 6.1. Analýza hustých (dense) obrázkov so zašifrovanými prvými 10 percentami pixelov.

	Počet párov U	SP originálu P	SP 10% P'	Pomer R v originály	Pomer R' v 10%	Pomer R'/R
1	2.36747712E10	1.4215947E7	1.4388249E7	6.004681895299584E-4	6.077460634550927E-4	1.0121203321875074
2	4.049955E9	5708825.0	5618345.0	0.001409602081998442	0.0013872610930244903	0.9841508541600066
3	2.82267612E10	9.9303936E7	9.9298345E7	0.0035180775894331088	0.003517879514990193	0.999943698102762
4	3.09237252096E11	5.35230462E8	5.31003899E8	0.0017308084920953908	0.0017171407888308182	0.9921032839121179
5	7.19994E9	8.1107433E7	8.0443702E7	0.011265015125126043	0.011172829495801354	0.9918166439813229
6	3.50064477E10	1.3208192E7	1.2865435E7	3.773074067152492E-4	3.675161533170931E-4	0.9740496655409007
7	5.91764283E10	5.93637794E8	6.05386638E8	0.01003165975125268	0.010230199006451357	1.0197912668612874
8	1.001726562E11	2.2217815E7	2.1631597E7	2.2179520682411534E-4	2.1594313079620624E-4	0.973614957186384
9	1.1519976E11	1.1066040901E10	1.115374876E10	0.096059582945317	0.0968209374717529	1.0079258571140899
10	4.71857664E10	1.676681E7	1.6450182E7	3.553361803613727E-4	3.486259364857958 4E-4	0.981115787678157
11	1.03217642776E11	3.6895887E7	3.778063E7	3.5745717503034253E-4	3.6602880073506865E-4	1.0239794478988946
12	8.154858195E9	5927813.0	5893408.0	7.269057116939849E-4	7.226867542115488E-4	0.9941960044960932
13	5.39963124E9	2347225.0	2371176.0	4.347009815433248E-4	4.391366548208948E-4	1.0102039642556637
14	2.2578864E9	1425698.0	1397002.0	6.314303500831574E-4	6.187211190075816E-4	0.9798723151747424
15	6.10065057E9	817767.0	805706.0	1.3404586783274822E-4	1.3206886556690626E-4	0.9852513001869725
16	7.8267483E8	814495.0	839077.0	0.0010406556705036753	0.0010720633497310753	1.0301806640924742
17	1.029605325E10	7550511.0	7437715.0	7.333403214479295E-4	7.223850556522714E-4	0.9850611435437946
18	2.227881376E9	2456562.0	2448234.0	0.0011026448833692303	0.001098906802836885	0.9966098962696647
19	3.09237252096E11	1.38616337E8	1.3489967E8	4.4825238893588334E-4	4.3623356851625876E-4	0.9731873812247687
20	2.1892676625E10	2.7274919E7	2.644614E7	0.0012458467033151092	0.0012079902541382375	0.9696138785966698
21	2.5490900736E10	3.4423677E7	3.0963215E7	0.001350429996825672	0.0012146771634582384	0.8994743646938125
22	2.44574235136E11	8046880.0	7970449.0	3.290158505668181E-5	3.2589078712922826E-5	0.9905017845425804
23	3.6449865E10	7348126.0	7229208.0	2.0159542429032317E-4	1.9833291563631307E-4	0.9838165540438474
24	8.909456328E9	3916600.0	3910635.0	4.396003365201073 6E-4	4.389308231648139E-4	0.9984769953531124
25	2.432496375E9	3422038.0	3447855.0	0.001406800863166754	0.0014174142397231733	1.0075443346917832
26	5.50374912E10	5.832772284E9	5.890307831E9	0.10597816428086024	0.10702355253794708	1.0098641853647925
27	4.1404545E9	7283516.0	7199514.0	0.0017591102619289743	0.0017388221510464613	0.9884668338752877
28	2.3169187216E10	2.6682057E7	2.6388748E7	0.0011516181707735568	0.0011389587279857906	0.9890072568243147
29	7.982224425E9	9.7016951E7	9.7016951E7	0.012154124694383045	0.012154124694383045	1.0
30	1.336604325E10	1634262.0	1628540.0	1.2226969264071474E-4	1.2184159287379232E-4	0.9964987254185682
31	2.1725597025E10	2.057206E7	1.9156503E7	9.469042427845548E-4	8.81748058658931 1E-4	0.9311903134639895
32	7.55825256E10	4.5205407E7	4.2949107E7	5.980933640566253E-4	5.68241225852871E-4	0.9500878290953115
33	3.6449865E10	8.9155314E7	9.2949009E7	0.0024459710344606213	0.0025500508438097095	1.042551529794399
34	3.6449865E10	9238073.0	9204967.0	2.5344601413475744E-4	2.5253775288330973E-4	0.9964163521981262
35	3.4359607296E10	1538031.0	1517731.0	4.4762764217594856E-5	4.417195420556183E-5	0.9868013063455809
36	1.1519976E11	1.29398873E8	1.13768141E8	0.0011232564460203736	9.875727258459566E-4	0.8792050375894696
37	8.75157885E9	4066810.0	3812351.0	4.6469443625020873E-4	4.35618654112909E-4	0.9374303200788824
38	2.879988E10	1.6612658E7	1.6491716E7	5.768308062394704E-4	5.726314137420017E-4	0.9927198886535796
39	1.98402204E10	6847562.0	6792521.0	3.4513537964527853E-4	3.4236116651204136E-4	0.9919619566788881
40	4.25151342E10	1.65884682E8	1.63733142E8	0.003901779569121059	0.0038511731194300217	0.9870299055099011
41	1.53474324E10	1136436.0	1122944.0	7.404730448592822E-5	7.316819978304644E-5	0.9881279602194 92
42	6.1249825E10	5.934646E7	5.1546751E7	9.689245642742652E-4	8.415820126833016E-4	0.8685733066471025
43	1.9601901E10	1.41515102E8	1.40775936E8	0.007219458051543062	0.007181749157900552	0.9947767694786384
44	3.96491392E10	2.11859655E8	2.08314082E8	0.005343360770868892	0.005253937064035932	0.9832645200899622
45	2.6236876056E10	3.5749931E7	3.5267469E7	0.0013625833702036528	0.0013441946718323133	0.9865045333933651
46	1.2254655735E10	3.5248463E7	2.9804792E7	0.002876332372139053	0.0024321198934112694	0.8455628831248614
47	7.730921472E10	1.1303601E7	1.128665E7	1.462128549738812E-4	1.4599359262512505E-4	0.9985003893891867
48	4.71857664E10	2.2843543E7	2.2535393E7	4.841193593498568E-4	4.775887883003634E-4	0.986510411279021
49	4.3379703975E10	4.3740916E7	3.8770456E7	0.001008326751727217	8.937464400942814E-4	0.886365891377309
50	5.7458664E9	5312449.0	5091641.0	9.245688343884919E-4	8.861398169647662E-4	0.9584357421595954
51	9.64931374E9	1195810.0	1153801.0	1.2392694778312805E-4	1.1957337392990603E-4	0.964869837181492
52	1.03217642776E11	3.6895887E7	3.7888338E7	3.5745717503034253E-4	3.6707230451119867E-4	1.0268986892766665
53	7.19994E9	1507474.0	1464541.0	2.0937313366500276E-4	2.0341016730694977E-4	0.9715199068109963
54	2.5798447675E10	3.0446037E7	3.0674734E7	0.0011801499603212077	0.0011890147184989493	1.0075115523245273
55	4.049955E9	1212982.0	1206395.0	2.9950505622901985E-4	2.97878618404402E-4	0.9945695814117603
56	7.3668683935E10	6487311.0	6273650.0	8.806063381998165E-5	8.516033767530612E-5	0.9670647823111918
57	1.3357869525E10	861156.0	850641.0	6.446806494016867E-5	6.36808885135446E-5	0.9877896687708149
58	2.713506432E10	1372306.0	1358395.0	5.057316186232648E-5	5.006050141993083E-5	0.9898630480373911
59	7.494207731328E12	1.657591379E9	1.59487041E9	2.2118300405135275E-4	2.1281374458476392E-4	0.962161380787442
60	1.0410461685E11	6.460281E7	6.0773571E7	6.20556628080035E-4	5.837740230826276E-4	0.9407264327975828

TABUĽKA 6.2. Analýza hustých (dense) obrázkov so zašifrovanými prvými 20 percentami pixelov.

