Covert Cryptography and Steganography

J M Blackledge

Stokes Professor
Dublin Institute of Technology
http://eleceng.dit.ie/blackledge

Distinguished Professor
Warsaw University of Technology

Friday 12th March, 2010: 11:00 -13:00

Lectures co-financed by the European Union in scope of the European Social Fund
What is the Problem?

Alice A

Message

Bob B

Attack?
F7&^%p£#29hGS

Attack What?
Have a nice day
Covert Encryption

Information Hiding

Related issues include:

- Camouflage
- Disinformation
- Authentication
- Self-authentication
Steganography (Greek in origin) means *Covered* or *Concealed Writing*

At what time should I confirm our activities? kindly acknowledge.

110000010000000000000000000000000000000000000000000
1100000000000010000010001110000000

Attack now
Watermarking and Authentication

[Diagram showing processes of digital watermarking in print, on web, and in ID card, with examples of content delivered and content tracked.]
Camouflage and Disinformation
Why Should Encrypted Information be Transmitted Covertly?
Focus of the Seminar

- **AudioCode**: Steganography for Digital Signals

![AudioCode](image)

- **StegoCrypt**: Steganography for Digital Images

![StegoCrypt](image)
Principal Publications


Contents of Presentation I

Part I:

- Principles of Steganography
- Signal Processing Model for Information Hiding
- Linear Frequency Modulation
- Chirp Coding
- Self-authentication
- Demonstration of Self-Authentication for Audio data
- Summary
- Interval (10 Minutes)
Part II:

• Hiding Information in Digital Images
• Fresnel Diffusion
• Stochastic Diffusion
• Demonstration of StegoCrypt
• Hardcopy Authentication
• Summary
• Research Project Proposals
• Q & A
Principals of Steganography

Data \rightarrow Covertext
\downarrow
Stegotext
\downarrow
Transmission

Plaintext \rightarrow Ciphertext
Hiding Data in Images

\[ \text{Stegotext image} = \text{Covertext image} + \text{Plaintext image} \]
Information Hiding: A Signal Processing Model

\( f \) - Information input (Plaintext or Ciphertext)
\( s \) - Output signal (Stegotext)
\( n \) - Noise (Covertext - cover signal including a cipher)
\( \hat{P} \) - Linear transformation operator (signal processor)

\[
s(t) = \hat{P} f(t) + n(t), \quad ||\hat{P} f(t)|| << ||n(t)||
\]

Diffusion + Confusion  Hiding condition
Information Retrieval 1: **Diffuser/Covertext Retrieval**

\[ f = \hat{P}^{-1}(s - n) \]

- Requires knowledge of both *processor* and *covertext*
- Inverse operator must be computationally stable
- If the *covertext* is a *cipher*, then retrieval is dependent on knowledge of a *private key*
Information Retrieval 2: **Diffuser Only** Retrieval

\[ f = \hat{P}^{-1}(s - n) = \hat{P}^{-1}s - \hat{P}^{-1}n = \hat{P}^{-1}s \]

- Requires knowledge of processor only
- Any *covertext* can be used provided \( \hat{P}^{-1}n = 0 \)
- Require a diffuser such that:
  - the inverse operator is computationally stable
  - simple to implement
Chirp based Diffusion

- A diffuser that provides these properties is a linear frequency modulated (FM) chirp.

- In complex form, a linear FM chirp is given by

\[ \exp(i\alpha t^2) \]

- Operator is based on convolution

- Inverse operator is based on correlation
Linear Frequency Modulation

Let

\[ \hat{P} f(t) = p(t) \otimes f(t) \equiv \int_{-\infty}^{\infty} p(t - \tau) f(\tau) d\tau \]

where

\[ p(t) = \exp(i\alpha t^2), \quad |t| \leq \frac{T}{2} \]

