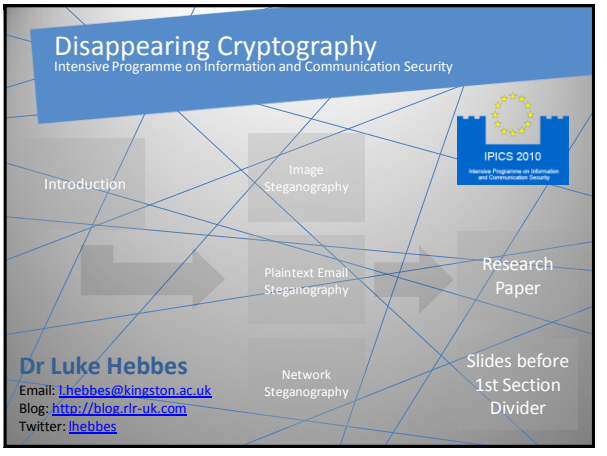



# Disappearing Cryptography (IPICS)

Dr Luke Hebbes
Email: l.hebbes@kingston.ac.uk
Blog: http://blog.rlr-uk.com
Twitter: lhebbes

Kingston University London

## Steganography

- From the Greek - Hidden writing
- Thought to be 'old-hat' & fell out of favour
- Most common form is embedding data within images
- You can steganographically embed data in almost any 'cover'
- Not really cryptography as you're hiding comms channel rather than encrypting

Kingston University London

## Steganography

- Steganography is split into two categories:
  - Watermarking
  - Data Hiding
- Three forms of embedding
  - Robust
  - Semi-Fragile
  - Fragile
- We won't look at Watermarking here

Kingston University London

## Steganography

- Will look at schemes to embed data in:
  - Images
  - TCP traffic
  - Plaintext Email
  - HTTP traffic
  - Twitter
- Will also look at a Semi-fragile Digital Signature for Images using steganography

Kingston University London

## Computer Colour Space

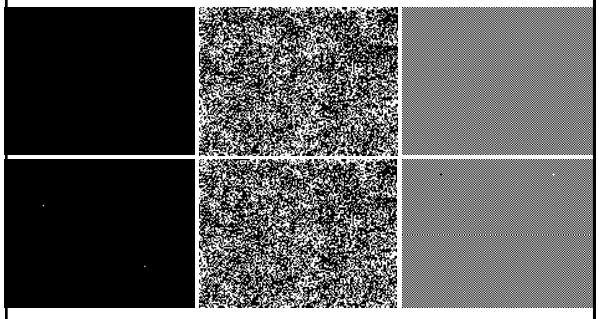
- Most often 24bpp RGB Colour – 'True Colour'
- RGB for transmitted & CMYK for reflected
- Hue, Saturation & Luminescence more accurate

RGB: (255,0,0)
RGB: (128,0,0)
RGB: (255,255,255)
RGB: (0,0,0)
RGB: (128,128,128)

RGB: (204,0,204)
Red: 11001100
Green: 00000000
Blue: 11001100
3 bytes ⇒ 24 bits

Kingston University London

## Visual Patterns





## LSB Embedding

- Least-Significant Bit embedding
- Overwrite the LSB of every pixel with 1 bit of your data
- 256x256 pixel true colour bitmap can hold 24KB data in this way
- Lots of tools to do this
- Can be detected easily



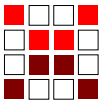
## The GIF Standard

- Proprietary standard by CompuServe
- 256-colour palette maximum ($2^n$ colours)
- Each colour indexed in lookup-table with 3-byte RGB colour definition
- Pixel data is 1-byte index value (can be interlaced), which is compressed
- Utilises the lossless Lempel-Ziv-Welch (LZW) compression algorithm



## GIF Palette

Colour 0
…
Colour 7
…
Colour 16
…
Colour 147
…
Colour 255



| | | | |
|---|---|---|---|
| 147 | 16 | 16 | 147 |
| 16 | 147 | 147 | 16 |
| 16 | 255 | 255 | 16 |
| 255 | 16 | 16 | 255 |

| Index | Red | Green | Blue |
|---|---|---|---|
| 0 | 0 | 0 | 0 |
| 1 | 16 | 16 | 16 |
| … | … | … | … |
| 7 | 128 | 128 | 128 |
| … | … | … | … |
| 16 | 255 | 255 | 255 |
| … | … | … | … |
| 147 | 255 | 0 | 0 |
| … | … | … | … |
| 254 | 204 | 0 | 204 |
| 255 | 128 | 0 | 0 |