	Počet párov U	SP originálu P	SP 20% P'	Pomer R v originály	Pomer R' v 20%	Pomer R'/R
1	2.36747712E10	1.4215947E7	1.4243171E7	6.004681895299584E-4	6.016181056060217E-4	1.001915032463191
2	4.049955E9	5708825.0	5593429.0	0.001409602081998442	0.0013811089259016458	0.9797863833626008
3	2.82267612E10	9.9303936E7	9.9294691E7	0.0035180775894331088	0.003517750063368942	0.9999069019781853
4	3.09237252096E11	5.35230462E8	5.30965245E8	0.0017308084920953908	0.0017170157909538223	0.9920310645547674
5	7.19994E9	8.1107433E7	7.6876759E7	0.011265015125126043	0.010677416617360701	0.9478386401404173
6	3.50064477E10	1.3208192E7	1.2638303E7	3.773074067152492E-4	3.610278628756725E-4	0.9568533679704232
7	5.91764283E10	5.93637794E8	6.12292775E8	0.01003165975125268	0.010346903194223366	1.0314248539910178
8	1.001726562E11	2.2217815E7	2.1389139E7	2.2179520682411534E-4	2.1352272976864518E-4	0.9627021829104256
9	1.1519976E11	1.1066040901E10	1.1191231502E10	0.0960595829453117	0.0971463091763385 6	1.0113130434018807
10	4.71857664E10	1.676681E7	1.6432931E7	3.553361803613727E-4	3.482603389483147E-4	0.9800869097938129
11	1.03217642776E11	3.6895887E7	3.8518951E7	3.5745717503034253E-4	3.731818511259043E-4	1.0439903775724377
12	8.154858195E9	5927813.0	5863737.0	7.269057116939849E-4	7.19048309582531E-4	0.9891906171804001
13	5.39963124E9	2347225.0	2379174.0	4.347009815433248E-4	4.406178670823454E-4	1.0136113921758672
14	2.2578864E9	1425698.0	1370371.0	6.314303500831574E-4	6.069264600734563E-4	0.9611930436880741
15	6.10065057E9	817767.0	792177.0	1.3404586783274822E-4	1.2985123322675405E-4	0.9687074680196192
16	7.8267483E8	814495.0	831913.0	0.0010406556705036753	0.0010629101232244814	1.0213850299879066
17	1.029605325E10	7550511.0	7459299.0	7.333403214479295E-4	7.244813929065489E-4	0.9879197580137291
18	2.227881376E9	2456562.0	2426535.0	0.0011026448833692303	0.0010891670562625144	0.9877768197993781
19	3.09237252096E11	1.38616337E8	1.32518647E8	4.4825238893588334E-4	4.2853390431389795E-4	0.9560103077893337
20	2.1892676625E10	2.7274919E7	2.6001652E7	0.0012458467033151092	0.0011876872090783007	0.9533172949111233
21	2.5490900736E10	3.4423677E7	3.0806611E7	0.001350429996825672	0.0012085336379068312	0.8949250540550913
22	2.44574235136E11	8046880.0	7894552.0	3.290158505668181E-5	3.227875575532349E-5	0.9810699302089754
23	3.6449865E10	7348126.0	7142341.0	2.0159542429032317E-4	1.9594972436797777E-4	0.9719949004685003
24	8.909456328E9	3916600.0	3905775.0	4.396003365201073 6E-4	4.3838533533468375E-4	0.997236123168054
25	2.432496375E9	3422038.0	3453150.0	0.001406800863166754	0.0014195910158345045	1.0090916582457587
26	5.50374912E10	5.832772284E9	5.909560508E9	0.10597816428086024	0.10737336275967463	1.0131649617473735
27	4.1404545E9	7283516.0	7157381.0	0.0017591102619289743	0.0017286462150471645	0.9826821276976668
28	2.3169187216E10	2.6682057E7	2.5819717E7	0.0011516181707735568	0.0011143989109022184	0.9676809025630971
29	7.982224425E9	9.7016951E7	9.7016951E7	0.012154124694383045	0.012154124694383045	1.0
30	1.336604325E10	1634262.0	1619735.0	1.2226969264071474E-4	1.2118283396995591E-4	0.9911109724144599
31	2.1725597025E10	2.057206E7	1.5554505E7	9.469042427845548E-4	7.159529370862019E-4	0.7560985628080027
32	7.55825256E10	4.5205407E7	4.0627766E7	5.980933640566253E-4	5.375285580560171E-4	0.8987368701270624
33	3.6449865E10	8.9155314E7	9.399311E7	0.0024459710344606213	0.0025786956961294646	1.0542625647642272
34	3.6449865E10	9238073.0	9161163.0	2.5344601413475744E-4	2.5133599260244175E-4	0.9916746706807794
35	3.4359607296E10	1538031.0	1495064.0	4.4762764217594856E-5	4.3512255164046914E-5	0.9720636320074173
36	1.1519976E11	1.29398873E8	1.05452349E8	0.0011232564460203736	9.153868810143354E-4	0.8149402429494111
37	8.75157885E9	4066810.0	3733695.0	4.6469443625020873E-4	4.2663101869898595E-4	0.9180893624241112
38	2.879988E10	1.6612658E7	1.6320584E7	5.768308062394704E-4	5.666893056498846E-4	0.9824185870798038
39	1.98402204E10	6847562.0	6699912.0	3.4513537964527853E-4	3.3769342602665847E-4	0.9784375811420182
40	4.25151342E10	1.65884682E8	1.62721566E8	0.003901779569121059	0.003827379803966372	0.9809318379378754
41	1.53474324E10	1136436.0	1117912.0	7.404730448592822E-5	7.284032735013056E-5	0.9836999179892224
42	6.1249825E10	5.934646E7	4.911044E7	9.689245642742652E-4	8.018053929133675E-4	0.8275209675522348
43	1.9601901E10	1.41515102E8	1.38237632E8	0.007219458051543062	0.007052256411253174	0.9768401396481344
44	3.96491392E10	2.11859655E8	2.05256484E8	0.005343360770868892	0.005176820686185288	0.9688323338391162
45	2.6236876056E10	3.5749931E7	3.4821488E7	0.0013625833702036528	0.0013271964210097651	0.9740295163087168
46	1.2254655735E10	3.5248463E7	2.6347239E7	0.002876332372139053	0.002149977899807562	0.7474719961548393
47	7.730921472E10	1.1303601E7	1.1253079E7	1.462128549738812E-4	1.4555934943533727E-4	0.9955304508713638
48	4.71857664E10	2.2843543E7	2.2173183E7	4.841193593498568E-4	4.699125327759856E-4	0.9706542894856547
49	4.3379703975E10	4.3740916E7	3.8186975E7	0.001008326751727217	8.802958872657913E-4	0.873026413072831
50	5.7458664E9	5312449.0	5006117.0	9.245688343884919E-4	8.712553776050205E-4	0.9423369523170951
51	9.64931374E9	1195810.0	1083224.0	1.2392694778312805E-4	1.1225917502398466E-4	0.9058495914902869
52	1.03217642776E11	3.6895887E7	3.8673327E7	3.5745717503034253E-4	3.7467748690916876E-4	1.0481744753825812
53	7.19994E9	1507474.0	1459077.0	2.0937313366500276E-4	2.0265127209393412E-4	0.9678953003501222
54	2.5798447675E10	3.0446037E7	3.0541107E7	0.001180149960321207 7	0.0011838350657662196	1.0031225738837537
55	4.049955E9	1212982.0	1218998.0	2.9950505622901985E-4	3.009905048327697E-4	1.00495967788475
56	7.3668683935E10	6487311.0	6197345.0	8.806063381998165E-5	8.41245515593586E-5	0.9553025899328704
57	1.3357869525E10	861156.0	840044.0	6.446806494016867E-5	6.28875733834509E-5	0.9754841166989487
58	2.713506432E10	1372306.0	1343274.0	5.057316186232648E-5	4.9503254687697015E-5	0.978844368530051
59	7.494207731328E12	1.657591379E9	1.548469953E9	2.2118300405135275E-4	2.066222352667032E-4	0.9341686815083272
60	1.0410461685E11	6.460281E7	5.6562815E7	6.20556628080035E-4	5.433266718756479E-4	0.8755472865653986

TABUĽKA 6.3. Analýza hustých (dense) obrázkov so zašifrovanými prvými 30 percentami pixelov.

	Počet párov U	SP originálu P	SP 30% P'	Pomer R v originály	Pomer R' v 30%	Pomer R'/R
1	2.36747712E10	1.4215947E7	1.4210625E7	6.004681895299584E-4	6.002433932708925E-4	0.9996256316937591
2	4.049955E9	5708825.0	5559759.0	0.001409602081998442	0.001372795253280592	0.9738884971951322
3	2.82267612E10	9.9303936E7	9.9283991E7	0.003518077589433108 8	0.003517370990476938	0.9997991519691626
4	3.09237252096E11	5.35230462E8	5.24210716E8	0.001730808492095390 8	0.001695173244624800 5	0.9794112129589515
5	7.19994E9	8.1107433E7	7.356697E7	0.011265015125126043	0.010217719869887804	0.9070311718532628
6	3.50064477E10	1.3208192E7	1.2427762E7	3.773074067152492E-4	3.550135136962212E-4	0.9409131847871381
7	5.91764283E10	5.93637794E8	6.15029365E8	0.010031659751252 68	0.010393147789894579	1.0360347188406942
8	1.001726562E11	2.2217815E7	2.1263377E7	2.217952068241153 4E-4	2.122672773850235 7E-4	0.9570417703090965
9	1.1519976E11	1.1066040901E10	1.1217929654E10	0.096059582945311 7	0.097378064450828 72	1.0137256634381564
10	4.71857664E10	1.676681E7	1.6392043E7	3.553361803613727E-4	3.473938064509216E-4	0.9776482825295927
11	1.03217642776E11	3.6895887E7	3.8661447E7	3.574571750303425 3E-4	3.745623903066840 5E-4	1.0478524882732863
12	8.154858195E9	5927813.0	5869003.0	7.269057116939849E-4	7.196940596218424E-4	0.9900789717894273
13	5.39963124E9	2347225.0	2398875.0	4.347009815433248E-4	4.442664495733231E-4	1.0220047076867365
14	2.2578864E9	1425698.0	1343811.0	6.314303500831574E-4	5.951632464768821E-4	0.9425635723694639
15	6.10065057E9	817767.0	782736.0	1.340458678327 4822E-4	1.283036933551170 5E-4	0.9571626147790262
16	7.8267483E8	814495.0	833469.0	0.001040655670503 6753	0.001064898177446 1815	1.0232954161781225
17	1.029605325E10	7550511.0	7468126.0	7.333403214479295E-4	7.253387117048953E-4	0.9890888179621221
18	2.227881376E9	2456562.0	2384248.0	0.001102644883369 2303	0.001070186243165 5787	0.970562924933301
19	3.09237252096E11	1.38616337E8	1.30207941E8	4.482523889358833 4E-4	4.210616286280 35E-4	0.9393405122225961
20	2.1892676625E10	2.7274919E7	2.5996759E7	0.001245846703315 1092	0.001187463709682 4154	0.9531378993279505
21	2.5490900736E10	3.4423677E7	3.1023338E7	0.001350429996825672	0.001217035769794 7767	0.9012209241912188
22	2.44574235136E11	8046880.0	7829360.0	3.290158505668181E-5	3.201202739370076E-5	0.9729684051458454
23	3.6449865E10	7348126.0	7065515.0	2.015954242903231 7E-4	1.938420073709463 6E-4	0.9615397177457218
24	8.909456328E9	3916600.0	3889932.0	4.396003365201073 6E-4	4.36607112352636E-4	0.9931910330388602
25	2.432496375E9	3422038.0	3427094.0	0.001406808631667 54	0.001408879386305 3547	1.0014774821319927
26	5.50374912E10	5.832772284E9	5.915929695E9	0.105978162808602 4	0.107489087275111 85	1.0142569274010766
27	4.1404545E9	7283516.0	7058348.0	0.001759110261928 9743	0.001704727826377 5149	0.9690852604703553
28	2.3169187216E10	2.6682057E7	2.5360008E7	0.001151618170773 5568	0.001094557515702 8848	0.9504517586481432
29	7.982224425E9	9.7016951E7	9.7016951E7	0.012154124694383 045	0.012154124694383 045	1.0
30	1.336604325E10	1634262.0	1611714.0	1.222696926407147 4E-4	1.205827311684031 9E-4	0.986202946651149
31	2.1725597025E10	2.057206E7	1.5089641E7	9.469042427845548E-4	6.94555872625093E-4	0.733501700850571
32	7.55825256E10	4.5205407E7	4.020394E7	5.980933640566253E-4	5.319210979104937E-4	0.8893613102521121
33	3.6449865E10	8.9155314E7	9.3864517E7	0.002445971034460 6213	0.002575167754393 6033	1.0528202166390217
34	3.6449865E10	9238073.0	9121070.0	2.534460141347574 4E-4	2.502360433982403E-4	0.9873469631599 57
35	3.4359607296E10	1538031.0	1469727.0	4.476276421759485 6E-5	4.277484859878184E-5	0.9555899718536233
36	1.1519976E11	1.29398873E8	1.01823539E8	0.001123256460203 736	8.838867285834623E-4	0.7868966447644409
37	8.75157885E9	4066810.0	3717626.0	4.646944362502087 3E-4	4.247948928666 74E-4	0.9141381082470044
38	2.879988E10	1.6612658E7	1.6223407E7	5.768308062394704E-4	5.633150902017648E-4	0.9765690114128637
39	1.98402204E10	6847562.0	6496234.0	3.451353796452785 3E-4	3.274275118435680 5E-4	0.9486929800708632
40	4.25151342E10	1.65884682E8	1.61289513E8	0.003901795691210 59	0.003793696433868954	0.9722990155293543
41	1.53474324E10	1136436.0	1114956.0	7.404730448592822E-5	7.264772184303611E-5	0.981098803628185
42	6.1249825E10	5.934646E7	4.71548E7	9.689245642742652E-4	7.698764853613868E-4	0.7945680332070355
43	1.9601901E10	1.41515102E8	1.34255788E8	0.007219458051543062	0.006849120807211 5044	0.9487029023941205
44	3.96491392E10	2.11859655E8	2.02321544E8	0.005343360770868892	0.005102797893781 26	0.9549791063333883
45	2.6236876056E10	3.5749931E7	3.3567449E7	0.001362583370203 6528	0.001279399610241464	0.9389514346195521
46	1.2254655735E10	3.5248463E7	2.6248277E7	0.002876332372139053	0.002141902438355197	0.7446644411133614
47	7.730921472E10	1.1303601E7	1.1011408E7	1.462128549738812E-4	1.424333184586252 7E-4	0.9741504499318403
48	4.71857664E10	2.2843543E7	2.2022759E7	4.841193593498568E-4	4.667246222793151 7E-4	0.9640693214708419
49	4.3379703975E10	4.3740916E7	3.753833E7	0.001008326751727217	8.653431572892609E-4	0.8581971625834266
50	5.7458664E9	5312449.0	4946792.0	9.245688343884919E-4	8.609305639267909E-4	0.9311697862887719
51	9.64931374E9	1195810.0	1024524.0	1.239269477831280 5E-4	1.061758408531133 5E-4	0.856761525660431
52	1.03217642776E11	3.6895887E7	3.8618497E7	3.574571750303425 3E-4	3.741462792732902E-4	1.0466884018806757
53	7.19994E9	1507474.0	1458822.0	2.093731336650027 6E-4	2.026158551321261E-4	0.9677261432037965
54	2.5798447675E10	3.0446037E7	2.8585196E7	0.001180149960321 2077	0.001108020000277 0127	0.9388806825663385
55	4.049955E9	1212982.0	1221221.0	2.995050562290198 5E-4	3.015393998204918 5E-4	1.006792351411645
56	7.3668683935E10	6487311.0	6121507.0	8.806063381998165E-5	8.309510463633614E-5	0.9436123842374753
57	1.3357869525E10	861156.0	828937.0	6.446806494016867E-5	6.20560785122656E-5	0.9625863374347968
58	2.713506432E10	1372306.0	1329273.0	5.057316186232648E-5	4.898728023357786E-5	0.9686418335269247
59	7.494207731328E12	1.657591379E9	1.526847324E9	2.211830040513527 5E-4	2.037369897844341 2E-4	0.921124073968775
60	1.0410461685E11	6.460281E7	5.4832456E7	6.20556628080035E-4	5.267053245006972E-4	0.8487627086190214

