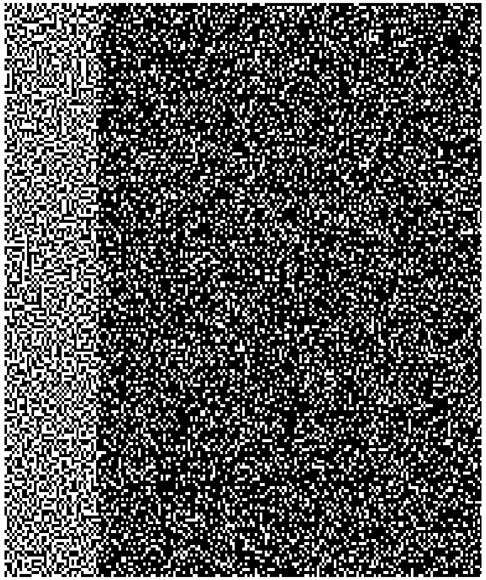
WARSAW UNIVERSITY OF TECHNOLOGY
DEVELOPMENT PROGRAMME

LexiconData



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

Covert Cryptography and *Steganography*

DIT – Dublin Institute of Technology

GCHQ

J M Blackledge

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

Distinguished Professor
Warsaw University of Technology

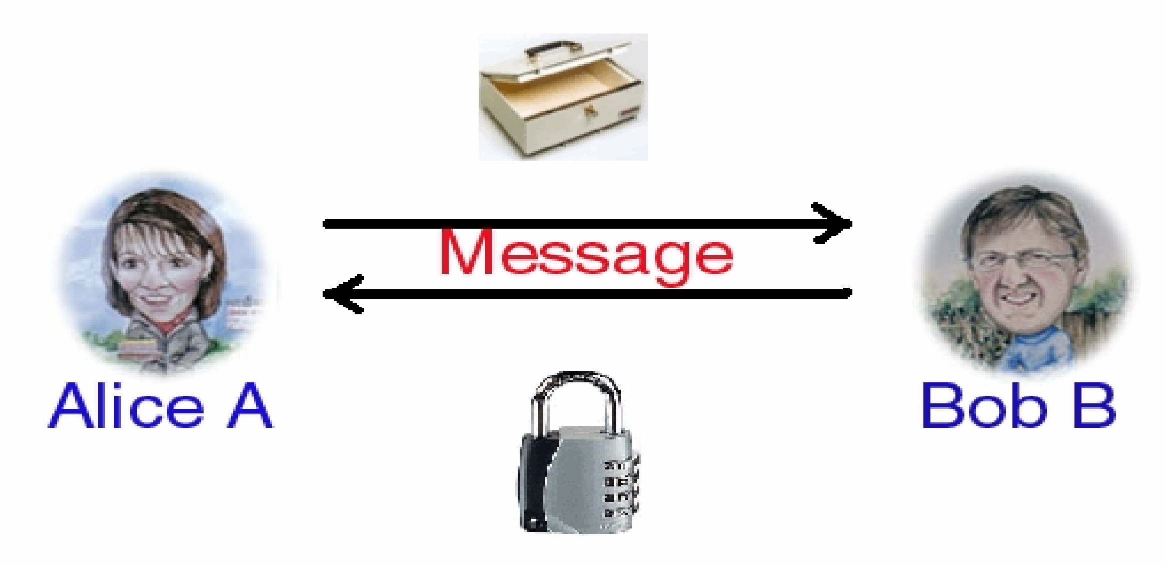
science foundation ireland
fondúireacht eolaíochta éireann

HUMAN CAPITAL
NATIONAL COHESION STRATEGY

EUROPEAN UNION
EUROPEAN SOCIAL FUND

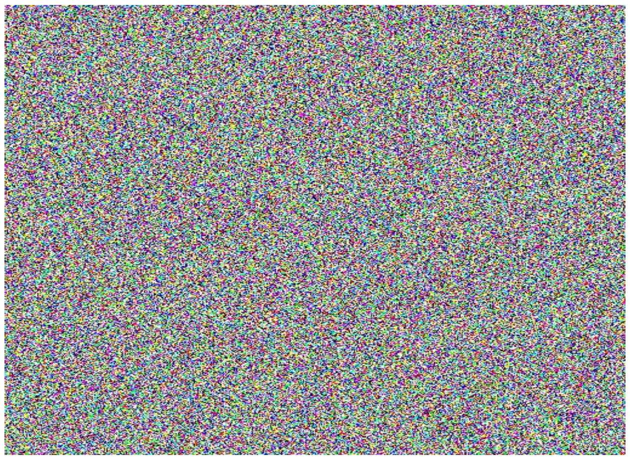
Lectures co-financed by the European Union in scope of the European Social Fund

What is the Problem ?



Attack ?

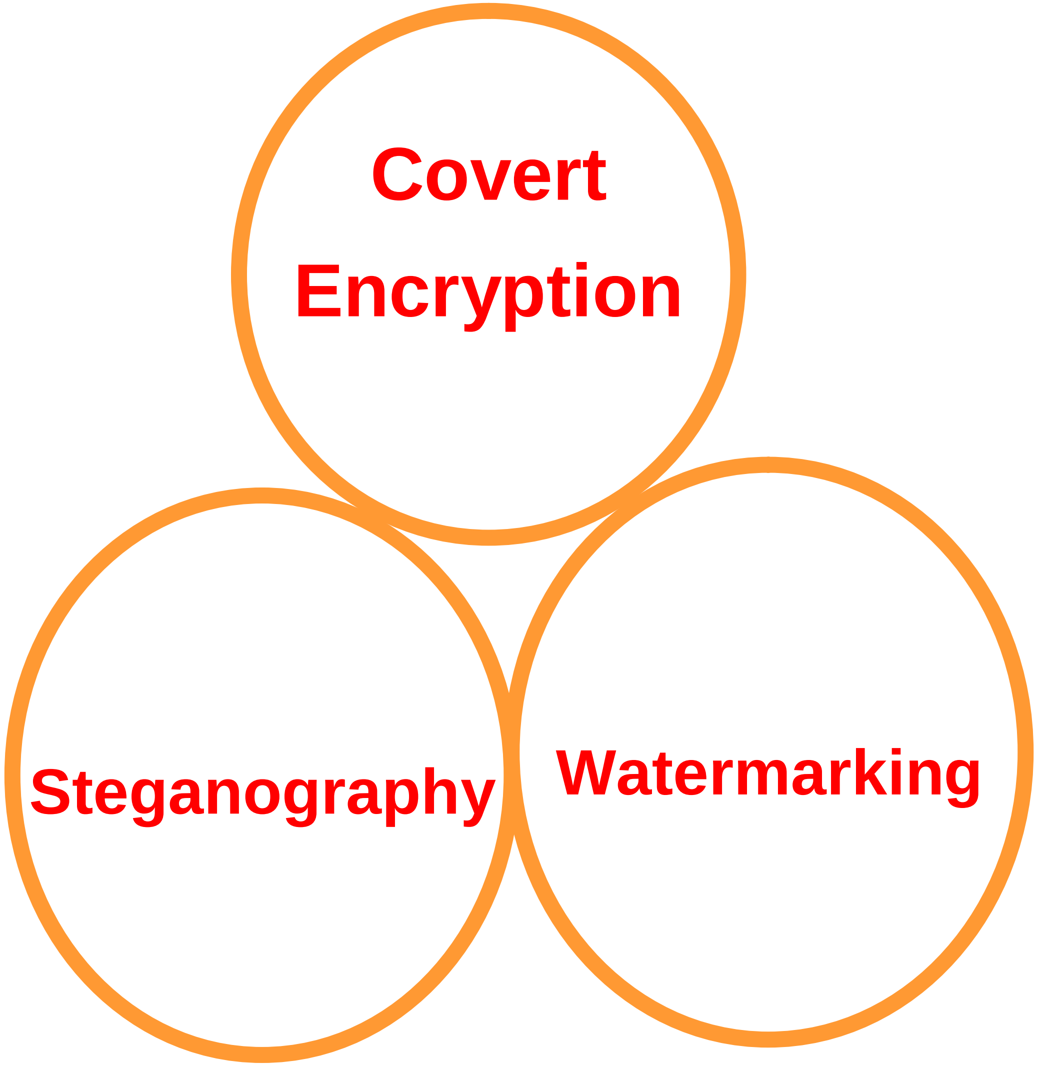
F7&^%p£#29hGS



Attack What ?

Have a nice day

Covert Encryption
Information Hiding



Related issues include:

- ***Camouflage***
- ***Disinformation***
- ***Authentication***
- ***Self-authentication***