## GIF Steganography Example

- Inherently 2 methods of embedding data
  - Embed data in palette
  - Embed data in image pixels
- Palette is very limited (max. 256 entries of 3-bytes ⇒ max. 762 bytes of data assuming a b&w image)
- Doesn't affect compression
- Image pixels provides more 'space' but does affect compression



## GIF Steganography Example

- Example here uses a 256-colour palette with only 16 distinct colours in a 40x40 pixel GIF (800 bytes)
- 4 MSB of each pixel determine colour
- 4 LSB of each pixel embedded data

Original

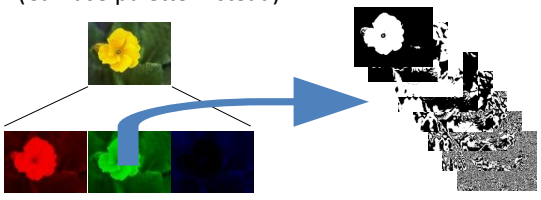
Stego

Piet Mondrian
==========
Dutch Neo-Plasticist Painter, 1872-1944

Biography: Pioneer of abstract art, who developed from early landscape pictures to geometric abstract works of a most rigorous kind. Born in Amerafoort, Utrecht. Studied painting at Amsterdam Academy 1892-4 & again 1896-7. Painted landscapes in Hague School tradition. Began to work in a more vividly coloured & sometimes pointillist style in 1908. Joined Theosophic Organisation in 1909 & made some works of Symbolist character. First one-man exhibition at Stedelijk Museum, Amsterdam, 1909. Lived in Paris 1912-14; was influenced by Cubism, which he carried to point of abstraction. Returned to Holland in 1914 & evolved a more simplified abstract style which he called Neo-Plasticism, restricted to the three primary colours and to a grid of black lines on a white ground; associated with van Doesburg in de Stijl movement 1917-25. Lived 1919-38 in Paris where he joined Abstraction-Cr-23ation in 1931. Moved to London 1938-40, then finally in 1940 to New York where he started to develop a more colourful style, with coloured lines & syncopated rhythms.

## Bitmap Image Format

- Uncompressed image format with 3 bytes per pixel (24bpp – 'true colour')
- (Can use palette instead)



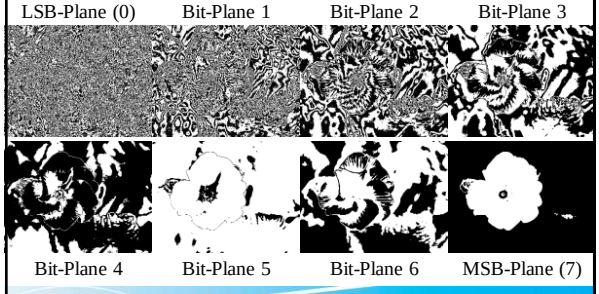


## Bitmap Steganography Example

- Bit-Plane Complexity Segmentation (BPCS)
  - Take Canonical Gray Code of each pixel
  - Bit-slice image – i.e. Split into bit-planes (separate colours)
  - Segment into "simple" & "complex" regions by threshold value
  - Compress steganographic data file & segment
  - Embed 8-byte segments into "complex" regions
  - Take conjugate if complexity below threshold
- 8×8-pixel regions chosen for visual properties



## Bitmap Steganography Example






## Bitmap Steganography Example

410KB Bitmap File, contains 185KB of essentially random data, which can be overwritten

Resulting image after overwriting 185KB of picture with steganographic data



## Plaintext Email Steganography

- We will look at plaintext emails only
- HTML emails and attachments make steganography easy
- We will use only ASCII text
- The embedded data must not be obvious to someone reading the email
- Data rates are quite low