Tabuľka 6.4. Analýza hustých (dense) obrázkov so zašifrovanými prvými 40 percentami pixelov.

	Počet párov U	SP originálu P	SP 40% P'	Pomer R v originály	Pomer R' v 40%	Pomer R'/R
1	2.36747712E10	1.4215947E7	1.4223633E7	6.004681895299584E-4	6.007928389187558E-4	1.0005406604287423
2	4.049955E9	5708825.0	5231632.0	0.001409602081998442	0.0012917753407136621	0.9164113455921314
3	2.82267612E10	9.9303936E7	9.9277707E7	0.0035180775894331088	0.003517148364864475	0.999735871496574
4	3.09237252096E11	5.35230462E8	5.13641289E8	0.0017308084920953908	0.0016609942221338344	0.9596637812441997
5	7.19994E9	8.1107433E7	7.2626624E7	0.011265015125126043	0.010087115170404198	0.8954373392633448
6	3.50064477E10	1.3208192E7	1.2360849E7	3.773074067152492E-4	3.5310206582314836E-4	0.9358471621248389
7	5.91764283E10	5.93637794E8	6.14933992E8	0.01003165975125268	0.010391536117768703	1.0358740602691479
8	1.001726562E11	2.2217815E7	2.0948369E7	2.2179520682411534E-4	2.091226268191938E-4	0.9428635984231573
9	1.1519976E11	1.1066040901E10	1.1257602238E10	0.0960595829453117	0.0977224452773313	1.0173107382047257
10	4.71857664E10	1.676681E7	1.6345221E7	3.553361803613727E-4	3.4640151569096907E-4	0.9748557417898814
11	1.03217642776E11	3.6895887E7	3.8591018E7	3.5745717503034253E-4	3.7388005540631397E-4	1.0459436305190333
12	8.154858195E9	5927813.0	5810783.0	7.269057116939849E-4	7.125547570603709E-4	0.9802574743838915
13	5.39963124E9	2347225.0	2428465.0	4.347009815433248E-4	4.497464534263269E-4	1.0346110833004931
14	2.2578864E9	1425698.0	1307745.0	6.314303500831574E-4	5.791899007850883E-4	0.9172664898176192
15	6.10065057E9	817767.0	773677.0	1.3404586783274822E-4	1.268187697562229E-4	0.946084887260063
16	7.8267483E8	814495.0	829759.0	0.0010406556705036753	0.0010601580224574234	1.0187404465343555
17	1.029605325E10	7550511.0	7364701.0	7.333403214479295E-4	7.152936004871576E-4	0.9753910695580738
18	2.227881376E9	2456562.0	2333080.0	0.0011026448833692303	0.0010472191316527259	0.9497338149820765
19	3.09237252096E11	1.38616337E8	1.28518774E8	4.4825238893588334E-4	4.1559926279548774E-4	0.9271545965032967
20	2.1892676625E10	2.7274919E7	2.6050354E7	0.0012458467033151092	0.0011899117885956533	0.9551028914146362
21	2.5490900736E10	3.4423677E7	3.1618379E7	0.001350429996825672	0.0012403790406412102	0.9185067301206667
22	2.44574235136E11	8046880.0	7785862.0	3.290158505668181E-5	3.183435080833649E-5	0.9675628318056191
23	3.6449865E10	7348126.0	6997443.0	2.0159542429032317E-4	1.919744558724703E-4	0.9522758591782449
24	8.909456328E9	3916600.0	3881228.0	4.396003365201073 6E-4	4.3563017283134944E-4	0.9909686973395292
25	2.432496375E9	3422038.0	3406468.0	0.001406800863166754	0.0014004000314286182	0.9954500797477993
26	5.50374912E10	5.832772284E9	5.923175295E9	0.10597816428086024	0.10762073571769201	1.0154991497350216
27	4.1404545E9	7283516.0	6958389.0	0.0017591102619289743	0.0016805857907628257	0.9553612568435355
28	2.3169187216E10	2.6682057E7	2.4856402E7	0.0011516181707735568	0.0010728214921080553	0.931577426732879
29	7.982224425E9	9.7016951E7	9.7016951E7	0.012154124694383045	0.012154124694383045	1.0
30	1.336604325E10	1634262.0	1606748.0	1.2226969264071474E-4	1.2021119264296859E-4	0.9831642661947717
31	2.1725597025E10	2.057206E7	1.4907636E7	9.469042427845548E-4	6.861784273567046E-4	0.7246545071324894
32	7.55825256E10	4.5205407E7	3.959906E7	5.980933640566253E-4	5.239181898944112E-4	0.87598061001862
33	3.6449865E10	8.9155314E7	9.3685407E7	0.0024459710344606213	0.0025702538815987382	1.05081125057784
34	3.6449865E10	9238073.0	9210488.0	2.5344601413475744E-4	2.5268922120836386E-4	0.9970139876573826
35	3.4359607296E10	1538031.0	1434724.0	4.4762764217594856E-5	4.175612333517632E-5	0.9328316529380748
36	1.1519976E11	1.29398873E8	9.9858473E7	0.0011232564460203736	8.668288284628371E-4	0.7717105310492156
37	8.75157885E9	4066810.0	3711075.0	4.6469443625020873E-4	4.240463422208668E-4	0.9125272633833397
38	2.879988E10	1.6612658E7	1.6022982E7	5.768308062394704E-4	5.563558598160826E-4	0.9645044158496492
39	1.98402204E10	6847562.0	6454532.0	3.4513537964527853E-4	3.253256198706341E-4	0.9426029293345574
40	4.25151342E10	1.65884682E8	1.59900297E8	0.003901779569121059	0.003761020634388589	0.9639244267291659
41	1.53474324E10	1136436.0	1109660.0	7.404730448592822E-5	7.230264783573831E-5	0.9764386203886537
42	6.1249825E10	5.934646E7	4.6438194E7	9.689245642742652E-4	7.581767621376878E-4	0.7824930754083732
43	1.9601901E10	1.41515102E8	1.31699121E8	0.007219458051543062	0.006718691263668764	0.930636512561041
44	3.96491392E10	2.11859655E8	1.99221471E8	0.005343360770868892	0.005024610244249641	0.940346433585951
45	2.6236876056E10	3.5749931E7	3.221976E7	0.0013625833702036528	0.001228033395867333	0.9012537674548238
46	1.2254655735E10	3.5248463E7	2.614201E7	0.002876332372139053	0.0021332308769259766	0.741649642992944
47	7.730921472E10	1.1303601E7	1.0897335E7	1.462128549738812E-4	1.409577763720428E-4	0.9640587101402464
48	4.71857664E10	2.2843543E7	2.1893466E7	4.841193593498568E-4	4.639845375066325E-4	0.9584093850940723
49	4.3379703975E10	4.3740916E7	3.6868908E7	0.001008326751727217	8.499114706095686E-4	0.8428929106102854
50	5.7458664E9	5312449.0	4852807.0	9.245688343884919E-4	8.445735877186424E-4	0.9134783223330708
51	9.64931374E9	1195810.0	1014359.0	1.2392694778312805E-4	1.051223980618543E-4	0.8482610113646817
52	1.03217642776E11	3.6895887E7	3.8516581E7	3.5745717503034253E-4	3.7315888993500455E-4	1.043926142770331
53	7.19994E9	1507474.0	1451625.0	2.0937313366500276E-4	2.0161626346886224E-4	0.9629519315092665
54	2.5798447675E10	3.0446037E7	2.7261347E7	0.0011801499603212077	0.0010567049360267371	0.8953988658688157
55	4.049955E9	1212982.0	1223390.0	2.9950505622901985E-4	3.0207496132673 08E-4	1.0085805065532711
56	7.3668683935E10	6487311.0	6083601.0	8.806063381998165E-5	8.258055764058085E-5	0.937769285301722
57	1.3357869525E10	861156.0	819659.0	6.446806494016867E-5	6.136150667334805E-5	0.951812447454352
58	2.713506432E10	1372306.0	1317127.0	5.057316186232648E-5	4.8539667511648634E-5	0.9597910378589032
59	7.494207731328E12	1.657591379E9	1.516273132E9	2.2118300405135275E-4	2.0232600781287804E-4	0.9147448226442543
60	1.0410461685E11	6.460281E7	5.3359032E7	6.20556628080035E-4	5.125520232871401E-4	0.8259552796542442

Tabuľka 6.5. Analýza hustých (dense) obrázkov so zašifrovanými prvými 50 percentami pixelov.