Steganography

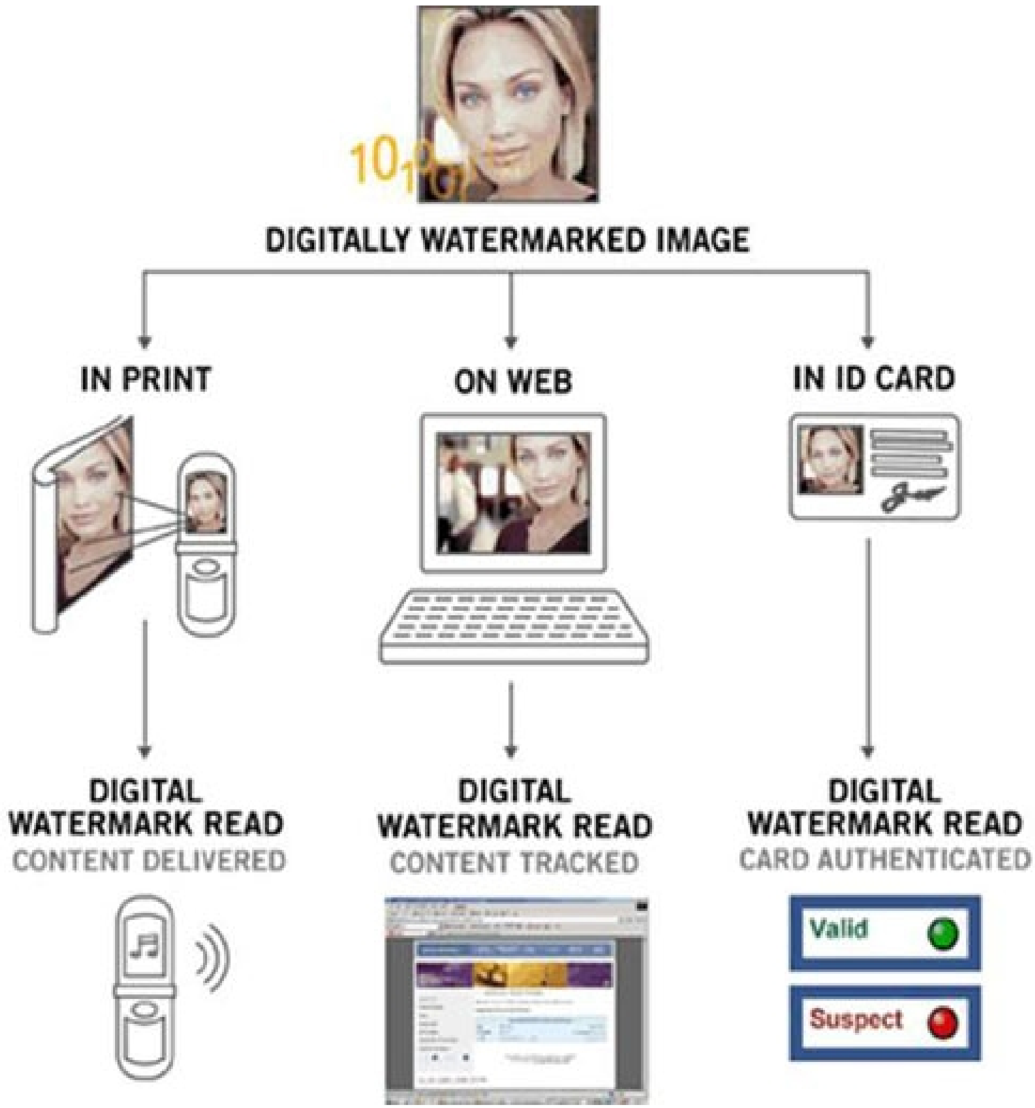
Steganography (Greek in origin) means ***Covered*** or ***Concealed Writing***

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

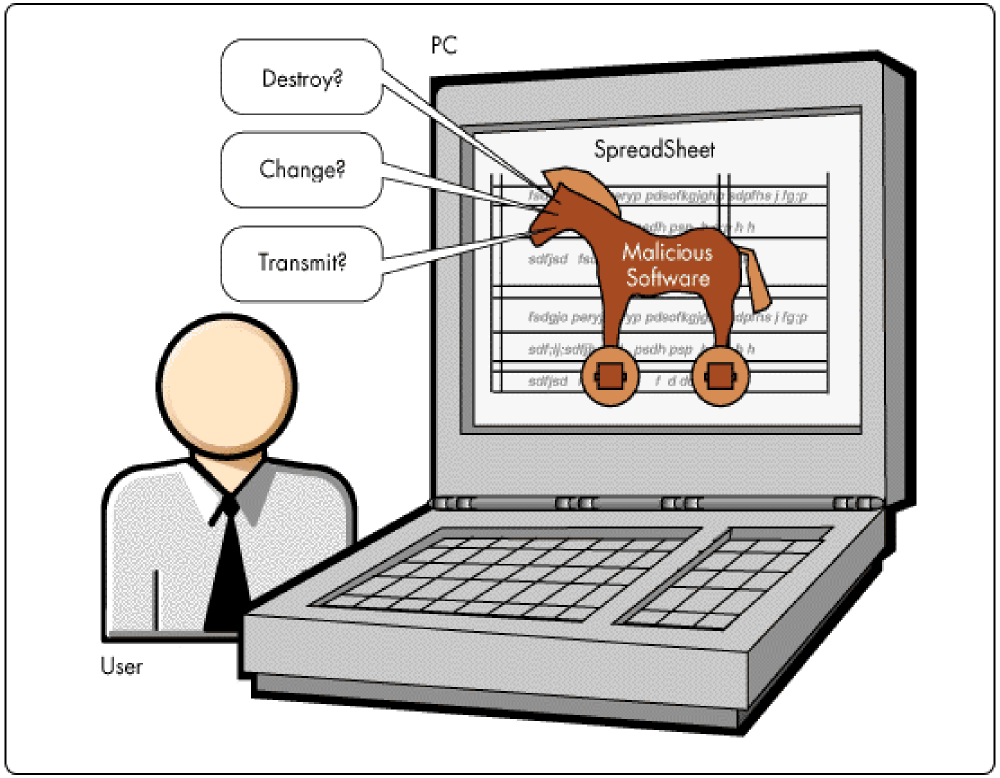
1100001000000000000000000000000000
1100000000000100000100011100000 0

Attack now

Watermarking and Authentication



Camouflage and Disinformation



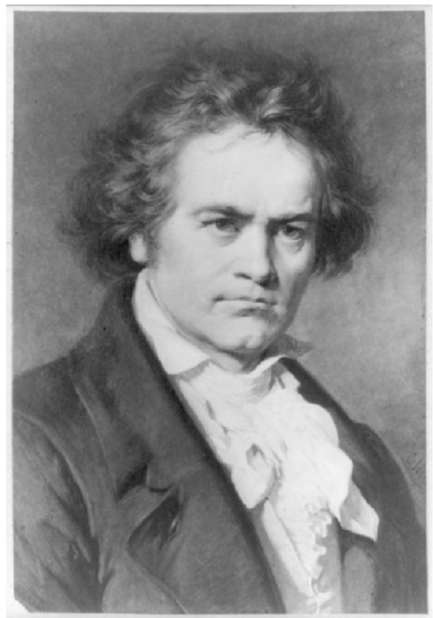
Why Should Encrypted Information be Transmitted Covertly ?

Type VII U-boot

Bundesarchiv, Bild 101II-MW-4222-02A
Foto: Dietrich |

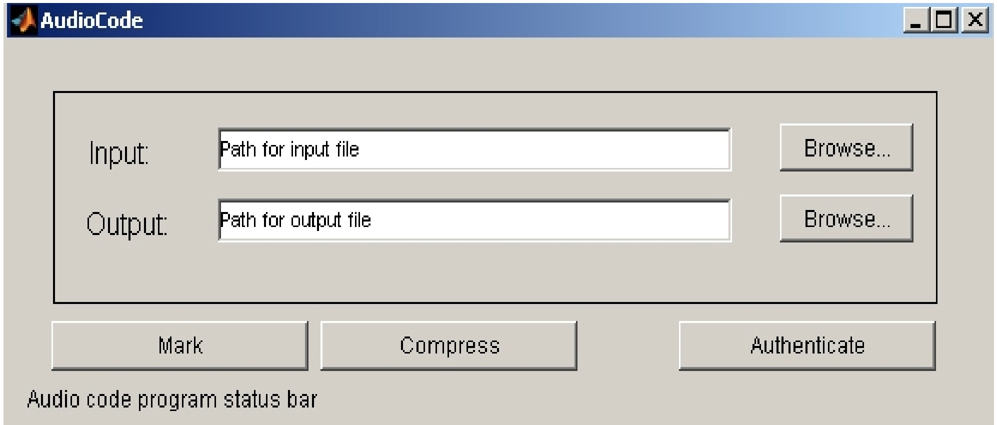
Kurzsignalheft

Bletchley Park



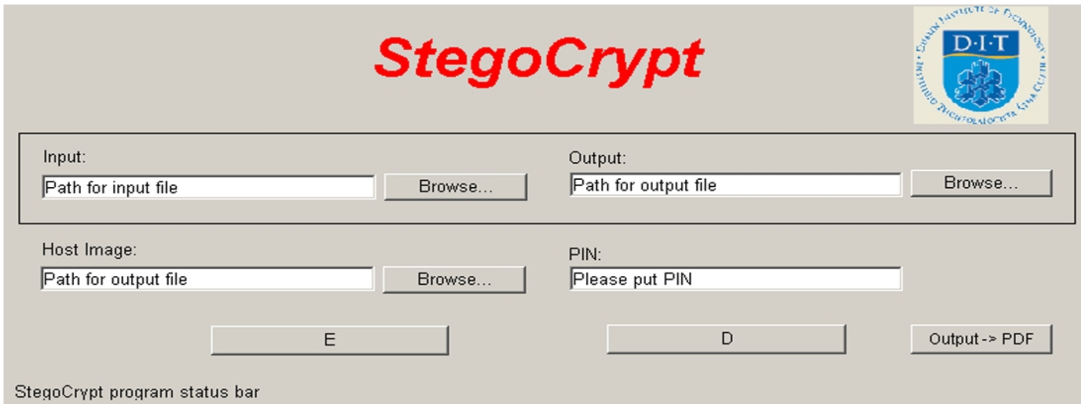
Focus of the Seminar

- ***AudioCode***: Steganography for Digital Signals



- ***StegoCrypt***: Steganography for Digital Images

CRYPSTIC



Principal Publications

Audio Data Verification and Authentication using Frequency Modulation based Watermarking , J M Blackledge and O Farooq, International Society for Advanced Science and Technology, Transactions on Electronics and Signal Processing, No. 2, Vol. 3, 51-63, 2008; http://eleceng.dit.ie/papers/111.pdf

A Covert Encryption Method for Applications in Electronic Data Interchange, J M Blackledge and D Dubovitskiy, International Society for Advanced Science and Technology, Transactions on Electronics and Signal Processing, No. 1, Vol. 4, 107-128, 2009; http://eleceng.dit.ie/papers/140.pdf

Printed Document Authentication using Texture Coding, J M Blackledge and K W Mahmoud, International Society for Advanced Science and Technology, Transactions on Electronics and Signal Processing, No. 1, Vol. 4, 81-98, 2009; http://eleceng.dit.ie/papers/135.pdf

Contents of Presentation I

Part I:

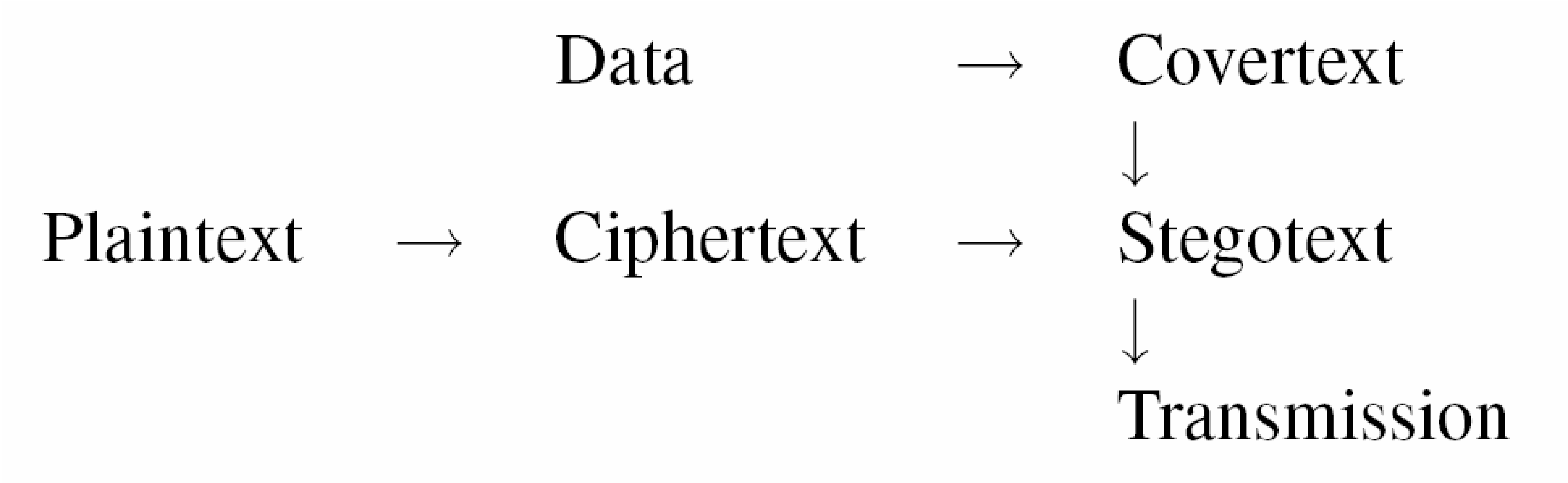
- Principles of Steganography
- Signal Processing Model for Information Hiding
- Linear Frequency Modulation
- Chirp Coding
- Self-authentication
- Demonstration of Self-Authentication for Audio data
- Summary
- Interval (10 Minutes)

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

Principals of Steganography



Hiding Data in Images

Stegotext image
= ***Covertext*** image
+ ***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

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

where

$$p(t) \odot f(t) \equiv \int_{-\infty}^{\infty} p(t+\tau) f(\tau) d\tau$$

Evaluation of the Correlation Integral

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

$$= \exp(-i\alpha t^2) \int_{-T/2}^{T/2} \exp(-2i\alpha t\tau) d\tau = T \exp(-i\alpha t^2) \mathrm{sinc}(\alpha T t)$$

where

$$\mathrm{sinc}(x) \equiv \frac{\sin x}{x}$$

Application of the Condition $T >> 1$

$$\cos(\alpha t^2)\mathrm{sinc}(\alpha T t) \simeq \mathrm{sinc}(\alpha T t)$$

$$\sin(\alpha t^2)\mathrm{sinc}(\alpha T t) \simeq 0$$

$$\hat{f}(t) = T\exp(-i\alpha t^2)\mathrm{sinc}(\alpha T t)$$

$$\simeq T\mathrm{sinc}(\alpha T t) \otimes f(t)$$

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 ***band-limited*** version of the input signal

- ***Band-width*** is determined by αT

Retrieval with Covertext

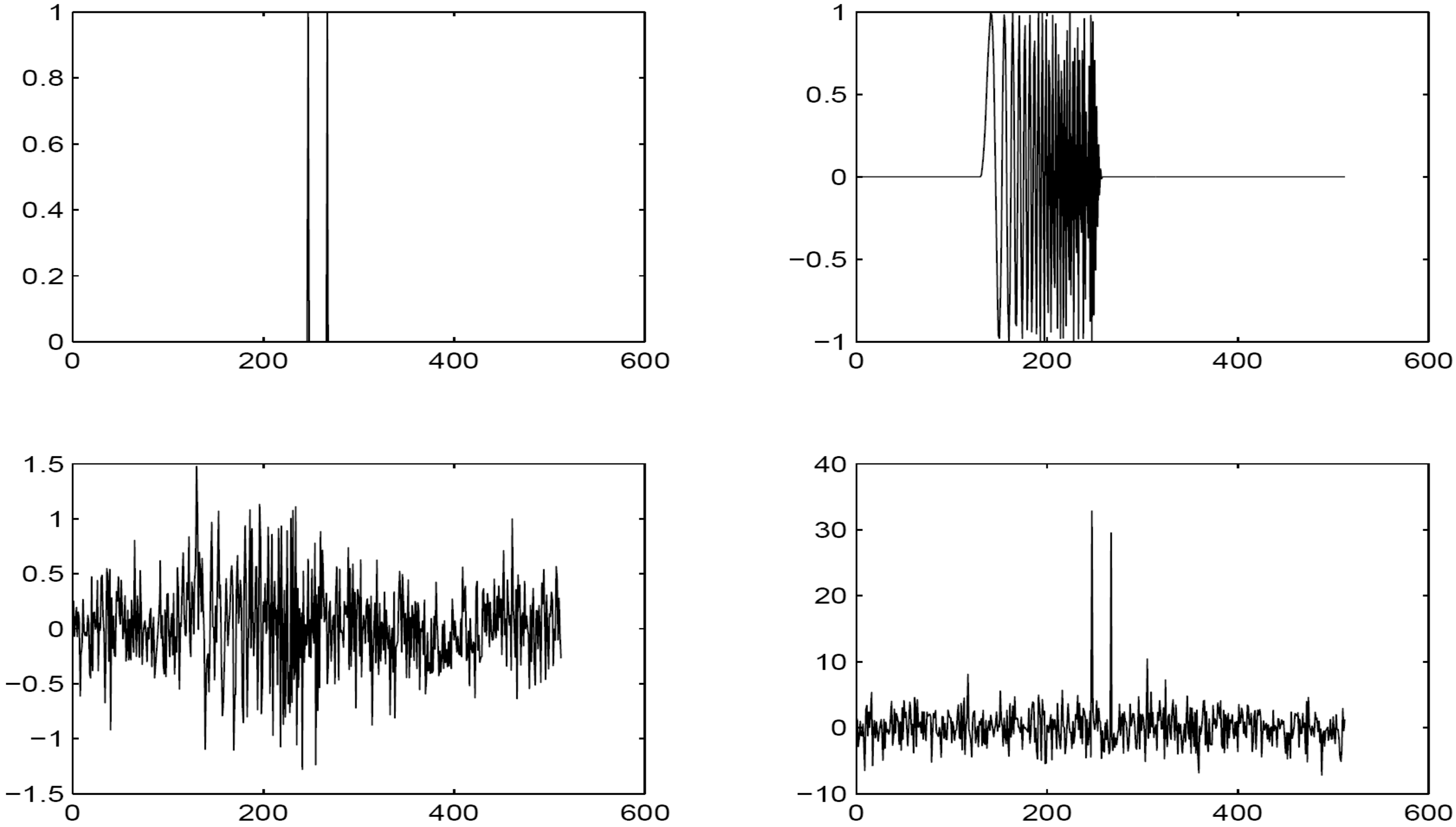
$$s(t) = \exp(i\alpha t^2) \otimes f(t) + n(t)$$

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

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

$$\|T\text{sinc}(\alpha T t) \otimes f(t)\| >> \|\exp(-i\alpha t^2) \odot n(t)\|$$

Graphical Example

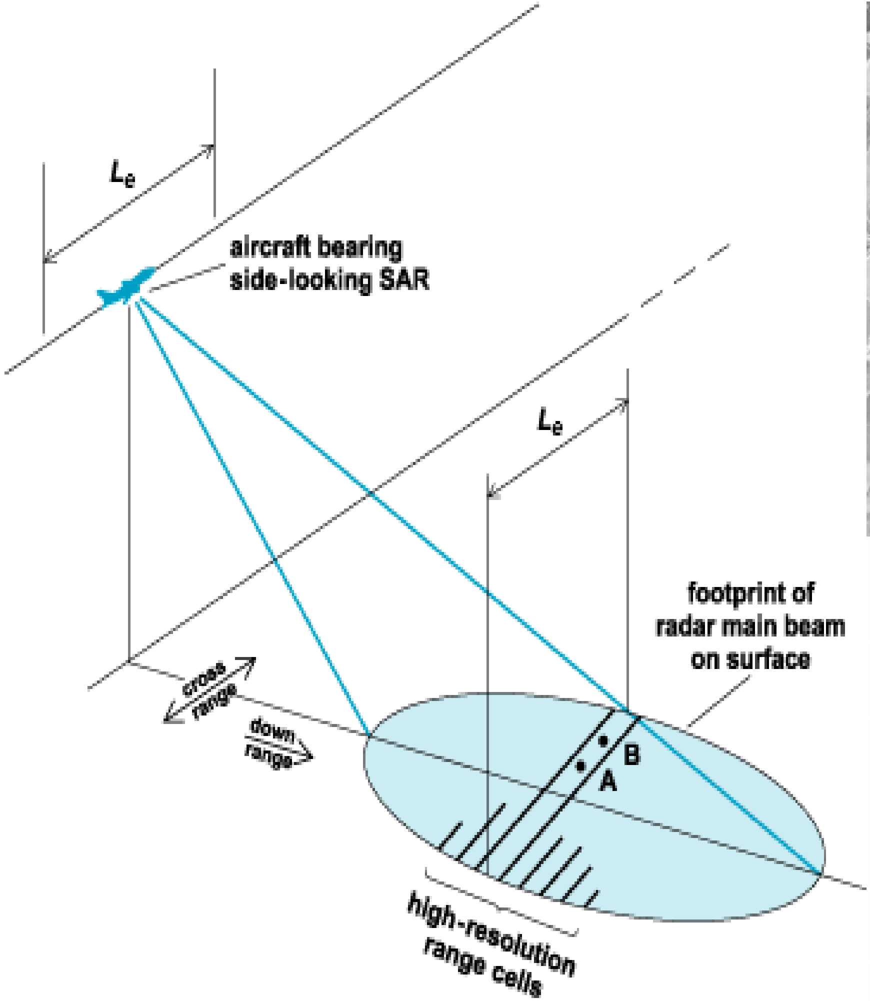


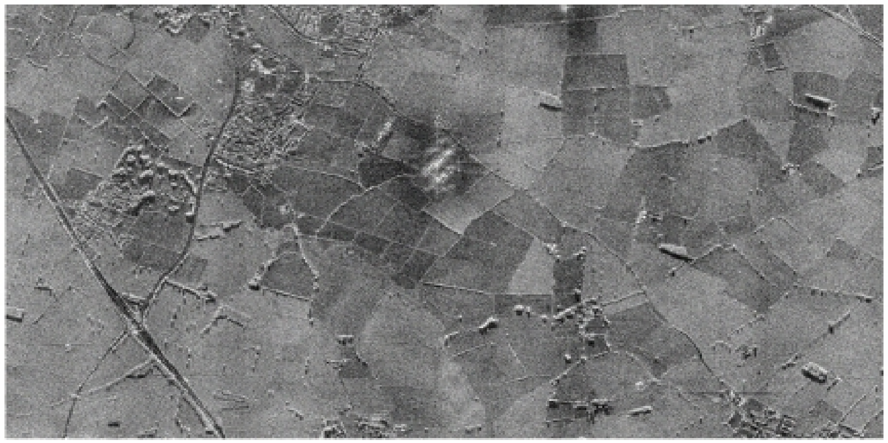
Why use Chirps ?