## SPAM-Mimic – Grammar-based

```
Dear Friend , Especially for you - this red-hot news
! If you no longer wish to receive our publications
simply reply with a Subject: of "REMOVE" and you will
immediately be removed from our mailing list . This
mail is being sent in compliance with Senate bill 1620
; Title 1 , Section 301 ! This is NOT unsolicited bulk
mail . Why work for somebody else when you can become
rich within 24 MONTHS ! Have you ever noticed nobody
is getting any younger and more people than ever are
surfing the web ! Well, now is your chance to capitalize
on this ! We will help you deliver goods right to the
customer's doorstep and sell more . You are guaranteed
to succeed because we take all the risk ! But don't
believe us . Mrs Jones who resides in Delaware tried
us and says "My only problem now is where to park all
my cars" ! We are licensed to operate in all states
! We beseech you - act now . Sign up a friend and your
friend will be rich too ! Thank-you for your serious
consideration of our offer !
```

IPICS 2010

## SPAM-Mimic – Fake PGP

```
-----BEGIN PGP MESSAGE-----
Charset: ISO-8859-1
Version: GnuPG v1.2.5 (MingW32)
Comment: Using GnuPG with Thunderbird - http://enigmail.mozdev.org

SW50ZW5zaXZlIFByb2dyYW1tZSBvbiBJbmZvcmlhdGlvbiBhbmQgQ29tbXVuaWNhdGlvbiBTZWN1
cml0eSAyMDEwDQpTYW1vcywgR3JlZWNlDQpodHRwOi8vd3d3LmlwaWNzLXNjaG9vbC51dS8=
-----END PGP MESSAGE-----
```

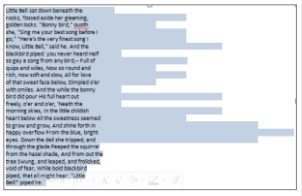
Intensive Programme on Information and Communication Security 2010
Samos, Greece
http://www.ipics-school.eu/



## SPAM-Mimic – Adding Whitespace

Little Bell sat down beneath the rocks, Tossed aside her gleaming, golden locks. "Bonny bird," quoth she, "Sing me your best song before I go," "Here's the very finest song I know, Little Bell," said he. And the blackbird piped: you never heard Half so gay a song from any bird,-- Full of quips and wiles, Now so round and rich, now soft and slow, All for love of that sweet face below, Dimpled o'er with smiles. And the while the bonny bird did pour His full heart out freely, o'er and o'er, 'Neath the morning skies, In the little childish heart below All the sweetness seemed to grow and grow, And shine forth in happy overflow From the blue, bright eyes. Down the dell she tripped; and through the glade Peeped the squirrel from the hazel shade, And from out the tree Swung, and leaped, and frolicked, void of fear, While bold blackbird piped, that all might hear: "Little Bell!" piped he.

IPICS 2010 - Samos





## Network Steganography

- Several schemes, but all rely on sending traffic on a busy public network
- Busy network provides cover
- Use standard protocols, etc.
- Eavesdropper has to find one transmission in thousands or millions
- With observation many can be detected



## TCP Retransmissions

- Send steganographic data in a carrier stream
- Receive steganographic data & extract, but do not send acknowledgement to sender
- Sender sends real packet as retransmission
- An attacker would have to store all packets sent
- Detection: you retransmitted due to error, so the packets will be different anyway



## HTTP Steganography

- HTTP headers are ASCII text

```
GET /index.html HTTP/1.1
Host: www.ipics-school.eu
User-agent: Mozilla/4.0
Connection: close
Accept-language: en-gb
```

- Order and CaPiTaLiSaTiOn are not significant
- Whitespace is removed from the end



## HTTP Steganography

- Consider the following examples:
  - 24 permutations of only 4 header lines (4 bits)
  - 5 lines gives 6 bits, 6 lines gives 9 bits, etc.
  - 4 header lines with added whitespace (4 bytes)
  - Capitalisation of only language gives 2 bytes

```
GET /index.html HTTP/1.1
Host: www.ipics-school.eu
User-agent: Mozilla/4.0
Connection: close
AccePt-LanguaGE: eL
```

```
GET /index.html HTTP/1.1
User-agent: Mozilla/4.0
aCCept-lAnGUage: El
Host: www.ipics-school.eu
Connection: close
```