	Počet párov U	SP originálu P	SP 50% P'	Pomer R v originály	Pomer R' v 50%	Pomer R'/R
1	2.36747712E10	1.4215947E7	1.4270602E7	6.004681895299584E-4	6.027767651667949E-4	1.0038446260386311
2	4.049955E9	5708825.0	4766980.0	0.001409602081998442	0.001177045177045177	0.8350194654766961
3	2.82267612E10	9.9303936E7	9.9267524E7	0.0035180775894331088	0.0035167876079243553	0.9996333277263049
4	3.09237252096E11	5.35230462E8	4.97437846E8	0.0017308084920953908	0.001608596126852061	0.9293900129324104
5	7.19994E9	8.1107433E7	7.0990717E7	0.011265015125126043	0.009859903971421984	0.875267708201294
6	3.50064477E10	1.3208192E7	1.2091725E7	3.773074067152492E-4	3.4541422493433976E-4	0.915471625488182
7	5.91764283E10	5.93637794E8	6.14927089E8	0.01003165975125268	0.010391419466591903	1.0358624319663852
8	1.001726562E11	2.2217815E7	2.0748947E7	2.2179520682411534E-4	2.071318440291094E-4	0.9338878283035482
9	1.1519976E11	1.1066040901E10	1.1277621648E10	0.0960595829453117	0.09789622520046917	1.019119823330933
10	4.71857664E10	1.676681E7	1.6318676E7	3.553361803613727E-4	3.458389519768402E-4	0.9732725545288579
11	1.03217642776E11	3.6895887E7	3.8595057E7	3.5745717503034253E-4	3.739191863135055E-4	1.046053100715535
12	8.154858195E9	5927813.0	5742233.0	7.269057116939849E-4	7.041487249307099E-4	0.9686933444088065
13	5.39963124E9	2347225.0	2454987.0	4.347009815433248E-4	4.546582703303272E-4	1.0459103835380077
14	2.2578864E9	1425698.0	1281170.0	6.314303500831574E-4	5.674200438073412E-4	0.898626497336743
15	6.10065057E9	817767.0	765688.0	1.3404586783274822E-4	1.255092372877865E-4	0.9363156008985444
16	7.8267483E8	814495.0	829045.0	0.0010406556705036753	0.001059245766214304	1.0178638297349891
17	1.029605325E10	7550511.0	7351463.0	7.333403214479295E-4	7.140078651011251E-4	0.9736378107389024
18	2.227881376E9	2456562.0	2262990.0	0.0011026448833692303	0.00101575874926655	0.9212020702103183
19	3.09237252096E11	1.38616337E8	1.27008666E8	4.4825238893588334E-4	4.107159313411932E-4	0.9162604404991599
20	2.1892676625E10	2.7274919E7	2.6019797E7	0.0012458467033151092	0.001188516025047713 8	0.9539825581150213
21	2.5490900736E10	3.4423677E7	3.2305891E7	0.001350429996825672	0.0012673499196666441	0.938478797602011
22	2.44574235136E11	8046880.0	7737853.0	3.290158505668181E-5	3.1638054579613525E-5	0.9615966685224583
23	3.6449865E10	7348126.0	6906593.0	2.0159542429032317E-4	1.894819912227384E-4	0.939912162638474
24	8.909456328E9	3916600.0	3865733.0	4.396003365201073 6E-4	4.3389100947170613E-4	0.9870124597865496
25	2.432496375E9	3422038.0	3425335.0	0.001406800863166754	0.0014081562608700702	1.0009634609551383
26	5.50374912E10	5.832772284E9	5.929583077E9	0.10597816428086024	0.10773716148238967	1.016597732310854
27	4.1404545E9	7283516.0	6953173.0	0.0017591102619289743	0.00167932602568148	0.9546451191979257
28	2.3169187216E10	2.6682057E7	2.4367536E7	0.0011516181707735568	0.0010517216582881445	0.9132555259888696
29	7.982224425E9	9.7016951E7	9.7016951E7	0.012154124694383045	0.012154124694383045	1.0
30	1.336604325E10	1634262.0	1604054.0	1.2226969264071474E-4	1.2000963710782546E-4	0.9815158157015216
31	2.1725597025E10	2.057206E7	1.4815102E7	9.469042427845548E-4	6.819192118380922E-4	0.7201564646418492
32	7.55825256E10	4.5205407E7	3.9422192E7	5.980933640566253E-4	5.215781251956471E-4	0.8720680692024297
33	3.6449865E10	8.9155314E7	9.3895588E7	0.0024459710344606213	0.0025760201855342 95	1.0531687208235283
34	3.6449865E10	9238073.0	9164604.0	2.5344601413475744E-4	2.5143039624426594E-4	0.9920471509588634
35	3.4359607296E10	1538031.0	1418435.0	4.4762764217594856E-5	4.12820492324174E-5	0.9222408390988219
36	1.1519976E11	1.29398873E8	9.9639182E7	0.0011232564460203736	8.649252567887294E-4	0.7700158408643946
37	8.75157885E9	4066810.0	3684377.0	4.6469443625020873E-4	4.2099569268006995E-4	0.9059624128002046
38	2.879988E10	1.6612658E7	1.5263681E7	5.768308062394704E-4	5.299911319074941E-4	0.9187982440859254
39	1.98402204E10	6847562.0	6424180.0	3.4513537964527853E-4	3.237957981555487E-4	0.9381704028382656
40	4.25151342E10	1.65884682E8	1.59160906E8	0.003901779569121059	0.003743629392095392	0.959467167679774
41	1.53474324E10	1136436.0	1101583.0	7.404730448592822E-5	7.177637088012194E-5	0.9693313129819893
42	6.1249825E10	5.934646E7	4.6065048E7	9.689245642742652E-4	7.520845651395739E-4	0.7762054889204849
43	1.9601901E10	1.41515102E8	1.28950216E8	0.007219458051543062	0.006578454610091134	0.9112116952719294
44	3.96491392E10	2.11859655E8	1.95704171E8	0.005343360770868892	0.004935899617210353	0.9237444052290181
45	2.6236876056E10	3.5749931E7	3.1667625E7	0.0013625833702036528	0.0012069891603104198	0.8858094019817827
46	1.2254655735E10	3.5248463E7	2.5857705E7	0.002876332372139053	0.00211003112279596	0.7335839012327998
47	7.730921472E10	1.1303601E7	1.0684685E7	1.462128549738812E-4	1.3820713402274229E-4	0.9452461211254715
48	4.71857664E10	2.2843543E7	2.1728769E7	4.841193593498568E-4	4.6049414172490795E-4	0.9511996015679354
49	4.3379703975E10	4.3740916E7	3.6387282E7	0.001008326751727217	8.388089052191371E-4	0.8318820300882588
50	5.7458664E9	5312449.0	4778668.0	9.245688343884919E-4	8.31670572790677E-4	0.8995226118876624
51	9.64931374E9	1195810.0	971648.0	1.2392694778312805E-4	1.0069607292093292E-4	0.8125437987640176
52	1.03217642776E11	3.6895887E7	3.8612193E7	3.5745717503034253E-4	3.7408520444315015E-4	1.04651754272773
53	7.19994E9	1507474.0	1445956.0	2.0937313366500276E-4	2.0082889579635385E-4	0.9591913359699736
54	2.5798447675E10	3.0446037E7	2.6695004E7	0.001180149960321207 7	0.0010347523361209368	0.8767973316198754
55	4.049955E9	1212982.0	1219476.0	2.9950505622901985E-4	3.011085308355278E-4	1.0053537480358323
56	7.3668683935E10	6487311.0	6067924.0	8.806063381998165E-5	8.236775351320113E-5	0.9353527216438366
57	1.3357869525E10	861156.0	815036.0	6.446806494016867E-5	6.101541854968822E-5	0.9464440821407503
58	2.713506432E10	1372306.0	1309026.0	5.057316186232648E-5	4.8241123903847815E-5	0.9538878355119048
59	7.494207731328E12	1.657591379E9	1.504428195E9	2.2118300405135275E-4	2.0074546222024866E-4	0.9075989499339692
60	1.0410461685E11	6.460281E7	5.0849991E7	6.20556628080035E-4	4.884508731564483E-4	0.787117325082299

TABUĽKA 6.6. Analýza hustých (dense) obrázkov so zašifrovanými prvými 60 percentami pixelov.

	Počet párov U	SP originálu P	SP 60% P'	Pomer R v originály	Pomer R' v 60%	Pomer R'/R
1	2.36747712E10	1.4215947E7	1.4308287E7	6.004681895299584E-4	6.043685440136376E-4	1.0064955222469527
2	4.049955E9	5708825.0	4439086.0	0.001409602081998442	0.001096082795981683 7	0.777583127876577
3	2.82267612E10	9.9303936E7	9.9246225E7	0.003518077589433108 8	0.003516033040305028	0.9994188447877836
4	3.09237252096E11	5.35230462E8	4.81993683E8	0.001730808492095390 8	0.001558653363180091	0.9005348484817742
5	7.19994E9	8.1107433E7	6.8658537E7	0.011265015125126043	0.009535987383228193	0.8465135001868447
6	3.50064477E10	1.3208192E7	1.1808931E7	3.773074067152492E-4	3.373358845547759E-4	0.8940611250956982
7	5.91764283E10	5.93637794E8	6.15749946E8	0.01003165975125268	0.010405324614699667	1.0372485583355562
8	1.001726562E11	2.2217815E7	2.041942E7	2.2179520682411534E-4	2.0384225371074865E-4	0.9190561718152752
9	1.1519976E11	1.1066040901E10	1.1296890991E10	0.0960595829453117	0.098063494151376 7	1.020861127485905
10	4.71857664E10	1.676681E7	1.631675E7	3.553361803613727E-4	3.457981345832289E-4	0.9731576847354984
11	1.03217642776E11	3.6895887E7	3.8613889E7	3.5745717503034253E-4	3.7410163574262944E-4	1.0465635099110098
12	8.154858195E9	5927813.0	5701584.0	7.269057116939849E-4	6.991640888980535E-4	0.9618360093343025
13	5.39963124E9	2347225.0	2461265.0	4.347009815433248E-4	4.5582094232049817E-4	1.048585031260318
14	2.2578864E9	1425698.0	1262810.0	6.314303500831574E-4	5.592885452518781E-4	0.8857485947234267
15	6.10065057E9	817767.0	759290.0	1.3404586783274822E-4	1.2446049667781578E-4	0.9284918564823474
16	7.8267483E8	814495.0	809915.0	0.0010406556705036753	0.0010348039427817042	0.9943768838359965
17	1.029605325E10	7550511.0	7435419.0	7.333403214479295E-4	7.221620575825985E-4	0.9847570581646726
18	2.227881376E9	2456562.0	2213218.0	0.0011026448833692303	9.93418242031213E-4	0.9009412341312777
19	3.09237252096E11	1.38616337E8	1.25358948E8	4.4825238893588334E-4	4.053811342272677E-4	0.9043591160542642
20	2.1892676625E10	2.7274919E7	2.6002901E7	0.0012458467033151092	0.0011877442601196783	0.953363087897713
21	2.5490900736E10	3.4423677E7	3.2920812E7	0.0013504299968256 72	0.0012914730766460116	0.956342113017154
22	2.44574235136E11	8046880.0	7683609.0	3.290158505668181E-5	3.141626506867082E-5	0.954855670769292
23	3.6449865E10	7348126.0	6850903.0	2.0159542429032317E-4	1.879541391991438E-4	0.9323333595531703
24	8.909456328E9	3916600.0	3869833.0	4.396003365201073 6E-4	4.343511946781945E-4	0.9880592861155083
25	2.432496375E9	3422038.0	3426740.0	0.001406800863166754	0.0014087338567976284	1.0013740350048714
26	5.50374912E10	5.832772284E9	5.933723056E9	0.10597816428086024	0.10781238255278612	1.0173075112630268
27	4.1404545E9	7283516.0	7066837.0	0.0017591102619289743	0.0017067780843866296	0.9702507689967318
28	2.3169187216E10	2.6682057E7	2.4001526E7	0.0011516181707735568	0.0010359243842367164	0.8995380678483672
29	7.982224425E9	9.7016951E7	9.7016951E7	0.012154124694383045	0.012154124694383045	1.0
30	1.336604325E10	1634262.0	1593867.0	1.2226969264071474E-4	1.1924748186042268E-4	0.9752824210561097
31	2.1725597025E10	2.057206E7	1.4759732E7	9.469042427845548E-4	6.793706052365666E-4	0.7174649500341725
32	7.55825256E10	4.5205407E7	3.9286691E7	5.980933640566253E-4	5.197853695431421E-4	0.8690706180346965
33	3.6449865E10	8.9155314E7	9.3889965E7	0.0024459710344606213	0.0025758659188444967	1.053105651111273
34	3.6449865E10	9238073.0	9106013.0	2.5344601413475744E-4	2.4982295544853184E-4	0.9857048109492098
35	3.4359607296E10	1538031.0	1415654.0	4.4762764217594856E-5	4.120111117116302E-5	0.9204326830863618
36	1.1519976E11	1.29398873E8	9.9423146E7	0.0011232564602037 36	8.630499403818202E-4	0.7683463054581627
37	8.75157885E9	4066810.0	3662879.0	4.6469443625020873E-4	4.185392216399901 6E-4	0.9006762056747181
38	2.879988E10	1.6612658E7	1.4455878E7	5.768308062394704E-4	5.019422997595823E-4	0.8701724913617074
39	1.98402204E10	6847562.0	6363141.0	3.4513537964527853E-4	3.207192698323049E-4	0.9292564273240608
40	4.25151342E10	1.65884682E8	1.5772422E8	0.003901779569121059	0.0037098370490384106	0.9508064162307645
41	1.53474324E10	1136436.0	1090743.0	7.404730448592822E-5	7.107006381080395E-5	0.959792720399565
42	6.1249825E10	5.934646E7	4.558859E7	9.689245642742652E-4	7.443056367916153E-4	0.7681770740832731
43	1.9601901E10	1.41515102E8	1.25684739E8	0.007219458051543062	0.006411864798215234	0.888136582058924
44	3.96491392E10	2.11859655E8	1.90722408E8	0.005343360770868892	0.004810253434203182	0.9002299564775558
45	2.6236876056E10	3.5749931E7	3.1010163E7	0.0013625833702036528	0.001181930460540039	0.8674188210321301
46	1.2254655735E10	3.5248463E7	2.5491647E7	0.002876332372139053	0.002080160189828458	0.7231988243005092
47	7.730921472E10	1.1303601E7	1.0496642E7	1.462128549738812E-4	1.357747849078139E-4	0.9286104490064714
48	4.71857664E10	2.2843543E7	2.1241629E7	4.841193593498568E-4	4.501702657520044E-4	0.9298745382885658
49	4.3379703975E10	4.3740916E7	3.6200843E7	0.001008326751727217	8.345110658399785E-4	0.8276196822215612
50	5.7458664E9	5312449.0	4662843.0	9.245688343884919E-4	8.1151260321681E-4	0.8777200496418884
51	9.64931374E9	1195810.0	946606.0	1.2392694778312805E-4	9.810086245573771E-5	0.7916023448541156
52	1.03217642776E11	3.6895887E7	3.8458612E7	3.5745717503034253E-4	3.7259727083151657E-4	1.042354992034749
53	7.19994E9	1507474.0	1447942.0	2.0937313366500276E-4	2.0110473142831745E-4	0.9605087716272387
54	2.5798447675E10	3.0446037E7	2.6163858E7	0.001180149960321207 7	0.001014164043108458 1	0.8593518427373651
55	4.049955E9	1212982.0	1212778.0	2.9950505622901985E-4	2.9945468529897246E-4	0.9998318194334292
56	7.3668683935E10	6487311.0	6005169.0	8.806063381998165E-5	8.151589901210308E-5	0.9256792220998808
57	1.3357869525E10	861156.0	810760.0	6.446806494016867E-5	6.069530762241818E-5	0.9414786635638606
58	2.713506432E10	1372306.0	1300023.0	5.057316186232648E-5	4.790933917344037E-5	0.947327345358834
59	7.494207731328E12	1.657591379E9	1.486459729E9	2.2118300405135275E-4	1.9834781504469908E-4	0.8967588440866282
60	1.0410461685E11	6.460281E7	5.0126051E7	6.20556628080035E-4	4.8149690683002593E-4	0.7759113109785782