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

$$\hat{f}(t) \simeq T\text{sinc}(\alpha T t) \otimes f(t)$$

Microwave Imaging



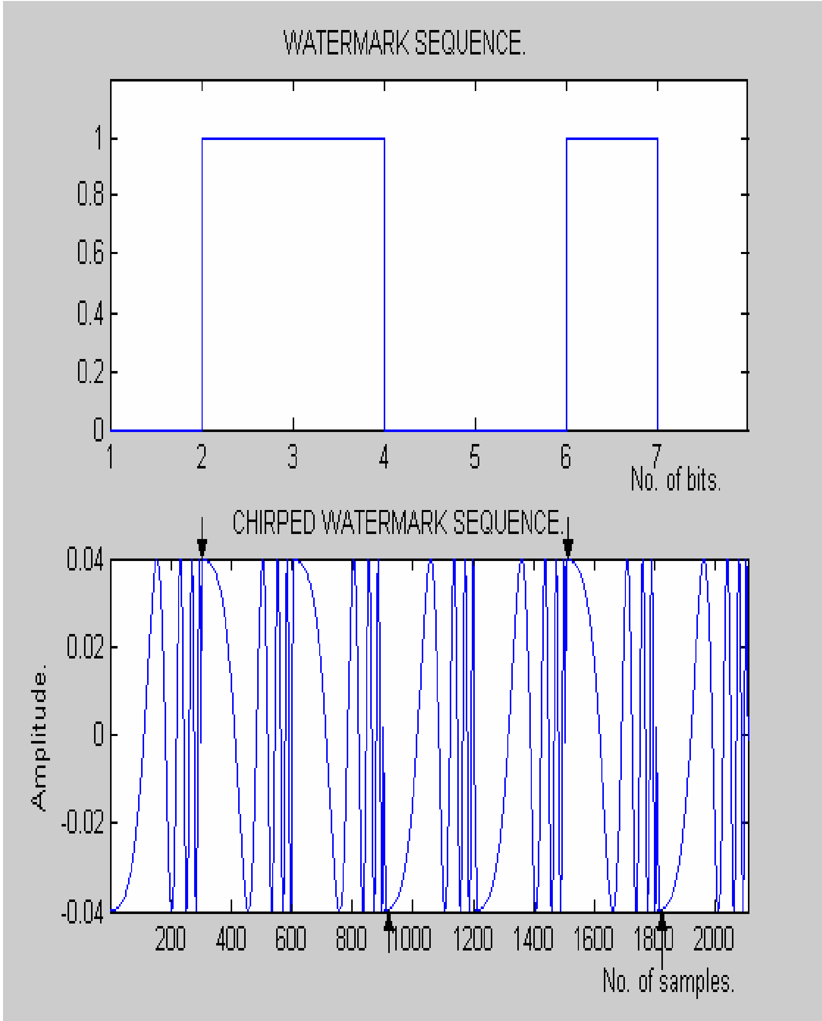


Chirp Coding

Binary code ...0110010...

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

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



Decoding

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

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: *The Problem*

$f(t)$ - audio signal
$w(t)$ - watermark obtained from the audio signal
$s(t)$ - watermarked signal

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

$$w(t) = \hat{T}f(t) \quad \text{and} \quad s(t) = f(t) + \hat{L}w(t)$$

such that

$$\|\hat{L}w(t)\| << \|f(t)\|$$

$$\hat{T}s(t) = w(t) \quad \text{and} \quad \hat{L}^{-1}s(t) = w(t)$$

Signal Coding (?) Chirp Coding (OK)