Then

\[ \hat{f}(t) = \exp(-i\alpha t^2) \otimes \exp(i\alpha t^2) \otimes f(t), \quad |t| \leq \frac{T}{2} \]

where

\[ p(t) \otimes f(t) \equiv \int_{-\infty}^{\infty} p(t + \tau) f(\tau) d\tau \]
Evaluation of the Correlation Integral

\[
\exp(-i\alpha t^2) \odot \exp(i\alpha t^2) \equiv \int_{-T/2}^{T/2} \exp[-i\alpha(\tau + t)^2] \exp(i\alpha \tau^2) d\tau
\]

\[
= \exp(-i\alpha t^2) \int_{-T/2}^{T/2} \exp(-2i\alpha t \tau) d\tau = T \exp(-i\alpha t^2) \text{sinc}(\alpha T t)
\]

where

\[
\text{sinc}(x) \equiv \frac{\sin x}{x}
\]
Application of the Condition \( T \gg 1 \)

\[
\cos(\alpha t^2) \text{sinc}(\alpha T t) \sim \text{sinc}(\alpha T t)
\]

\[
\sin(\alpha t^2) \text{sinc}(\alpha T t) \sim 0
\]

\[
\hat{f}(t) = T \exp(-i\alpha t^2) \text{sinc}(\alpha T t)
\]

\[
\sim T \text{sinc}(\alpha T t) \otimes f(t)
\]
Spectral Response

- In Fourier space (ignoring scaling constant)

\[ \hat{F}(\omega) = \begin{cases} F(\omega), & |\omega| \leq \alpha T; \\ 0, & |\omega| > \alpha T. \end{cases} \]

- Retrieved information is a \textit{band-limited} version of the input signal

- \textit{Band-width} is determined by $\alpha T$
Retrieval with Covertext

\[ s(t) = \exp(i\alpha t^2) \otimes f(t) + n(t) \]

\[ \hat{f}(t) \simeq T \text{sinc}(\alpha T t) \otimes f(t) + \exp(-i\alpha t^2) \circ n(t) \]

Provided the covertext does not have any features that match with \( n(t) \), then

\[ \| T \text{sinc}(\alpha T t) \otimes f(t) \| >> \| \exp(-i\alpha t^2) \circ n(t) \| \]
Graphical Example
Why use Chirps?

\[ s(t) = \exp(i\alpha t^2) \otimes f(t) + n(t) \]

\[ \hat{f}(t) \approx T\text{sinc}(\alpha T t) \otimes f(t) \]
Microwave Imaging
Chirp Coding

Binary code

\[ \text{chirp}(t) = a \cos(\alpha t^2), \quad \forall t \in [0, T) \]

\[ s(t) = \begin{cases} 
-\text{chirp}(t), & t \in [0, T); \\
+\text{chirp}(t), & t \in [T, 2T); \\
+\text{chirp}(t), & t \in [2T, 3T); \\
-\text{chirp}(t), & t \in [3T, 4T); \\
-\text{chirp}(t), & t \in [4T, 5T); \\
+\text{chirp}(t), & t \in [5T, 6T); \\
-\text{chirp}(t), & t \in [6T, 7T). 
\end{cases} \]
Decoding

\[
s(t) \odot \text{chirp}(t) = \begin{cases} 
-a, & t \in [0, T); \\
+a, & t \in [T, 2T); \\
+a, & t \in [2T, 3T); \\
-a, & t \in [3T, 4T); \\
-a, & t \in [4T, 5T); \\
+a, & t \in [5T, 6T); \\
-a, & t \in [6T, 7T). 
\end{cases}
\]

Chirp function must be an identical replica of that used to chirp code the binary stream.
Applications

• Covert information exchange using digital signals
  - plaintext
  - ciphertext

• *Covert key exchange*

• Authentication of digital signals
  - Copyright protection
  - Digital Rights Management

• *Self-authentication of digital signals*
  - Speech
  - Audio
Self-authentication of Audio Data: \textit{The Problem}

\begin{align*}
  f(t) & \text{ - audio signal} \\
  w(t) & \text{ - watermark obtained from the audio signal} \\
  s(t) & \text{ - watermarked signal}
\end{align*}

Find transforms $\hat{T}$ and $\hat{L}$ where

\begin{align*}
  w(t) &= \hat{T} f(t) \quad \text{and} \quad s(t) = f(t) + \hat{L} w(t)
\end{align*}

such that

\begin{align*}
  \|\hat{L} w(t)\| &\ll \|f(t)\| \\
  \hat{T} s(t) &= w(t) \quad \text{and} \quad \hat{L}^{-1} s(t) = w(t)
\end{align*}

Signal Coding (?) \quad \text{Chirp Coding (OK)}
Signal Coding using the Wavelet Transformation

\[ F_L(t) = \frac{1}{\sqrt{L}} \int f(\tau) W \left( \frac{t - \tau}{L} \right) d\tau \]

\[ E_L = \frac{100}{E} \int |F_L(t)|^2 \, dt, \quad E = \sum_L E_L \]

Binary[Round(E_L)] is concatenated to produce a binary string which is then

**Chirp Coded**
Demonstration of an Audio Self-Authenticator: AudioCode

http://eleceng.dit.ie/arg/downloads/Audio_Self_Authentication.zip
Multilevel Watermarking
Perceptual Evaluation of Audio Quality: BS.1387
Commercials Applications

Technology to License

Self-authentication of Audio Data for Copyright Protection

Tamborine lives and breathes sound

Tamborine is 100% dedicated to audio post production for television programming and film: from children's programming to documentaries; from drama to animation; from movies to commercials.