TABUĽKA 6.7. Analýza hustých (dense) obrázkov so zašifrovanými prvými 70 percentami pixelov.

	Počet párov U	SP originálu P	SP 70% P'	Pomer R v originály	Pomer R' v 70%	Pomer R'/R
1	2.36747712E10	1.4215947E7	1.4309662E7	6.004681895299584E-4	6.044266227164214E-4	1.0065922446109288
2	4.049955E9	5708825.0	4389624.0	0.001409602081998442	0.0010838698207757864	0.7689189982176718
3	2.82267612E10	9.9303936E7	9.9227928E7	0.0035180775894331088	0.0035153848256597006	0.9992345922723547
4	3.09237252096E11	5.35230462E8	4.73612812E8	0.0017308084920953908	0.0015315516122002373	0.8848764142277089
5	7.19994E9	8.1107433E7	6.6604746E7	0.011265015125126043	0.009250736256135468	0.8211916409683437
6	3.50064477E10	1.3208192E7	1.0998686E7	3.773074067152492E-4	3.141902912931094E-4	0.8327169986626481
7	5.91764283E10	5.93637794E8	6.15964988E8	0.01003165975125268	0.010408958527833285	1.0376108027919797
8	1.001726562E11	2.2217815E7	1.9743758E7	2.2179520682411534E-4	1.9709727932721026E-4	0.8886453505891556
9	1.1519976E11	1.1066040901E10	1.1302938162E10	0.0960595829453117	0.0981159706455639	1.021407589500107
10	4.71857664E10	1.676681E7	1.6189079E7	3.553361803613727E-4	3.430924245833591E-4	0.9655431772650851
11	1.03217642776E11	3.6895887E7	3.8480989E7	3.5745717503034253E-4	3.7281406516432805E-4	1.0429614824004636
12	8.154858195E9	5927813.0	5675606.0	7.269057116939849E-4	6.959785031553207E-4	0.9574536173796305
13	5.39963124E9	2347225.0	2466905.0	4.347009815433248E-4	4.568654580937642E-4	1.0509878686534098
14	2.2578864E9	1425698.0	1235701.0	6.314303500831574E-4	5.472821839043806E-4	0.8667340488658888
15	6.10065057E9	817767.0	753960.0	1.3404586783274822E-4	1.2358681936441412E-4	0.921974107539189
16	7.8267483E8	814495.0	809034.0	0.0010406556705036753	0.0010336783156806	0.9932952320149294
17	1.029605325E10	7550511.0	7475960.0	7.333403214479295E-4	7.260995857805999E-4	0.990126363632872
18	2.227881376E9	2456562.0	2182845.0	0.0011026448833692303	9.797851104259153E-4	0.888577206681533
19	3.09237252096E11	1.38616337E8	1.2375801E8	4.4825238893588334E-4	4.0020408007499826E-4	0.8928096981815354
20	2.1892676625E10	2.7274919E7	2.5966611E7	0.0012458467033151092	0.0011860866281808518	0.9520325614899168
21	2.5490900736E10	3.4423677E7	3.2983817E7	0.001350429996825672	0.0012939447429340144	0.9581723939601223
22	2.44574235136E11	8046880.0	7635753.0	3.290158505668181E-5	3.1220594416881 24E-5	0.9489085210665501
23	3.6449865E10	7348126.0	6827913.0	2.0159542429032317E-4	1.8732340983978953E-4	0.929204670687465
24	8.909456328E9	3916600.0	3857002.0	4.396003365201073 6E-4	4.329110394624744E-4	0.9847832303528571
25	2.432496375E9	3422038.0	3444387.0	0.001406800863166754	0.0014159885438678197	1.0065309035142216
26	5.50374912E10	5.832772284E9	5.941222647E9	0.10597816428086024	0.10794864586778258	1.018593279099459
27	4.1404545E9	7283516.0	7086429.0	0.0017591102619289743	0.0017115099320618062	0.9729406786502561
28	2.3169187216E10	2.6682057E7	2.3454821E7	0.0011516181707735568	0.0010123281745422104	0.8790484556719146
29	7.982224425E9	9.7016951E7	9.7016951E7	0.012154124694383045	0.012154124694383045	1.0
30	1.336604325E10	1634262.0	1583245.0	1.2226969264071474E-4	1.184527814542273E-4	0.9687828512196943
31	2.1725597025E10	2.057206E7	1.480091E7	9.469042427845548E-4	6.812659731729513E-4	0.7194665969280666
32	7.55825256E10	4.5205407E7	3.8976684E7	5.980933640566253E-4	5.156837998014715E-4	0.8622128764375464
33	3.6449865E10	8.9155314E7	9.372364E7	0.0024459710344606213	0.0025713028018073594	1.0512400864854787
34	3.6449865E10	9238073.0	9056005.0	2.5344601413475744E-4	2.4845098877595293E-4	0.9802915608049426
35	3.4359607296E10	1538031.0	1408811.0	4.4762764217594856E-5	4.100195289961908E-5	0.915983487979111
36	1.1519976E11	1.29398873E8	9.9108049E7	0.0011232564460203736	8.603147176695507E-4	0.7659112224261798
37	8.75157885E9	4066810.0	3626059.0	4.6469443625020873E-4	4.143319807945283E-4	0.8916224264226753
38	2.879988E10	1.6612658E7	1.4032993E7	5.768308062394704E-4	4.8725873163360403E-4	0.8447169020153187
39	1.98402204E10	6847562.0	6279288.0	3.4513537964527853E-4	3.164928550894525E-4	0.9170107550687383
40	4.25151342E10	1.65884682E8	1.5457809E8	0.003901779569121059	0.0036358368122003954	0.9318406506032908
41	1.53474324E10	1136436.0	1083613.0	7.404730448592822E-5	7.060549098753483E-5	0.9535187199279149
42	6.1249825E10	5.934646E7	4.5429806E7	9.689245642742652E-4	7.417132375480256E-4	0.7655015311781023
43	1.9601901E10	1.41515102E8	1.20022559E8	0.007219458051543062	0.0061230060798694984	0.8481254460036357
44	3.96491392E10	2.11859655E8	1.85711157E8	0.005343360770868892	0.004683863527609699	0.8765763212443634
45	2.6236876056E10	3.5749931E7	3.0348829E7	0.0013625833702036528	0.0011567241822244174	0.8489199321811278
46	1.2254655735E10	3.5248463E7	2.4502112E7	0.002876332372139053	0.001999412511444166	0.6951256853383934
47	7.730921472E10	1.1303601E7	1.0405752E7	1.462128549738812E-4	1.345991165178401E-4	0.9205696485571279
48	4.71857664E10	2.2843543E7	2.09439E7	4.841193593498568E-4	4.4386054520034247E-4	0.9168411397478929
49	4.3379703975E10	4.3740916E7	3.5855365E7	0.001008326751727217	8.265470188700152E-4	0.8197214022678446
50	5.7458664E9	5312449.0	4580168.0	9.245688343884919E-4	7.971239985670394E-4	0.8621575473006894
51	9.64931374E9	1195810.0	942187.0	1.2392694778312805E-4	9.764290242675848E-5	0.7879069417382359
52	1.03217642776E11	3.6895887E7	3.8544874E7	3.5745717503034253E-4	3.7343300005066954E-4	1.0446929762116843
53	7.19994E9	1507474.0	1441240.0	2.0937313366500276E-4	2.0017389033797503E-4	0.9560629238049876
54	2.5798447675E10	3.0446037E7	2.5635052E7	0.0011801499603212077	9.93666453227791E-4	0.8419832111483015
55	4.049955E9	1212982.0	1221612.0	2.9950505622901985E-4	3.0163594410308 26E-4	1.007114697497572
56	7.3668683935E10	6487311.0	5950761.0	8.806063381998165E-5	8.077734910061008E-5	0.9172923881713085
57	1.3357869525E10	861156.0	803074.0	6.446806494016867E-5	6.011991646549639E-5	0.9325534514071782
58	2.713506432E10	1372306.0	1292332.0	5.057316186232648E-5	4.762590516682439E-5	0.941722910196414
59	7.494207731328E12	1.657591379E9	1.475716562E9	2.2118300405135275E-4	1.9691428565971948E-4	0.8902776526807696
60	1.0410461685E11	6.460281E7	4.9106116E7	6.20556628080035E-4	4.7169969484403323E-4	0.7601235302303414

TABUĽKA 6.8. Analýza hustých (dense) obrázkov so zašifrovanými prvými 80 percentami pixelov.