Signal Coding using the Wavelet Transformation

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

$$E_L = \frac{100}{E} \int \mid F_L(t) \mid^2 dt, \quad E = \sum_L E_L$$

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

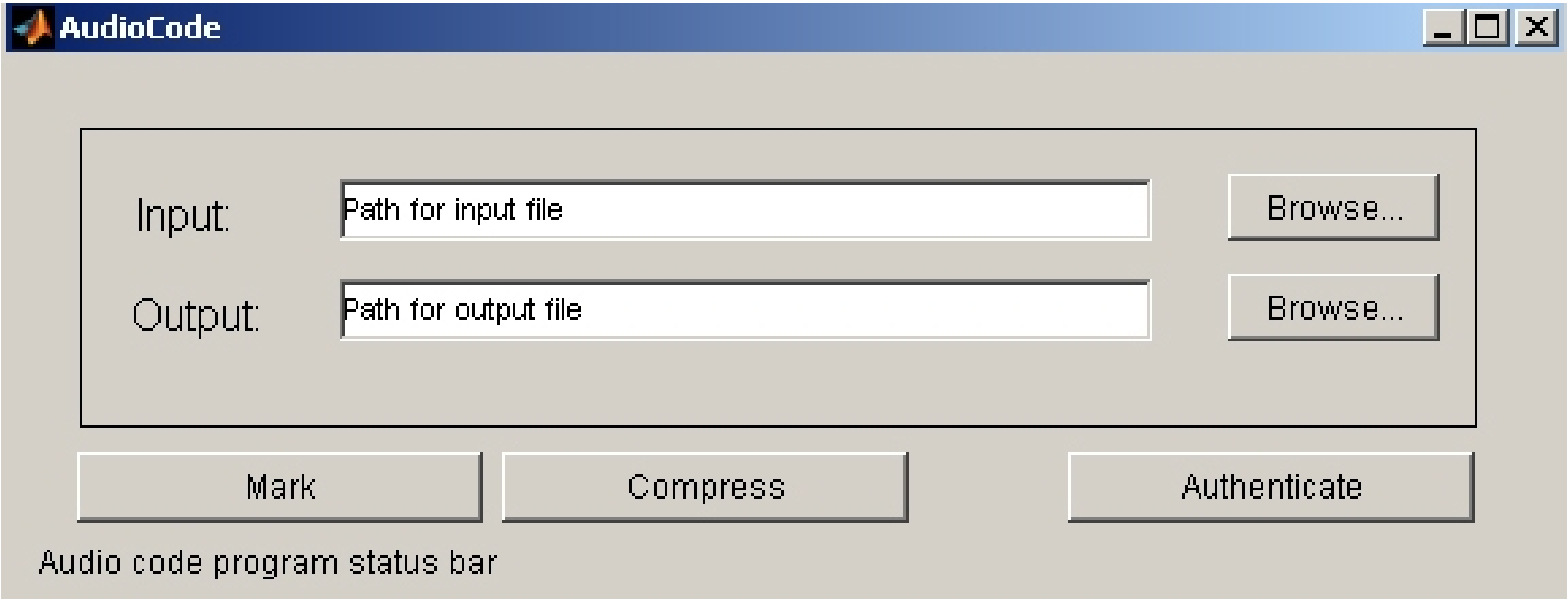
Chirp Coded

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

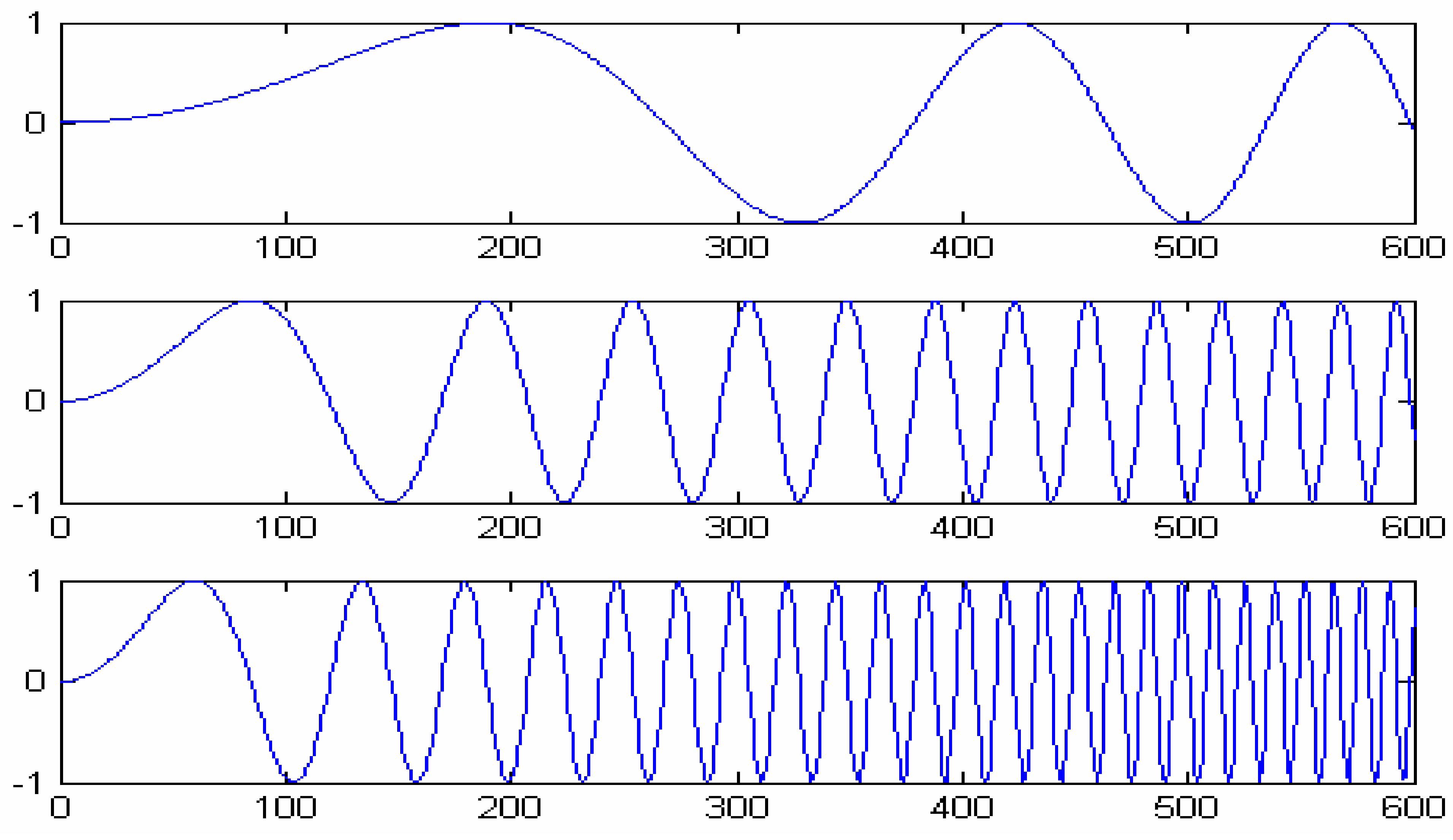
Dublin Institute Of Technology

ARG Audio Research Group

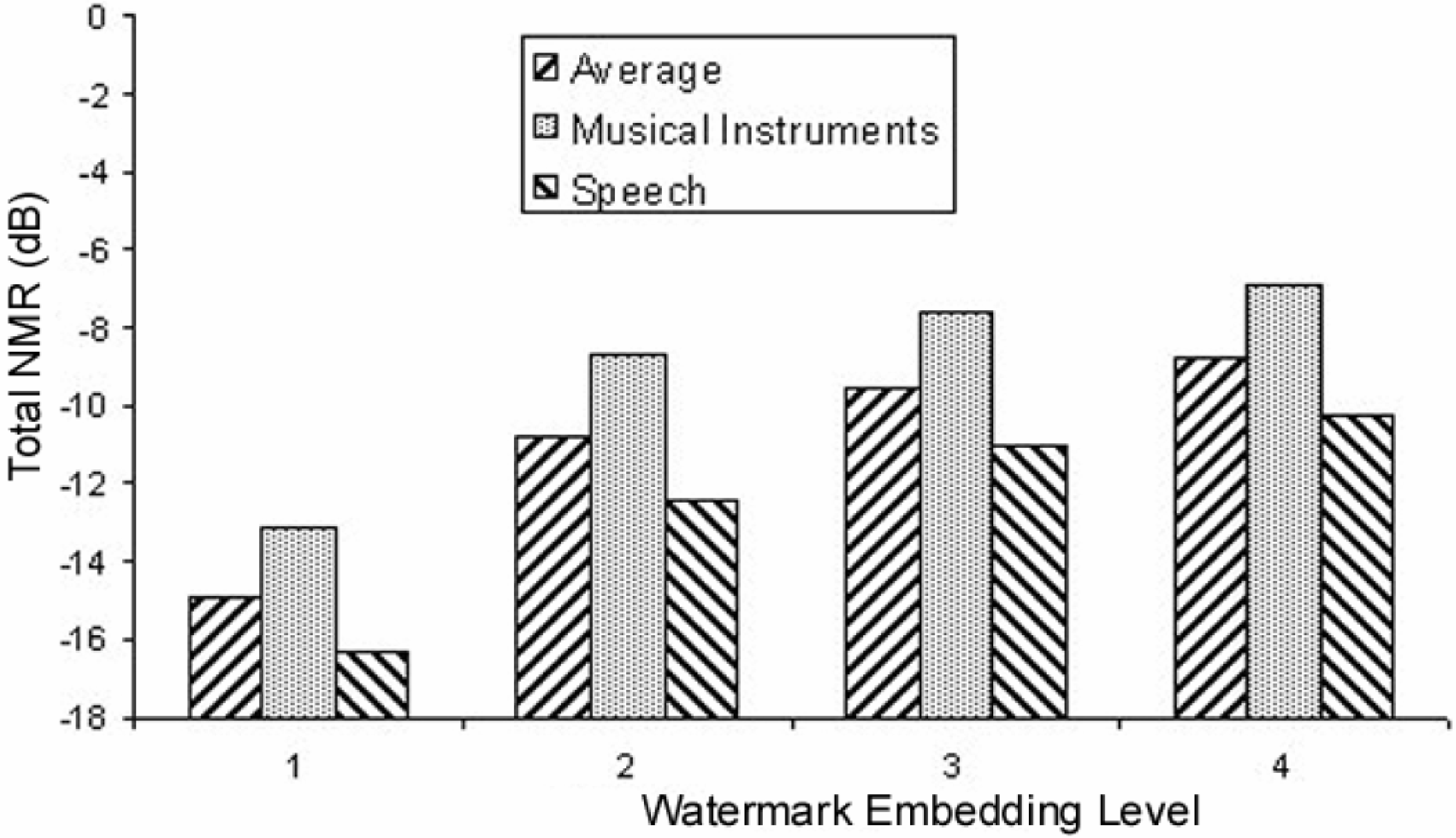
http://eleceng.dit.ie/arg/downloads/Audio_Self_Authentication.zip



Multilevel Watermarking



Perceptual Evaluation of Audio Quality: BS.1387



Commercial Applications

Technology to License

Hothouse
where business meets innovation

Self-authentication of Audio Data for Copyright Protection

ENTERPRISE IRELAND

BBC

Disney

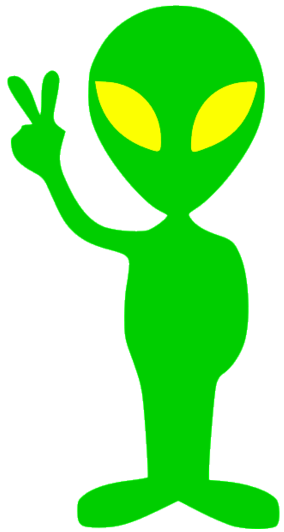
http://www.tamborine.co.uk

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

+

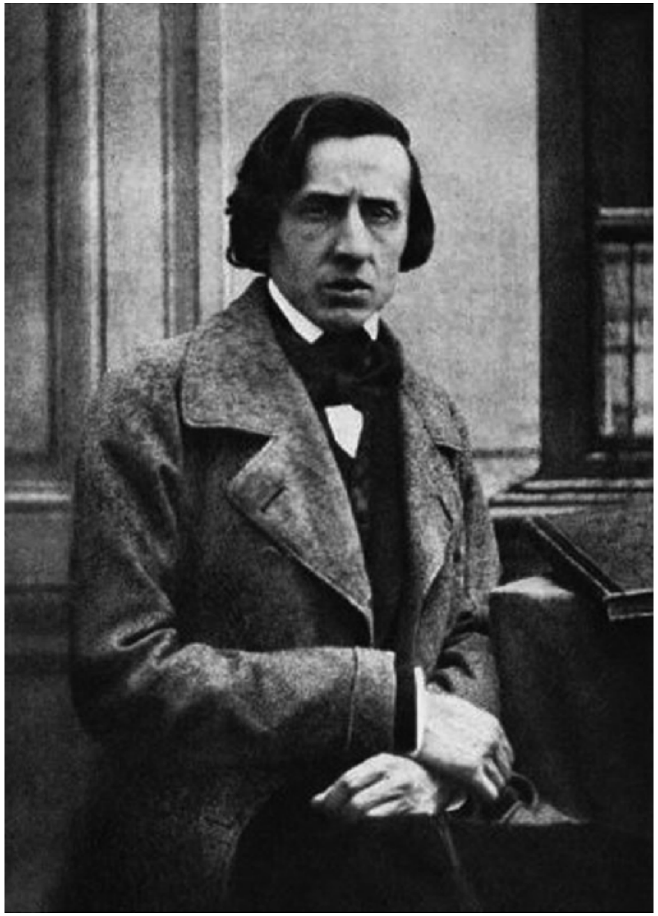
Interval (10 Minutes)

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



Information

Host Image

Retrieval

Basic Model

$$stegotext = ciphertext + covertext$$

$$ciphertext = cipher \otimes \otimes plaintext$$

$\otimes\otimes$ denotes the 2D convolution integral

- ***Ciphertext*** generated by process of ***Diffusion***
- ***Stegotext*** generated by process of ***Confusion***

Fresnel Diffusion

Consider a watermarking model given by

$$I_3(x, y) = rp(x, y) \otimes \otimes I_1(x, y) + I_2(x, y)$$

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

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

where $\odot\odot$ denote two-dimensional correlation.