It all happens under one roof, in our heart-of-Soho studios where we offer sound editing, ADR track-laying, voice-over recording (for up to 7 artists), Foley recording and the final mix - in either stereo or surround sound. All at extremely competitive rates.

Explore and enjoy the site and sounds of Tamborine now.

If you would like to receive a DVD showreel of some of our work please email us. We'd be delighted to send one to you.

http://www.tamborine.co.uk
On the Search for Extraterrestrial Intelligence

- Chirp coding provides a solution for communicating over ‘channels’ with very noisy environments

- Interstellar space becomes very noisy when radio waves propagate over many light years

- Suggests correlating SETI data with different chirp codes and searching for an output with minimum Information Entropy
Summary

- Covert encryption uses **Steganography** to hide encrypted information in a **Covertext**

- Chirp coding provides an effective method of hiding bit streams in digital signals which has many applications including
  - *key exchange*
  - *authentication and copyright protection*

- Chirp coding is unique in that it provides a method of **self-authenticating** a digital signal
In the Following Lecture…

• We shall investigate a method to hide encrypted information in digital images using the process of stochastic diffusion

• Consider an approach for e-fraud prevention of e-documents

• Investigate a method for authenticating hardcopy documents based on texture coding

• Provide a demonstration of the product
Questions

+ Interval (10 Minutes)
Contents of Presentation II

Part II:

• Hiding Information in Digital Images
• Fresnel Diffusion
• Stochastic Diffusion
• Demonstration of StegoCrypt
• Hardcopy Authentication
• Summary
• Research Project Proposals
• Q & A
Hiding Information in Digital Images
Basic Model

\[ \text{stegotext} = \text{ciphertext} + \text{covertext} \]

\[ \text{ciphertext} = \text{cipher} \otimes \otimes \text{plaintext} \]

\(\otimes\otimes\) denotes the 2D convolution integral

- **Ciphertext** generated by process of **Diffusion**
- **Stegotext** generated by process of **Confusion**
Consider a watermarking model given by

\[ I_3(x, y) = r p(x, y) \otimes \otimes I_1(x, y) + I_2(x, y) \]

with ‘Fresnel’ Point Spread Function (PSF)

\[ p(x, y) = \frac{1}{2} (1 + \cos[\alpha(x^2 + y^2)]) \]

and where

\[ \|p(x, y) \otimes \otimes I_1(x, y)\|_{\infty} = 1 \quad \text{and} \quad \|I_2(x, y)\|_{\infty} = 1. \]
Watermark Retrieval

\[ I_1(x, y) = \frac{1}{r} p(x, y) \circ \circ [I_3(x, y) - I_2(x, y)] \]

where \( \circ \circ \) denote two-dimensional correlation.

Implemented using a Fast Fourier Transform and application of the two-dimensional convolution and correlation theorems, i.e.

\[ p \otimes \otimes f \iff PF \]

and

\[ p \bullet \bullet f \iff P^*F \]

respectively, where \( \iff \) denotes transformation from ‘image space’ to ‘Fourier space’.
Example of Fresnel Watermarking
Stochastic Diffusion

\[ E = mc^2 \]
Let \( n(x, y) \) be a cipher with Fourier transform \( N(k_x, k_y) \) and compute

\[
m(x, y) = \mathcal{F}_2^{-1} \left[ \frac{N(k_x, k_y)}{|N(k_x, k_y)|^2} \right], \quad |N(k_x, k_y)|^2 > 0
\]

so that the diffused field is given by

\[
I(x, y) = m(x, y) \otimes I_0(x, y).
\]
How Does it Work? 2: Condition for Regularisation

\[ \forall k_x, k_y \]

if \[ |N(k_x, k_y)|^2 = 0 \]