	Počet párov U	SP originálu P	SP 80% P'	Pomer R v originály	Pomer R' v 80%	Pomer R'/R
1	2.36747712E10	1.4215947E7	1.4414215E7	6.004681895299584E-4	6.088428427979907E-4	1.013946872480602
2	4.049955E9	5708825.0	4342663.0	0.001409602081998442	0.0010722743832956168	0.7606929622120139
3	2.82267612E10	9.9303936E7	9.9226311E7	0.0035180775894331088	0.0035153275395974227	0.9992183089298695
4	3.09237252096E11	5.35230462E8	4.68180924E8	0.0017308084920953908	0.0015139861734855195	0.8747277242975755
5	7.19994E9	8.1107433E7	6.4007008E7	0.011265015125126043	0.008889936305024763	0.789163281742624
6	3.50064477E10	1.3208192E7	1.074807E7	3.773074067152492E-4	3.070311530067074E-4	0.8137427136128851
7	5.91764283E10	5.93637794E8	6.16164094E8	0.01003165975125268	0.010412323144551797	1.0379462025963933
8	1.001726562E11	2.2217815E7	1.8607442E7	2.2179520682411534E-4	1.8575370471208449E-4	0.8375009873833228
9	1.1519976E11	1.1066040901E10	1.1312953697E10	0.0960595829453117	0.09820292765366873	1.0223126589002294
10	4.71857664E10	1.676681E7	1.6170563E7	3.553361803613727E-4	3.42700018113937E-4	0.964438852709609
11	1.03217642776E11	3.6895887E7	3.8513256E7	3.5745717503034253E-4	3.731266764498815E-4	1.0438360243243372
12	8.154858195E9	5927813.0	5642050.0	7.269057116939849E-4	6.918636553924774E-4	0.9517928450172096
13	5.39963124E9	2347225.0	2466503.0	4.347009815433248E-4	4.567910085652442E-4	1.0508166025839023
14	2.2578864E9	1425698.0	1206843.0	6.314303500831574E-4	5.34501204312139E-4	0.8464927354881608
15	6.10065057E9	817767.0	750165.0	1.3404586783274822E-4	1.2296475456059436E-4	0.9173334213779719
16	7.8267483E8	814495.0	807719.0	0.0010406556705036753	0.0010319981798826978	0.991680734688365
17	1.029605325E10	7550511.0	7487325.0	7.333403214479295E-4	7.272034068005621E-4	0.9916315597712526
18	2.227881376E9	2456562.0	2132354.0	0.0011026448833692303	9.571218750562418E-4	0.8680236851339391
19	3.09237252096E11	1.38616337E8	1.2291864E8	4.4825238893588334E-4	3.97489756382394E-4	0.8867543513287326
20	2.1892676625E10	2.7274919E7	2.5966129E7	0.0012458467033151092	0.0011860646116861008	0.9520148895767573
21	2.5490900736E10	3.4423677E7	3.2883171E7	0.001350429996825672	0.00128999643208214	0.9552486505145863
22	2.44574235136E11	8046880.0	7591396.0	3.290158505668181E-5	3.1039230259796844E-5	0.9433961982780903
23	3.6449865E10	7348126.0	6802799.0	2.0159542429032317E-4	1.866344086596754E-4	0.9257869285311655
24	8.909456328E9	3916600.0	3862504.0	4.396003365201073 6E-4	4.335285855152296E-4	0.9861880202216209
25	2.432496375E9	3422038.0	3427140.0	0.001406800863166754	0.001408898296919353	1.001490924414048
26	5.50374912E10	5.832772284E9	5.947026362E9	0.10597816428086024	0.10805409607769331	1.0195882973716313
27	4.1404545E9	7283516.0	7042567.0	0.0017591102619289743	0.001700916409056059	0.9669185871219339
28	2.3169187216E10	2.6682057E7	2.3068119E7	0.0011516181707735568	9.956378178026803E-4	0.864555495102945
29	7.982224425E9	9.7016951E7	9.7016951E7	0.012154124694383045	0.012154124694383045	1.0
30	1.336604325E10	1634262.0	1570429.0	1.2226969264071474E-4	1.1749393374138603E-4	0.9609407793854352
31	2.1725597025E10	2.057206E7	1.466082E7	9.469042427845548E-4	6.748178189593388E-4	0.7126568753931303
32	7.55825256E10	4.5205407E7	3.8787995E7	5.980933640566253E-4	5.131873365184294E-4	0.8580388403537657
33	3.6449865E10	8.9155314E7	9.3542952E7	0.0024459710344606213	0.0025663456366710824	1.049213420974548
34	3.6449865E10	9238073.0	9021795.0	2.5344601413475744E-4	2.4751243934648316E-4	0.9765884075607542
35	3.4359607296E10	1538031.0	1402490.0	4.4762764217594856E-5	4.081798688552741E-5	0.9118736878515453
36	1.1519976E11	1.29398873E8	9.8981706E7	0.0011232564460203736	8.592179879541416E-4	0.7649348383428347
37	8.75157885E9	4066810.0	3591443.0	4.6469443625020873E-4	4.1037658022129343E-4	0.8831105952822974
38	2.879988E10	1.6612658E7	1.3876112E7	5.768308062394704E-4	4.818114519921611E-4	0.8352734402887244
39	1.98402204E10	6847562.0	6165915.0	3.4513537964527853E-4	3.1077855364953507E-4	0.9004540594155993
40	4.25151342E10	1.65884682E8	1.51951532E8	0.003901779569121059	0.00357405744705376	0.9160070126306178
41	1.53474324E10	1136436.0	1072181.0	7.404730448592822E-5	6.986061069081497E-5	0.943459200518111
42	6.1249825E10	5.934646E7	4.5195399E7	9.689245642742652E-4	7.378861735523327E-4	0.7615517252419101
43	1.9601901E10	1.41515102E8	1.16348948E8	0.007219458051543062	0.005935595124166784	0.822166301374676
44	3.96491392E10	2.11859655E8	1.79902251E8	0.005343360770868892	0.00453735578198883	0.849157669967885
45	2.6236876056E10	3.5749931E7	2.9868885E7	0.0013625833702036528	0.001138431455644637	0.8354948992768685
46	1.2254655735E10	3.5248463E7	2.3740077E7	0.002876332372139053	0.0019372292060557015	0.6735067285061479
47	7.730921472E10	1.1303601E7	1.0319216E7	1.462128549738812E-4	1.334797674167864E-4	0.9129140350937722
48	4.71857664E10	2.2843543E7	2.073928E7	4.841193593498568E-4	4.395240680036936E-4	0.9078836851183725
49	4.3379703975E10	4.3740916E7	3.5438684E7	0.001008326751727217	8.169415821837683E-4	0.810195287176885
50	5.7458664E9	5312449.0	4521076.0	9.245688343884919E-4	7.868397357794466E-4	0.8510342405169443
51	9.64931374E9	1195810.0	935059.0	1.2392694778312805E-4	9.690419704396512E-5	0.7819461285655748
52	1.03217642776E11	3.6895887E7	3.8350661E7	3.5745717503034253E-4	3.715514128066993E-4	1.0394291645570142
53	7.19994E9	1507474.0	1430047.0	2.0937313366500276E-4	1.9861929404967264E-4	0.9486379201233321
54	2.5798447675E10	3.0446037E7	2.5211638E7	0.0011801499603212077	9.772540703846826E-4	0.8280761795040845
55	4.049955E9	1212982.0	1215020.0	2.9950505622901985E-4	3.00008271696846E-4	1.0016801568366223
56	7.3668683935E10	6487311.0	5903899.0	8.806063381998165E-5	8.01412307732982E-5	0.9100687480529298
57	1.3357869525E10	861156.0	799037.0	6.446806494016867E-5	5.98176976129732E-5	0.9278655667498106
58	2.713506432E10	1372306.0	1287428.0	5.057316186232648E-5	4.7445179595579454E-5	0.9381493631886766
59	7.494207731328E12	1.657591379E9	1.466138736E9	2.2118300405135275E-4	1.9563625516692143E-4	0.8844994940094942
60	1.0410461685E11	6.460281E7	4.7927468E7	6.20556628080035E-4	4.6037792991502664E-4	0.7418789987618186

TABUĽKA 6.9. Analýza hustých (dense) obrázkov so zašifrovanými prvými 90 percentami pixelov.