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

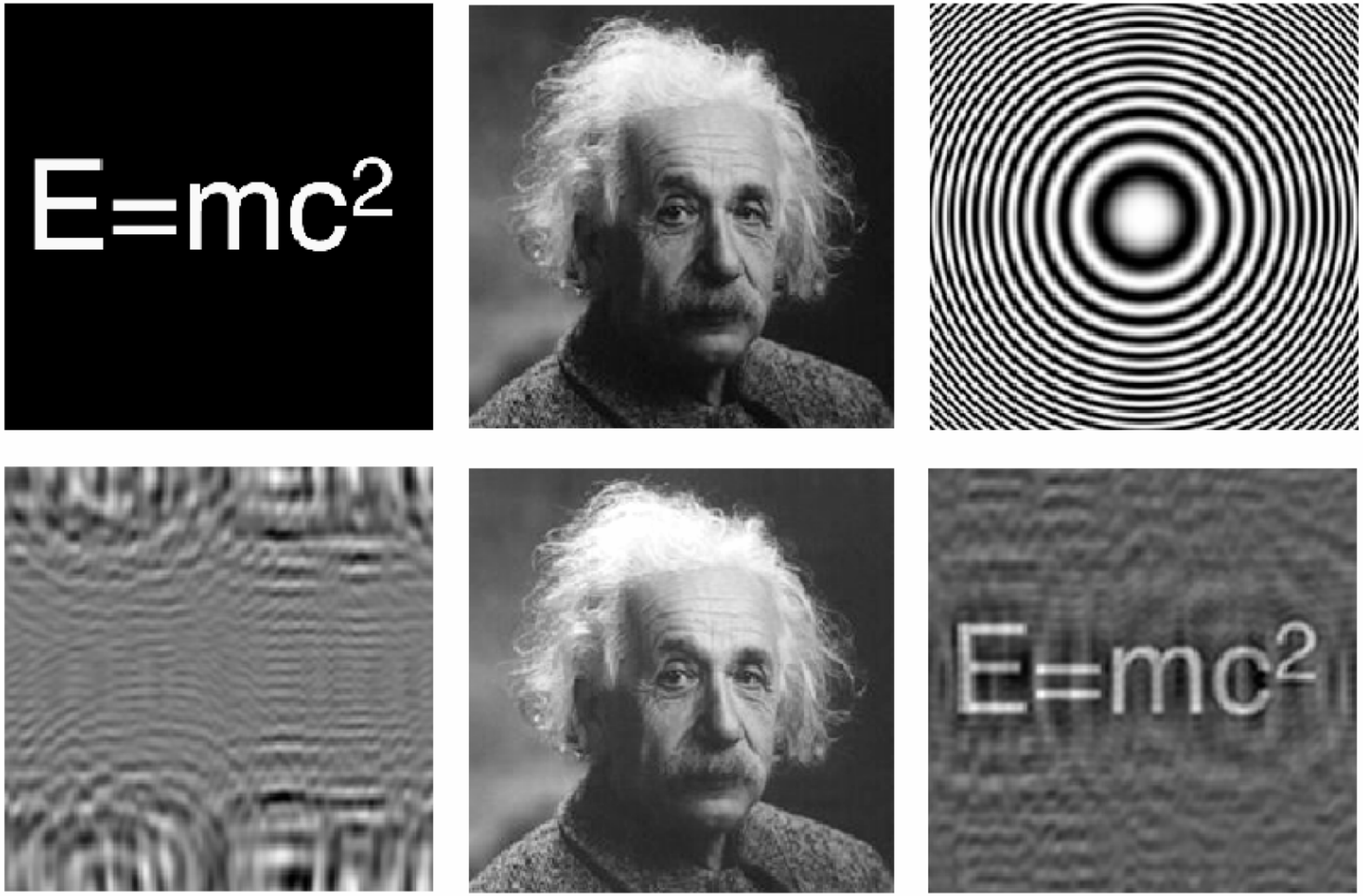
$$p \otimes\otimes f \iff PF$$

and

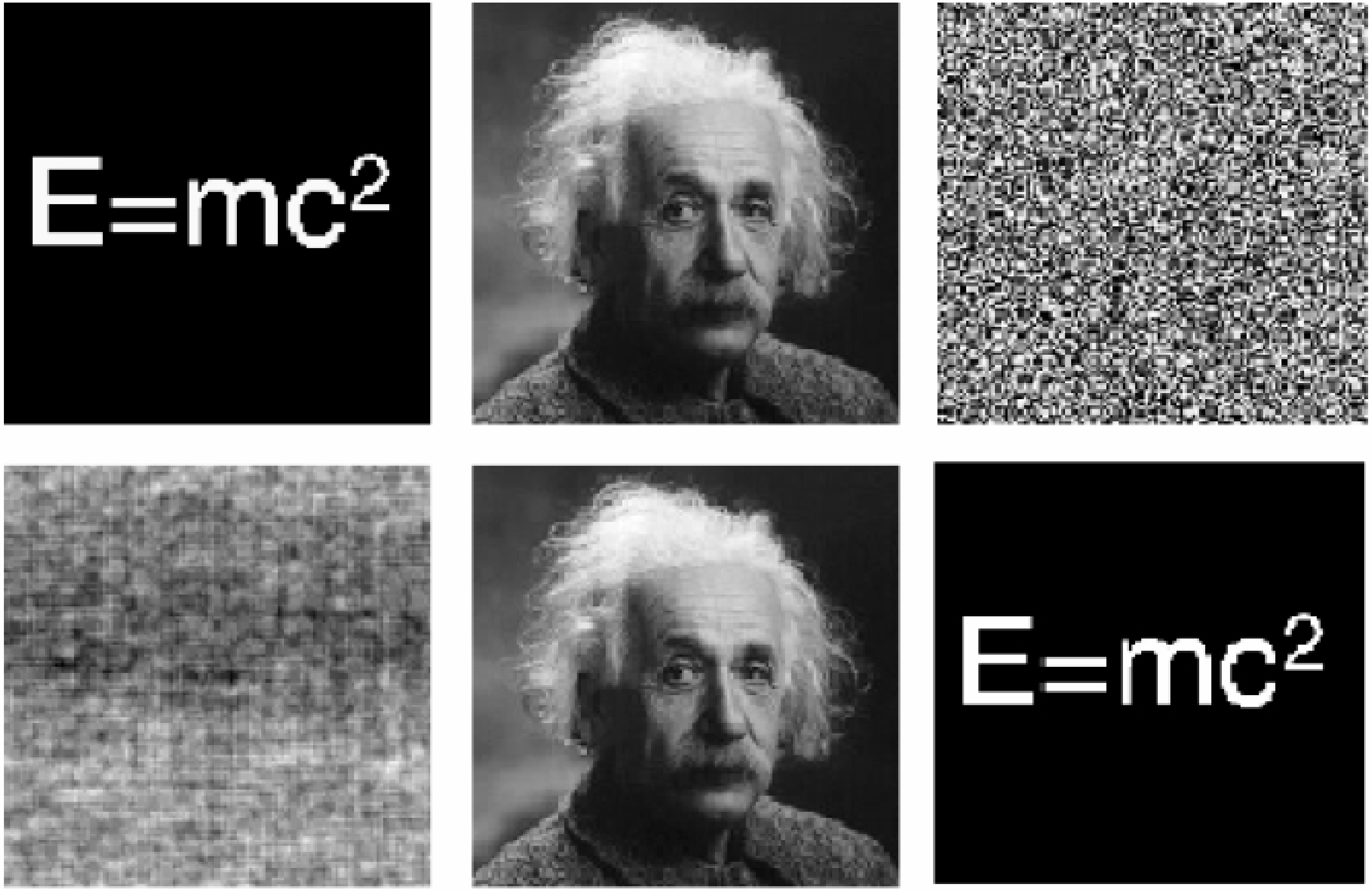
$$p \odot\odot f \iff P^* F$$

respectively, where $\iff$ denotes transformation from 'image space' to 'Fourier space'.

Example of Fresnel Watermarking



Stochastic Diffusion



How Does it Work? 1: *Data Diffusion*

Let $n(x, y)$ be a cipher with Fourier transform $N(k_x, k_y)$ and compute

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

so that the diffused field is given by

$$I(x,y) = m(x,y) \otimes \otimes I_0(x,y).$$

How Does it Work? 2:
Condition for Regularisation

$$\forall k_x, k_y$$

$$\text{if} \qquad | N(k_x, k_y) |^2 = 0$$

$$\text{then} \quad | N(k_x, k_y) |^2 = 1$$

How Does it Work? 3: *Data Retrieval*

$$n(x,y) \odot \odot I(x,y) \Longleftrightarrow N^*(k_x,k_y)\widetilde{I}(k_x,k_y)$$

and

$$N^*(k_x,k_y)\widetilde{I}(k_x,k_y) = N^*(k_x,k_y)M(k_x,k_y)\widetilde{I}_0(k_x,k_y)$$

$$= N^*(k_x,k_y)\frac{N(k_x,k_y)}{\mid N(k_x,k_y)\mid^2}\widetilde{I}_0(k_x,k_y) = \widetilde{I}_0(k_x,k_y)$$