then \[ |N(k_x, k_y)|^2 = 1 \]
How Does it Work? 3: Data Retrieval

\[ n(x, y) \odot \odot I(x, y) \iff N^*(k_x, k_y) \tilde{I}(k_x, k_y) \]

and

\[ N^*(k_x, k_y) \tilde{I}(k_x, k_y) = N^*(k_x, k_y) M(k_x, k_y) \tilde{I}_0(k_x, k_y) \]

\[ = N^*(k_x, k_y) \frac{N(k_x, k_y)}{|N(k_x, k_y)|^2} \tilde{I}_0(k_x, k_y) = \tilde{I}_0(k_x, k_y) \]

so that

\[ I_0(x, y) = n(x, y) \odot \odot I(x, y). \]
How Does it Work? 4: **Covertext Model**

\[ I_3(x, y) = rm(x, y) \otimes \otimes I_1(x, y) + I_2(x, y) \]

\[ \| m(x, y) \otimes \otimes I_1(x, y) \|_\infty = 1 \text{ and } \| I_2(x, y) \|_\infty = 1 \]

- \( r \) is the **Diffusion-to-Confusion** watermarking ratio

- \( m \) is a **pre-conditioned** stochastic field

- \( n \) is a **key dependent cipher**
Further Example of Watermarking by Stochastic Diffusion
Image Data Diffusion
Data Redundancy

• For binary plaintext images, stochastic diffusion (with a grey level stochastic field) yields a field that is data redundant.

• The data field can therefore be binarized to compress the encrypted information
Algorithm I: Encryption and Watermarking Algorithm

Step 1: Read the binary plaintext image from a file and compute the size $I \times J$ of the image.

Step 2: Compute a cipher of size $I \times J$ using a private key and pre-condition the result.

Step 3: Convolve the binary plaintext image with the pre-conditioned cipher and normalise the output.

Step 4: Binarize the output obtained in Step 3 using a threshold based on computing the mode of the Gaussian distributed ciphertext.

Step 5: Insert the binary output obtained in Step 4 into the lowest 1-bit layer of the host image and write the result to a file.
Algorithm II: Decryption Algorithm

**Step 1:** Read the watermarked image from a file and extract the lowest 1-bit layer from the image.

**Step 2:** Regenerate the (non-preconditioned) cipher using the same key used in Algorithm I.

**Step 3:** Correlate the cipher with the input obtained in Step 1 and normalise the result.

**Step 4:** Quantize and format the output from Step 3 and write to a file.
StegoCrypt

http://eleceng.dit.ie/arg/downloads/StegoCrypt.zip

Document Authentication for Electronic Data Interchange

Dublin Institute of Technology (DIT) is seeking companies to license a novel technology that provides a facility for authenticating documents (letters, certificates, spreadsheets etc.) communicated via the Internet as attachments.

---

<table>
<thead>
<tr>
<th>Encryption Mode</th>
<th>Decryption Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Inputs:</strong></td>
<td><strong>Inputs:</strong></td>
</tr>
<tr>
<td>Plaintext image</td>
<td>Stegotext image</td>
</tr>
<tr>
<td>Covertext image</td>
<td>Private key (PIN)</td>
</tr>
<tr>
<td>Private Key (PIN)</td>
<td></td>
</tr>
<tr>
<td><strong>Output:</strong></td>
<td><strong>Output:</strong></td>
</tr>
<tr>
<td>Watermarked Covertext image</td>
<td>Decrypted watermark</td>
</tr>
<tr>
<td><strong>Operation:</strong></td>
<td><strong>Operation:</strong></td>
</tr>
<tr>
<td>Encrypt by clicking on button E (for Encrypt)</td>
<td>Decrypt by clicking on button D (for Dcrypt)</td>
</tr>
</tbody>
</table>
Authentication of e-Certificates
Authentication of e-Letters

Jonathan Blackledge
Stokes Professor of DSP
http://eleceng.dit.ie/blackledge

Dublin Institute of Technology
Kevin Street, Dublin 8, Ireland

Tel: +35 3 1 402 4707
Email: jonathan.blackledge@dit.ie

cc: Prof Eugene Coyle
Dr Marek Rebow

4 August, 2009

Dear Sir

Re: A Covert Encryption Method for Applications in Electronic Data Interchange

Please find enclosed the manuscript for the above paper which I am submitting to the ISAST Transactions on Electronics and Signal Processing.