	Počet párov U	SP originálu P	SP 90% P'	Pomer R v originály	Pomer R' v 90%	Pomer R'/R
1	2.36747712E10	1.4215947E7	1.4321177E7	6.004681895299584E-4	6.049130054528257E-4	1.0074022504445184
2	4.049955E9	5708825.0	4205667.0	0.001409602081998442	0.0010384478346055696	0.7366957298568444
3	2.82267612E10	9.9303936E7	9.9209447E7	0.0035180775894331088	0.0035147300923777255	0.9990484868595741
4	3.09237252096E11	5.35230462E8	4.60096595E8	0.001730808492095 3908	0.0014878433690685075	0.8596233354894514
5	7.19994E9	8.1107433E7	5.966388E7	0.011265015125126043	0.008286719055992132	0.7356154398327462
6	3.50064477E10	1.3208192E7	9925068.0	3.773074067152492E-4	2.835211411639462E-4	0.7514327471920457
7	5.91764283E10	5.93637794E8	6.17971169E8	0.01003165975125268	0.010442860219057864	1.040990272597098
8	1.001726562E11	2.2217815E7	1.8189281E7	2.2179520682411534E-4	1.8157930207704726E-4	0.8186800097129263
9	1.1519976E11	1.1066040901E10	1.133561881E10	0.096059582945 3117	0.0983996738361 2605	1.024360827093603
10	4.71857664E10	1.676681E7	1.6028855E7	3.553361803613727E-4	3.3969682433726453E-4	0.955987155577
11	1.03217642776E11	3.6895887E7	3.8357613E7	3.5745717503034253E-4	3.716187656333385E-4	1.039617586643194
12	8.154858195E9	5927813.0	5582643.0	7.269057116939849E-4	6.845787954256389E-4	0.9417711051276415
13	5.39963124E9	2347225.0	2492231.0	4.347009815433248E-4	4.615557783905258E-4	1.0617776310323894
14	2.2578864E9	1425698.0	1172199.0	6.314303500831574E-4	5.191576511555232E-4	0.8221930591191122
15	6.10065057E9	817767.0	746436.0	1.3404586783274822E-4	1.2235350827510187E-4	0.9127734428021672
16	7.8267483E8	814495.0	810896.0	0.0010406556705036753	0.0010360573368636372	0.9955813111191596
17	1.029605325E10	7550511.0	7494620.0	7.333403214479295E-4	7.279119307196667E-4	0.9925977195450745
18	2.227881376E9	2456562.0	2079135.0	0.0011026448833692303	9.332341579752045E-4	0.8463596685123355
19	3.09237252096E11	1.38616337E8	1.22129339E8	4.4825238893588334E-4	3.949373439720193E-4	0.8810602100963034
20	2.1892676625E10	2.7274919E7	2.593866E7	0.0012458467033151092	0.0011848098998721679	0.9510077738452679
21	2.5490900736E10	3.4423677E7	3.3070504E7	0.001350429996825672	0.0012973454466163907	0.9606906316254363
22	2.44574235136E11	8046880.0	7544591.0	3.290158505668181E-5	3.0847856871778384E-5	0.9375796582029308
23	3.6449865E10	7348126.0	6750711.0	2.0159542429032317E-4	1.8520537730386656E-4	0.9186983184556171
24	8.909456328E9	3916600.0	3806462.0	4.396003365201073 6E-4	4.2723814499029796E-4	0.9718791809222285
25	2.432496375E9	3422038.0	3404544.0	0.001406800863166754	0.0013996090744431222	0.9948878416896598
26	5.50374912E10	5.832772284E9	5.958464461E9	0.10597816428086024	0.10826191984928267	1.0215493029523524
27	4.1404545E9	7283516.0	6998656.0	0.0017591102619289743	0.0016903110516007362	0.9608897680735513
28	2.3169187216E10	2.6682057E7	2.2869542E7	0.0011516181707735568	9.870670812399897E-4	0.8571131528577427
29	7.982224425E9	9.7016951E7	9.7016951E7	0.012154124694383045	0.012154124694383045	1.0
30	1.336604325E10	1634262.0	1509414.0	1.2226969264071474E-4	1.1292900761786776E-4	0.9236058844909814
31	2.1725597025E10	2.057206E7	1.4675362E7	9.469042427845548E-4	6.754871676535665E-4	0.713363756473586
32	7.55825256E10	4.5205407E7	3.867477E7	5.980933640566253E-4	5.11689305073976E-4	0.8555341620970253
33	3.6449865E10	8.9155314E7	9.3287931E7	0.0024459710344606213	0.0025593491498528183	1.0463530081897305
34	3.6449865E10	9238073.0	8994585.0	2.5344601413475744E-4	2.4676593452403734E-4	0.9736429880993579
35	3.4359607296E10	1538031.0	1396763.0	4.4762764217594856E-5	4.065130861267455E-5	0.9081500958043108
36	1.1519976E11	1.29398873E8	9.8862753E7	0.0011232564460203736	8.581854076779327E-4	0.7640155644941359
37	8.75157885E9	4066810.0	3499218.0	4.6469443625020873E-4	3.9983848171578777E-4	0.8604331158819812
38	2.879988E10	1.6612658E7	1.3602161E7	5.768308062394704E-4	4.7229922485788136E-4	0.8187829425008328
39	1.98402204E10	6847562.0	6038273.0	3.4513537964527853E-4	3.043450565700369E-4	0.8818135564161376
40	4.25151342E10	1.65884682E8	1.48136774E8	0.003901775691210 59	0.0034843303869895818	0.8930105674253878
41	1.53474324E10	1136436.0	1068948.0	7.404730448592822E-5	6.964995656211524E-5	0.9406143416787219
42	6.1249825E10	5.934646E7	4.5154611E7	9.689245642742652E-4	7.372202451190676E-4	0.7608644390920705
43	1.9601901E10	1.41515102E8	1.07986458E8	0.007219458051543062	0.005508978848531069	0.7630737389427172
44	3.96491392E10	2.11859655E8	1.71962185E8	0.005343360770868892	0.004337097563015945	0.8116797178773844
45	2.6236876056E10	3.5749931E7	2.9450438E7	0.0013625833702036528	0.0011224826437850669	0.8237900654969096
46	1.2254655735E10	3.5248463E7	2.3410322E7	0.002876332372139053	0.0019103206574084964	0.6641515688215965
47	7.730921472E10	1.1303601E7	1.0074325E7	1.462128549738812E-4	1.303120855190081E-4	0.8912491691806884
48	4.71857664E10	2.2843543E7	2.010112E7	4.841193593498568E-4	4.2599965060650155E-4	0.8799475633004915
49	4.3379703975E10	4.3740916E7	3.5064137E7	0.001008326751727217	8.083074292117734E-4	0.8016324349494647
50	5.7458664E9	5312449.0	4403208.0	9.245688343884919E-4	7.663262062619486E-4	0.8288471098734312
51	9.64931374E9	1195810.0	924271.0	1.2392694778312805E-4	9.578619007573072E-5	0.7729246284944933
52	1.03217642776E11	3.6895887E7	3.8235093E7	3.5745717503034253E-4	3.704317592582182E-4	1.0362968913039006
53	7.19994E9	1507474.0	1439058.0	2.0937313366500276E-4	1.9987083225693548E-4	0.9546154693215273
54	2.5798447675E10	3.0446037E7	2.4947285E7	0.001180149960321 2077	9.67007213545456E-4	0.8193935059594126
55	4.049955E9	1212982.0	1185393.0	2.9950505622901985E-4	2.9269288177276044E-4	0.9772552272004036
56	7.3668683935E10	6487311.0	5880883.0	8.806063381998165E-5	7.982880493954354E-5	0.9065208990288888
57	1.3357869525E10	861156.0	792817.0	6.446806494016867E-5	5.935205449613044E-5	0.9206427174635025
58	2.713506432E10	1372306.0	1286436.0	5.057316186232648E-5	4.740862173124932E-5	0.937426492342087
59	7.494207731328E12	1.657591379E9	1.441488304E9	2.2118300405135275E-4	1.923469905930354E-4	0.8696282583646328
60	1.0410461685E11	6.460281E7	4.6459472E7	6.20556628080035E-4	4.462767685600487E-4	0.7191555909100549

TABUĽKA 6.10. Analýza hustých (dense) obrázkov so zašifrovanými prvými 100 percentami pixelov.

	Počet párov U	SP originálu P	SP 100% P'	Pomer R v originály	Pomer R' v 100%	Pomer R'/R
1	2.36747712E10	1.4215947E7	1.4377393E7	6.004681895299584E-4	6.072875162569681E-4	1.011356682745089
2	4.049955E9	5708825.0	4056648.0	0.001409602081998442	0.0010016526109549366	0.7105924599195107
3	2.82267612E10	9.9303936E7	9.9227252E7	0.0035180775894331088	0.0035153608767554954	0.999227784888607
4	3.09237252096E11	5.35230462E8	4.53012512E8	0.0017308084920953908	0.0014649351232087855	0.8463877603438797
5	7.19994E9	8.1107433E7	5.75629E7	0.011265015125126043	0.007994913846504276	0.709711772039438
6	3.50064477E10	1.3208192E7	9046229.0	3.773074067152492E-4	2.584160803039721E-4	0.6848953285960713
7	5.91764283E10	5.93637794E8	6.21026425E8	0.01003165975125268	0.010494489830505705	1.0461369395224185
8	1.001726562E11	2.2217815E7	1.7728721E7	2.2179520682411534E-4	1.7698164022528933E-4	0.7975506985722943
9	1.1519976E11	1.1066040901E10	1.1360625107E10	0.0960595829453117	0.0981674283870035	1.0266205600210079
10	4.71857664E10	1.676681E7	1.5862648E7	3.553361803613727E-4	3.3617442737986344E-4	0.9460742979731983
11	1.03217642776E11	3.6895887E7	3.8304747E7	3.5745717503034253E-4	3.711065857522815E-4	1.038184744006832
12	8.154858195E9	5927813.0	5534663.0	7.269057116939849E-4	6.786951860663225E-4	0.9336770576264805
13	5.39963124E9	2347225.0	2479173.0	4.347009815433248E-4	4.5913746509844997E-4	1.0562144660183834
14	2.2578864E9	1425698.0	1169136.0	6.314303500831574E-4	5.178010727200447E-4	0.8200446377844396
15	6.10065057E9	817767.0	744912.0	1.3404586783274822E-4	1.2210369885190785E-4	0.9109098312844611
16	7.8267483E8	814495.0	798355.0	0.0010406556705036753	0.0010200340797978645	0.980184040417682
17	1.029605325E10	7550511.0	7504737.0	7.333403214479295E-4	7.288945402453119E-4	0.9939376288571727
18	2.227881376E9	2456562.0	2035837.0	0.0011026448833692303	9.137995505196951E-4	0.8287342228691967
19	3.09237252096E11	1.38616337E8	1.20000485E8	4.4825238893588334E-4	3.8805313456461224E-4	0.8657023233848692
20	2.1892676625E10	2.7274919E7	2.5992976E7	0.0012458467033151092	0.0011872909121727823	0.9529992004742526
21	2.5490900736E10	3.4423677E7	3.363136E7	0.001350429996825672	0.0013193476506894667	0.9769833710675359
22	2.44574235136E11	8046880.0	7519661.0	3.290158505668181E-5	3.074592463028068E-5	0.9344815630405822
23	3.6449865E10	7348126.0	6713610.0	2.0159542429032317E-4	1.8418751345169592E-4	0.9136492760194912
24	8.909456328E9	3916600.0	3795508.0	4.396003365201073 6E-4	4.260089348069141E-4	0.9690823673594444
25	2.432496375E9	3422038.0	3395578.0	0.001406800863166754	0.0013959231491146621	0.9922677655829655
26	5.50374912E10	5.832772284E9	6.006733074E9	0.10597816428086024	0.1091389331714306	1.0298247182522786
27	4.1404545E9	7283516.0	6990998.0	0.0017591102619289743	0.0016884614961956471	0.9598383527955454
28	2.3169187216E10	2.6682057E7	2.2622959E7	0.0011516181707735568	9.764243686708703E-4	0.8478716239906092
29	7.982224425E9	9.7016951E7	9.7016951E7	0.012154124694383045	0.012154124694383045	1.0
30	1.336604325E10	1634262.0	1373166.0	1.2226969264071474E-4	1.027354149852837E-4	0.8402361432866946
31	2.1725597025E10	2.057206E7	1.4582594E7	9.469042427845548E-4	6.712171814297932E-4	0.7088543393320843
32	7.55825256E10	4.5205407E7	3.8596481E7	5.980933640566253E-4	5.106534968712398E-4	0.853802311745584
33	3.6449865E10	8.9155314E7	9.2648869E7	0.0024459710344606213	0.002541816519759401	1.03918504510006
34	3.6449865E10	9238073.0	8967593.0	2.5344601413475744E-4	2.460254105193531E-4	0.9707211666329113
35	3.4359607296E10	1538031.0	1381310.0	4.4762764217594856E-5	4.0201565404992455E-5	0.8981028340781168
36	1.1519976E11	1.29398873E8	9.8658902E7	0.0011232564460203736	8.564158640608279E-4	0.7624401952867086
37	8.75157885E9	4066810.0	3337480.0	4.6469443625020873E-4	3.8135747357175443E-4	0.8206628782756018
38	2.879988E10	1.6612658E7	1.3061131E7	5.768308062394704E-4	4.535133826946501E-4	0.7862156074000921
39	1.98402204E10	6847562.0	5928905.0	3.4513537964527853E-4	2.988326178070078E-4	0.8658417404617877
40	4.25151342E10	1.65884682E8	1.45229439E8	0.003901779569121059	0.003415946855931599	0.875484325912624
41	1.53474324E10	1136436.0	1064557.0	7.404730448592822E-5	6.936385007305847E-5	0.9367505077276679
42	6.1249825E10	5.934646E7	4.4897508E7	9.689245642742652E-4	7.330226331258905E-4	0.7565322009097089
43	1.9601901E10	1.41515102E8	9.9059037E7	0.007219458051543062	0.005053542357958037	0.69998915734096
44	3.96491392E10	2.11859655E8	1.65861111E8	0.005343360770868892	0.004183220981503679	0.7828820027107095
45	2.6236876056E10	3.5749931E7	2.8938208E7	0.0013625833702036528	0.0011029593591186037	0.8094619259544864
46	1.2254655735E10	3.5248463E7	2.3178911E7	0.002876332372139053	0.0018914371404004193	0.657586431499155
47	7.730921472E10	1.1303601E7	1.0076581E7	1.462128549738812E-4	1.3034126703389182E-4	0.8914487515969468
48	4.71857664E10	2.2843543E7	1.8093193E7	4.841193593498568E-4	3.8344599188284035E-4	0.7920484576319882
49	4.3379703975E10	4.3740916E7	3.5021833E7	0.001008326751727217	8.073322266141628E-4	0.8006652855646644
50	5.7458664E9	5312449.0	4334927.0	9.245688343884919E-4	7.544427068474826E-4	0.8159940923668162
51	9.64931374E9	1195810.0	917038.0	1.2392694778312805E-4	9.503660309007634E-5	0.7668760087304839
52	1.03217642776E11	3.6895887E7	3.8308792E7	3.5745717503034253E-4	3.711457747890703E-4	1.038294376823086
53	7.19994E9	1507474.0	1418453.0	2.0937313366500276E-4	1.9700900285280154E-4	0.9409469085370626
54	2.5798447675E10	3.0446037E7	2.4680053E7	0.0011801499603212077	9.566487608444836E-4	0.8106162716678035
55	4.049955E9	1212982.0	1183889.0	2.9950505622901985E-4	2.9232151962182295E-4	0.976015307729216
56	7.3668683935E10	6487311.0	5712179.0	8.806063381998165E-5	7.753876810178963E-5	0.880515671285067
57	1.3357869525E10	861156.0	790365.0	6.446806494016867E-5	5.9168492289940976E-5	0.9177953820213759
58	2.713506432E10	1372306.0	1282985.0	5.057316186232648E-5	4.7281443112496E-5	0.9349117470884774
59	7.494207731328E12	1.657591379E9	1.408013808E9	2.2118300405135275E-4	1.8788027480397786E-4	0.8494335973498086
60	1.0410461685E11	6.460281E7	4.5427446E7	6.20556628080035E-4	4.3636341379032703E-4	0.7031806511202842