so that

$$I_0(x,y) = n(x,y) \odot \odot I(x,y).$$

How Does it Work? 4: ***Covertext Model***

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

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

- *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

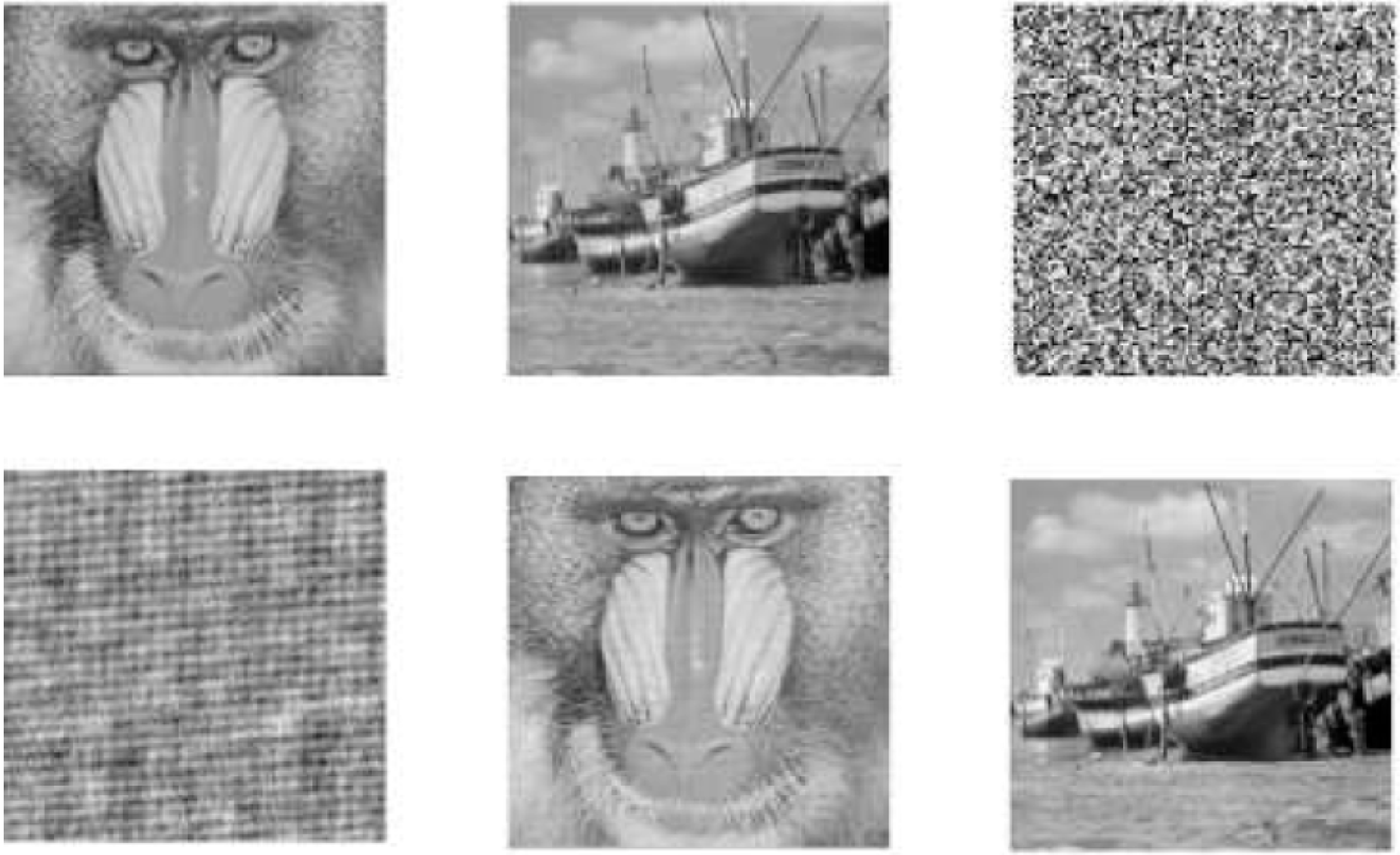
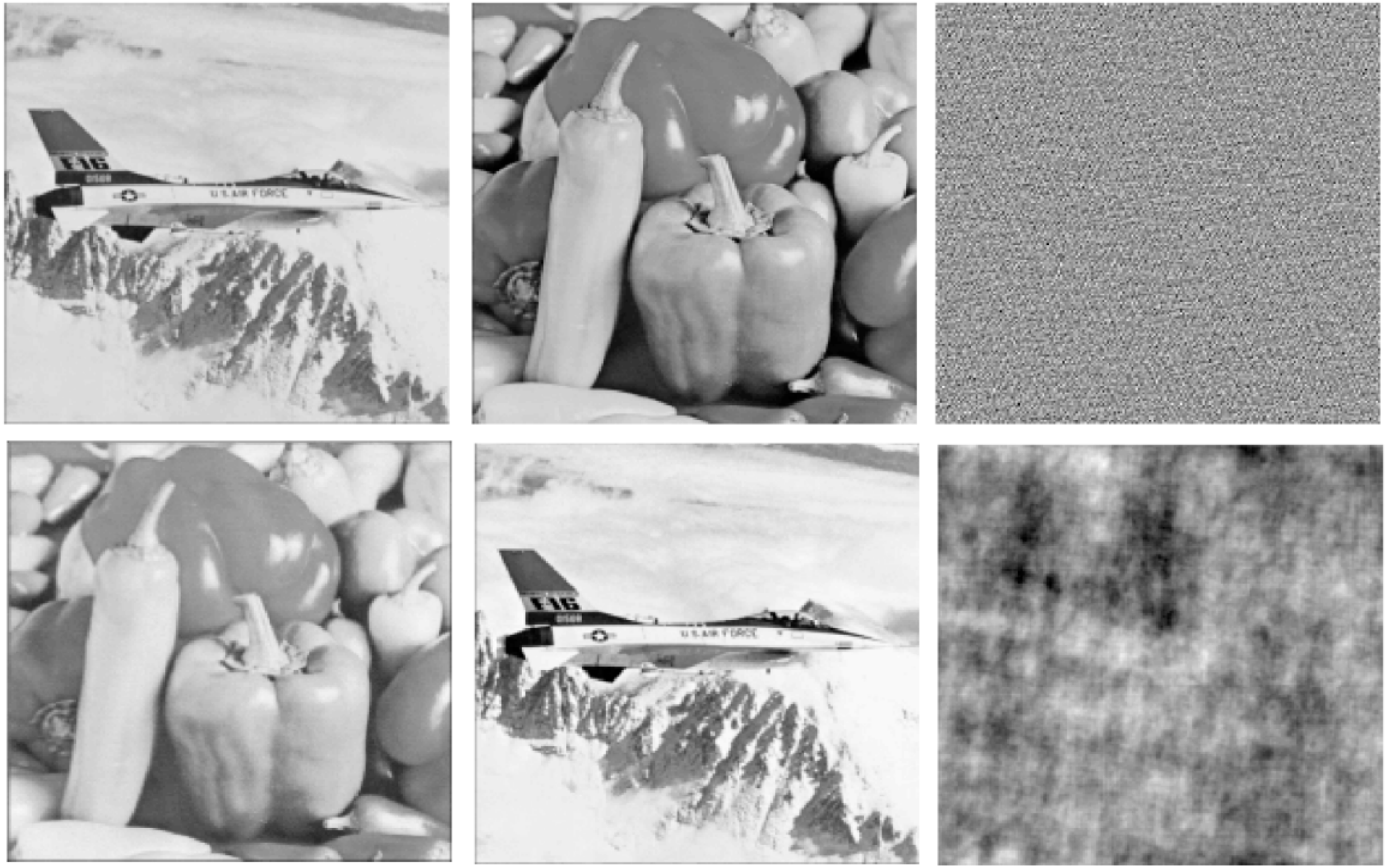


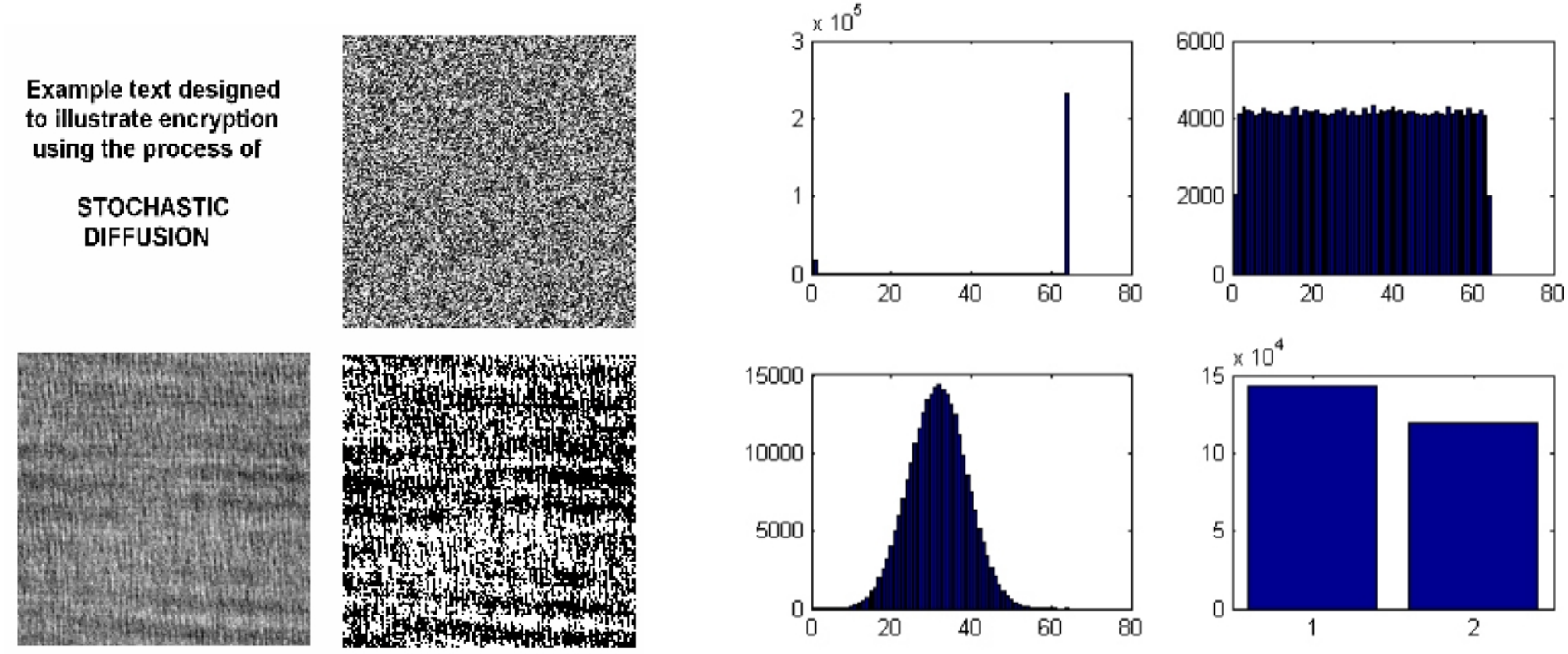
Image Data Diffusion



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



Principal Algorithms 1

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 planitext 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.

Principal Algorithms 2

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

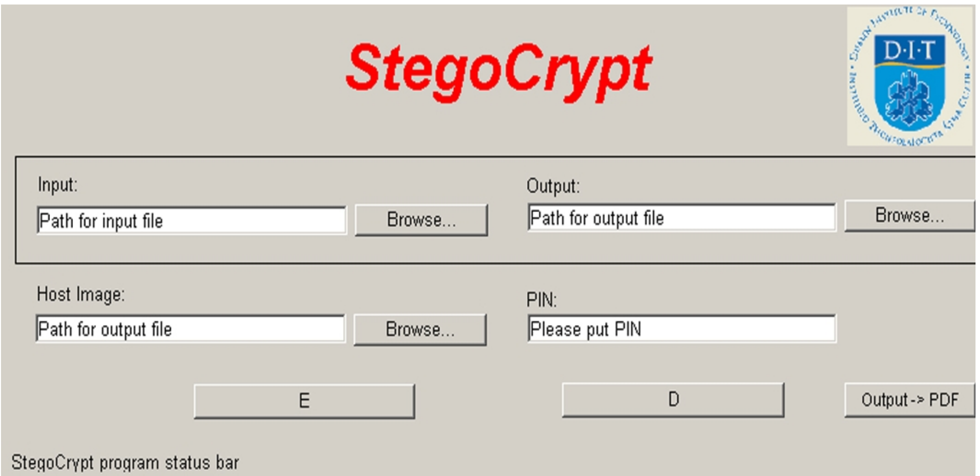
http://eleceng.dit.ie/arg/downloads/StegoCrypt.zip