Yours Faithfully

J M Blackledge
Stokes Professor
Camouflage

MS Word

(Format→Background→Fill Effect...)
(Format→Background→Printed Watermark...)

Jonathan Blackledge
Stokes Professor of DSP
http://eleceng.dit.ie/ebblackledge

Tel: +353 1 402 4707
Email: jonathan.blackledge@dit.ie

cc: Prof Eugene Coyle
Dr Marek Reboir

4 August, 2009

Dear Sir,

Re: A Covert Encryption Method for Applications in Electronic Data Interchange

Please find enclosed the manuscript for the above paper which I am submitting to the ISAST Transactions on Electronics and Signal Processing.

Yours Faithfully,

J M Blackledge
Stokes Professor
Other Applications

• **Disinformation:**
  Watermark one letter (consisting of disinformation to be intercepted) with another (secret information)

• **Plausible Deniability**
  Watermark one letter (consisting of information of value to an attacker) with another (consisting of secretive information) and encrypt the result

• **Cribb Camouflage**

• **Covert Key Exchange**
Hardcopy Authentication using Stochastic Diffusion

- The covertext model

\[ I_3(x, y) = rm(x, y) \otimes I_1(x, y) + I_2(x, y) \]

...can not be applied to hardcopy applications due to the de-registration and distortion of pixels that occurs with covertext removal.

- However, we can use a **diffusion only** approach

\[ I(x, y) = m(x, y) \otimes I_0(x, y) \]  

**Texture Coding**
Print/Scan Cycle

\[ I_{\text{print}} = p_{\text{print}} \otimes m \otimes I_0 \]

\[ I_{\text{scan}} = p_{\text{scan}} \otimes I_{\text{print}} \]

Because convolution is \textit{commutative}

\[ I_{\text{scan}} = p_{\text{scan}} \otimes p_{\text{print}} \otimes m \otimes I_0 \]

\[ = m \otimes p_{\text{scan/print}} \otimes I_0 \]
Conditions Required for Hidden Data Retrieval

- $I_{\text{scan}}$ must be re-sampled to the size of the original e-image $I_0$ before correlating with $n$

- Fidelity of the reconstruction critically depends on:
  - orientation
  - cropping

- Method is robust to *hardcopy soiling*
Applications of Texture Coding 1: **Identity Cards**

Printed at 600dpi; scanned with flat-bed scanner at 300dpi

Printed at 600dpi; scanned with mobile phone camera
Applications of Texture Coding 2: Signature Authentication
Applications of Texture Coding 3: Passport Authentication

Printed at 400dpi;

Scanned with flat-bed scanner at 300dpi
Applications of Texture Coding 4: Currency Authentication

Binary texture code printed using UV ink at 150 dpi

Scanned with camera at 300dpi under UV lamp
Applications of Texture Coding 5:

Statistical Authentication

Texture code generated of basic statistics associated with a scan of a high value bank bond and printed on the back of the bond at 300dpi; flat-bed scanned at 150dpi.
Attack and Robustness Analysis

*Printed Document Authentication using Texture Coding*,
Summary

• Fundamental steganographic model

\[ I_3(x, y) = r m(x, y) \otimes I_1(x, y) + I_2(x, y) \]

Diffusion + Confusion
Ciphertext + Covertext

• Retrieval of \( I_1 \) requires knowledge of the Covertext and the Key used to compute \( m \)
Summary (Continued)

\[ I_3(x, y) = rm(x, y) \otimes \otimes I_1(x, y) + I_2(x, y) \]

- **Self-Authentication:** \( I_1 = I_2 \)

- **Stegocrypt:** Based on *binarisation* of ciphertext

- Binary ciphertext embedded in covertext using *1-bit layer replacement method*
• **Diffusion + Confusion** model suitable for electronic-to-electronic (e-to-e) applications

• For hardcopy authentication, a **diffusion only** approach is used called **Texture Coding**

• Based on an application of the model

\[ I(x, y) = m(x, y) \otimes \otimes I_0(x, y) \]
Research Project Proposal
FP7 Security

Can you tell the difference?

Can you tell the difference?

Can you tell the difference?

Can you tell the difference?

Can you tell the difference?

Can you tell the difference?

Can you tell the difference?

Can you tell the difference?

Can you tell the difference?

Can you tell the difference?

Can you tell the difference?

Can you tell the difference?

Can you tell the difference?

Can you tell the difference?

Can you tell the difference?
Q & A