Literatúra

[1] Anderson, R., Needham, R., and Shamir, A. Steganographic file system. In: *Proceedings of the Second International Workshop on Information Hiding* (IH '98), Lecture Notes in Computer Science, vol. 1525. D. Aucsmith, ed., Portland, Oregon, April 14-17, 1998. Springer-Verlag, Berlin, Germany, 1998, pp. 73-82. Also available: http://www.cl.cam.ac.uk/ftp/users/rja14/sfs3.pdf.

[2] Arnold, M., Schmucker, M., and Wolthusen, S. D. *Techniques and Applications of Digital Watermarking and Content Protection.* Artech House, Norwood, Massachusetts, 2003.

[3] Artz, D. Digital Steganography: Hiding data within data. *IEEE Internet Computing* (2001) 5(3):75-80. Also available: http://www.cc.gatech.edu/classes/AY2003/cs6262_fall/digital_steganography.pdf.

[4] Barni, M., Podilchuk, C. I., Bartolini, F., and Delp, E. J. Watermark embedding: Hiding a signal within a cover image, *IEEE Communications* (2001) 39(8):102-108.

[5] Bauer, F. L. *Decrypted Secrets: Methods and Maxims of Cryptology*, 3rd ed. Springer-Verlag, New York, 2002.

[6] Curran, K. and Bailey, K. An evaluation of image-based steganography methods. *International Journal of Digital Evidence* [Online]. (Fall 2003). Available: http://www.ijde.org/docs/03_fall_steganography.pdf.

[7] Wilfrid J. Dixon, Frank J. Massey: Introduction to Statistical Analysis. McGrawhill Book Company, Inc., New York 1957.

[8] Farid, H. *Detecting Steganographic Messages in Digital Images.* Technical Report TR2001-412, Dartmouth College, Computer Science Department, 2001. Also available: http://www.cs.dartmouth.edu/ farid/publications/tr01.pdf.

[9] Farid, H. and Lyu, S. Higher-order wavelet statistics and their application to digital forensics. *IEEE Workshop on Statistical Analysis in Computer Vision*, Madison, Wisconsin, June 2003. Also available: http://www.cs.dartmouth.edu/ farid/publications/sacv03.pdf.

[10] Fridrich, J. and Du, R. Secure steganographic methods for palette images. In: *Proceedings of the 3rd Information Hiding Workshop*, Lecture Notes in Computer Science, vol. 1768. Dresden, Germany, September 1999. Springer-Verlag, Berlin, Germany, 2000, pp. 47-60. Also available: http://www.ws.binghamton.edu/fridrich/Research/ihw99_paper1.dot.

[11] Fridrich, J., Du, R., and Meng, L., "Steganalysis of LSB Encoding in Color Images," *Proceedings IEEE International Conference on Multimedia and Expo*, July 30 - August 2, 2000, New York City, NY.

[12] Fridrich, J. and Goljan, M. Practical steganalysis of digital images: State of the art. In: *Proceedings of the SPIE Security and Watermarking of Multimedia Contents IV*, vol. 4675. International Society for Optical Engineering, San Jose, California, January 21-24, 2002, pp. 1-13. Also available: http://www.ws.binghamton.edu/fridrich/Research/steganalysis01.pdf.

[13] Fridrich, J., Goljan, M., and Hogea, D. Attacking the OutGuess. In: *Proceedings of the ACM Workshop on Multimedia and Security 2002*, Juan-les-Pins, France, December 2002A. Also available: http://www.ws.binghamton.edu/fridrich/Research/acm_outguess.pdf.

[14] Fridrich, J., Goljan, M., and Hogea, D. Steganalysis of JPEG images: Breaking the F5 algorithm. *Proceedings of the 5th International Workshop on Information Hiding* (IH 2002). F. A. P. Petitcolas, ed., Noordwijkerhout, The Netherlands, October 7-9, 2002B. Springer-Verlag, Berlin, Germany, pp. 310-323. Also available: http://www.ws.binghamton.edu/fridrich/Research/f5.pdf.

[15] Fridrich, J., Goljan, M., and Hogea, D. New methodology for breaking steganographic techniques for JPEGs. In: Proceedings of the SPIE Security and Watermarking of Multimedia Contents V, vol. 5020. International Society for Optical Engineering, Santa Clara, California, January 21-24, 2003A, pp. 143-155. Also available: http://www.ws.binghamton.edu/fridrich/Research/jpeg01.pdf.

[16] Fridrich, J., Goljan, M., Hogea, D., and Soukal, D. Quantitative steganalysis of digital images: Estimating the secret message length, *Multimedia Systems* (2003B) 9(3):288-302. Also available: http://www.ws.binghamton.edu/fridrich/Research/mms100.pdf.

[17] Fries, B. and Fries, M. *MP3 and Internet Audio Handbook*. TeamCom Books, Burtonsville, Maryland, 2000.

[18] Hosmer, C. and Hyde, C. Discovering covert digital evidence. *Digital Forensic Research Workshop*(DFRWS) 2003, August 2003 [Online]. (January 4, 2004). Available: http://www.dfrws.org/dfrws2003/presentations/Paper-Hosmer-digitalevidence.pdf.

[19] Chandramouli, R. Mathematical approach to steganalysis. In: *Proceedings of the SPIE Security and Watermarking of Multimedia Contents IV*, vol. 4675. International Society for Optical Engineering, San Jose, California, January 21-24, 2002, pp. 14-25. Also available: http://www.ece.stevens-tech.edu/ mouli/spiesteg02.pdf.

[20] Jackson, J. T., Gregg, H., Gunsch, G. H., Claypoole, R. L., and Lamont, G. B. Blind Steganography detection using a computational immune system: A work in progress. *International Journal of Digital Evidence* [Online]. (Winter 2003) (December 21, 2003). Available: http://www.ijde.org/docs/02_winter_art4.pdf.

[21] Johnson, N. F. and Jajodia, S. *Exploring steganography: Seeing the unseen*, Computer (1998A) 31(2):26-34. Also available: http://www.jjtc.com/pub/r2026.pdf.

[22] Johnson, N. F. and Jajodia, S. Steganalysis of images created using current steganography software. In: *Proceedings of the Second International Workshop on Information Hiding* (IH '98), Lecture Notes in Computer Science, vol. 1525. D. Aucsmith, ed. Portland, Oregon, April 14-17, 1998. Springer-Verlag, Berlin, Germany, 1998B, pp.273-289. Also available: http://www.jjtc.com/ihws98/jjgmu.html.

[23] Johnson, N. F., Duric, Z. and Jajodia, S. *Information Hiding: Steganography and Watermarking: Attacks and Countermeasures.* Kluwer Academic, Norwell, Massachusetts, 2001.

[24] Kahn, D. Codebreakers: *The Story of Secret Writing.* Revised ed., Scribner, New York, 1996.

[25] Kwok, S. H. Watermark-based copyright protection system security, *Communications of the ACM* (2003) 46(10):98-101.

[26] McDonald, A. D. and Kuhn, M. G. StegFS: A steganographic file system for Linux. In: *Proceedings of the Third International Workshop on Information Hiding* (IH '99), Lecture Notes in Computer Science, vol. 1768. A. Pfitzmann, ed., Dresden, Germany, September 29-October 1, 1999. Springer-Verlag, Berlin, Germany, 2000, pp. 462-477. Also available: http://www.cl.cam.ac.uk/ mgk25/ih99-stegfs.pdf.

[27] Monash University. JPEG Image Coding Standard [Online]. (January 10, 2004). Available: http://www.ctie.monash.edu.au/emerge/multimedia/jpeg/.

[28] Ozer, H., Avcibas, I., Sankur, B., and Memon N. Steganalysis of audio based on audio quality metrics. In: *Proceedings of the SPIE, Security and Watermarking of Multimedia Contents V*, vol. 5020, SPIE, Santa Clara, California, 2003, pp. 55-66. Also available: www.busim.ee.boun.edu.tr/ sankur/SankurFolder/Audio_Steganalysis_16.doc.

[29] Provos, N. and Honeyman, P. *Detecting Steganographic Content on the Internet.* Center for Information Technology Integration, University of Michigan, CITI Technical Report 01-11 [Online]. (August 2001). Available: http://www.citi.umich.edu/techreports/reports/citi-tr-01-11.pdf.

[30] Provos, N. and Honeyman, P. Hide and seek: An introduction to steganography. *IEEE Security & Privacy* (2003) 1(3):32-44. Also available: http://niels.xtdnet.nl/papers/practical.pdf.

[31] Rey, R. F. (ed.). *Engineering and Operations in the Bell System*, 2nd. ed., AT&T Bell Laboratories, Murray Hill, New Jersey, 1983.

[32] Rowland, C. H. Covert Channels in the TCP/IP Protocol Suite. *First Monday*, 1996 [Online]. (January 10, 2004). Available: http://www.firstmonday.dk/issues/issue2_5/rowland/ or http://www.guides.sk/psionic/covert/covert.tcp.txt.

[33] Seward, J. Personal communication, January 2004.

[34] Simmons, G. J. Prisoners' problem and the subliminal channel. In: *Advances in Cryptology: Proceedings of CRYPTO 83.* D. Chaum, ed. Plenum, New York, 1983, pp. 51-67.

[35] spam mimic [Online]. (December 29, 2003). Available: http://www.spammimic.com/.

[36] Wayner, P. *Disappearing Cryptography: Information Hiding: Steganography & Watermarking.* 2nd. ed., Morgan Kaufmann, San Francisco, California, 2002.