## Twitter Steganography

- Only 140 plaintext characters
- Can use similar techniques:
  - Capitalisation (easy to spot?)
  - Word order/grammar (low data rate?)
  - URL shortening service:
    - URL is base-64 encoded data – 8 chars are 6 bytes
    - URL service takes specific user to different URL
  - Stego profile image



## Introduction

- Very easy to manipulate & forge digital images (consider news images)
- Can also 'hack' web sites & change images or upload photos from mobiles
- Require three checks:
  - Integrity
  - Authentication
  - Non-repudiation
- Digital Signatures & PKI can provide these



## Introduction

- Digital signatures usually appended to file
- Hide a digital signature within the image
- Use Steganography to achieve this
- Do not require digital watermarking as image manipulation must result in a failed integrity check
- Not interested in copyright issues
- 'End consumer' can verify origin & integrity of image with 'plug-in'



## Introduction

← Original Mona Lisa. Has copyright - Leonardo da Vinci - & integrity check

Defaced Mona → Lisa. Still has copyright, but fails integrity check



## Digital Signature

- Normal Hash not appropriate
- Use BPCS compression to identify visually important regions in image & overwrite complex regions with zeros
- Compress 'hash' & Encrypt
- Embed signature into original image
- Differences in visually important regions can be identified



## Semi-Fragile Embedding

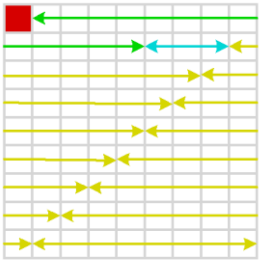
- Three forms of embedding
  - Robust
  - Semi-Fragile
  - Fragile
- BPCS-Steganography is inherently fragile
- Use Channel Coding to correct errors
- Convolutional Coding chosen
- Speed, lack of complexity & high code rate

## Semi-Fragile Embedding

- Write parity data as two separate blocks
- Viterbi (trellis) decoding
- Sequence numbers aide in process of recovering from errors
- Always assume fewest errors
- Most significant changes occur in the LSB planes with low levels of image processing
- Signature is not written into these areas



## Modified Scheme



- 9×9-pixel regions
- Control bit indicates conjugate
- 13-bit Sequence Number
- 3-bit byte count
- Write in spiral from centre of MSB to LSB
- Blue, Red then Green
- No additional information required

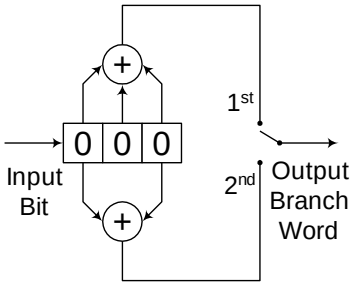


## Convolutional Codes

- Convolutional encoding process is a discrete-time convolution of input sequence with impulse response of encoder
- Modelled as a finite-state machine consisting of an *M*-stage shift register
- Used for streamed data



## Convolutional Codes



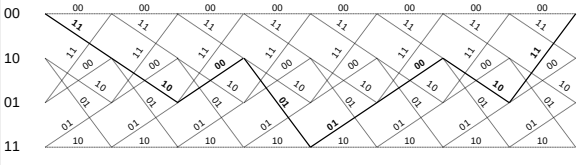



## Convolutional Codes

- Generators are $G_1 = 7_o$ and $G_2 = 5_o$
- Input sequence 101
- Output obtained: 11 10 00 10 11
- Includes 2 appended zeros to flush the register
- Trellis diagram for an encoded sequence shows how this code works



## Convolutional Codes



## Convolutional Codes

- Decoded by applying principle of maximum likelihood decoding to minimum distance decoding
- Fewest errors are the most likely
- Path with minimum distance from received bits taken as decoded data
- Viterbi algorithm chooses survivor paths

Kingston University London

## Digital Signature

← Original Black-&-White Image (138KB)

← Image used for 'Hash' (20KB)

Digitally signed image (138KB) →

Kingston University London