Hothouse
where business meets innovation

Technology to License

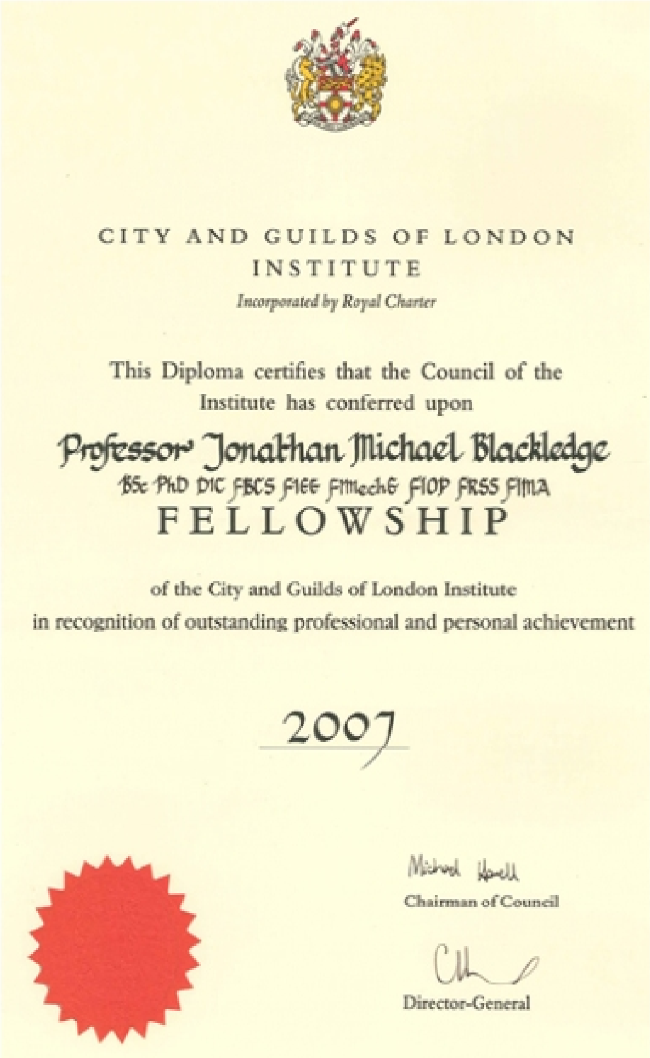
Document Authentication for Electronic Data Interchange

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



Encryption Mode	**Decryption Mode**
Inputs: Plaintext image Covertext image Private Key (PIN)	*Inputs:* Stegotext image Private key (PIN)
Output: Watermarked Covertext image	*Output:* Decrypted watermark
Operation: Encrypt by clicking on button E (for Encrypt)	*Operation:* Decrypt by clicking on button D (for Dycrypt)

Authentication of e-Certificates


CITY AND GUILDS OF LONDON INSTITUTE

Incorporated by Royal Charter

This Diploma certifies that the Council of the Institute has conferred upon

Professor Jonathan Michael Blackledge

BSc PhD DIC FBCS FIEE FIMechE FIOP FRSS FIMA

FELLOWSHIP

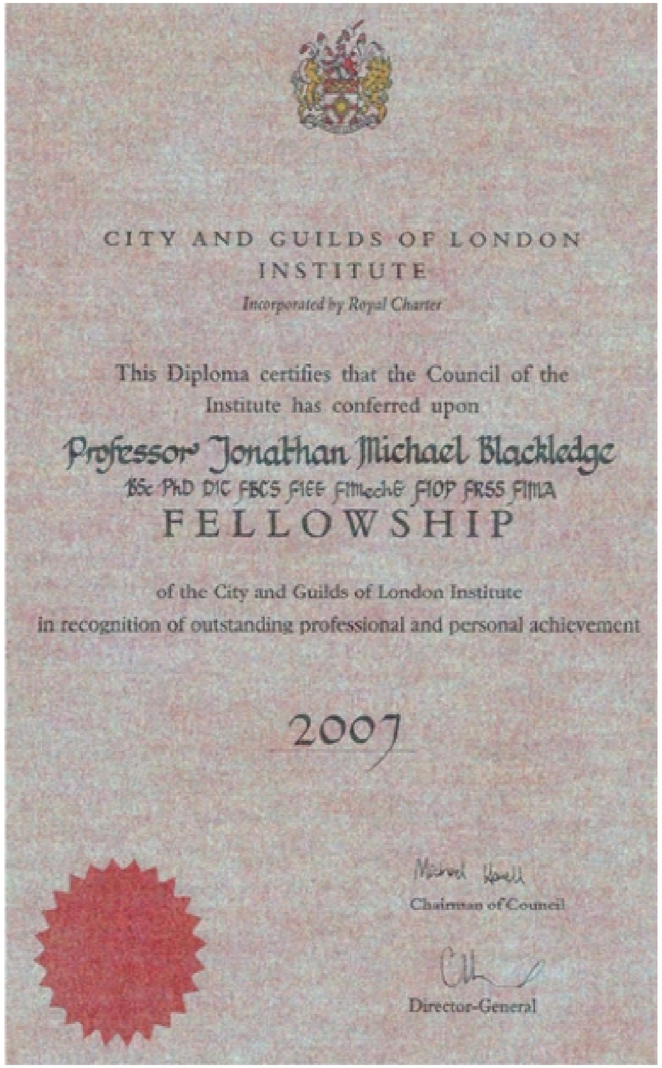
of the City and Guilds of London Institute

in recognition of outstanding professional and personal achievement

2007

Chairman of Council

Director-General


CITY AND GUILDS OF LONDON INSTITUTE

Incorporated by Royal Charter

This Diploma certifies that the Council of the Institute has conferred upon

Professor Jonathan Michael Blackledge

BSc PhD DIC FBCS FIEE FIMechE FIOP FRSS FIMA

FELLOWSHIP

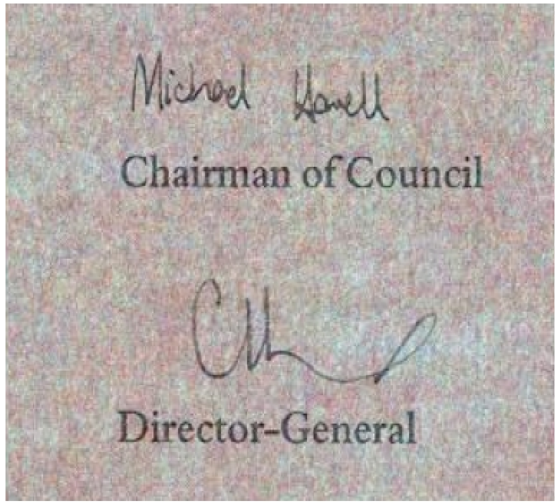
of the City and Guilds of London Institute

in recognition of outstanding professional and personal achievement

2007

Chairman of Council

Director-General



Authentication of e-Letters


School of Electrical Engineering Systems, Faculty of Engineering

Dublin Institute of Technology
Institiúid Teicneolaíochta Bhaile Átha Cliath

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

Dublin Institute of Technology
Kevin Street, Dublin 8, Ireland

science foundation ireland
fondúireacht eolaíochta éireann

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


School of Electrical Engineering Systems, Faculty of Engineering

Dublin Institute of Technology

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


SCHOOL OF ELECTRICAL ENGINEERING SYSTEMS, FACULTY OF ENGINEERING

DIT DUBLIN INSTITUTE of TECHNOLOGY
Institiúid Teicneolaíochta Bhaile Átha Cliath

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

Dublin Institute of Technology
Kevin Street, Dublin 8, Ireland

sfi
science foundation ireland
fondúireacht eolaíochta éireann

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

cc: Prof Eugene Coyle
Dr Marek Rebow

4 August, 2009

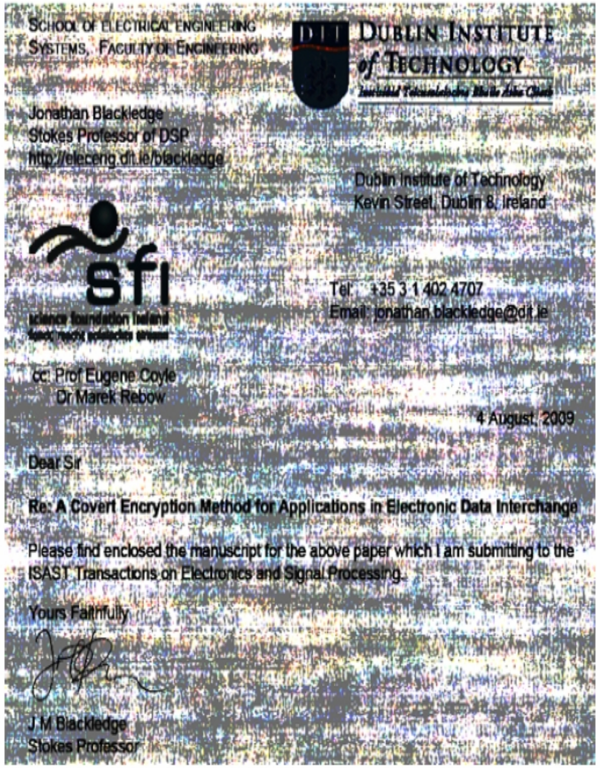
Dear Sir

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


SCHOOL OF ELECTRICAL ENGINEERING SYSTEMS, FACULTY OF ENGINEERING

DIT DUBLIN INSTITUTE of TECHNOLOGY

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

Dublin Institute of Technology
Kevin Street, Dublin 8, Ireland

sfi
science foundation 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


SCHOOL OF ELECTRICAL ENGINEERING SYSTEMS, FACULTY OF ENGINEERING

DIT DUBLIN INSTITUTE of TECHNOLOGY
Institiúid Teicneolaíochta Bhaile Átha Cliath

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

Dublin Institute of Technology
Kevin Street, Dublin 8, Ireland

sfi
science foundation ireland
fondúireacht eolaíochta éireann

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

MS Word

(Format→Background→Fill Effect...)

(Format→Background→Printed Watermark...)

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 secrete information) and encrypt the result

- ***Cribb Camouflage***

- ***Covert Key Exchange***

Hardcopy Authentication using Stochastic Diffusion

- The covertext model

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

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

$$I(x,y) = m(x,y) \otimes \otimes I_0(x,y)$$ ***Texture Coding***

Print/Scan Cycle

$$I_{\text{print}} = p_{\text{print}} \otimes \otimes m \otimes \otimes I_0$$

$$I_{\text{scan}} = p_{\text{scan}} \otimes \otimes I_{\text{print}}$$

Because convoution is ***commutative***

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

$$= m \otimes \otimes p_{\text{scan/print}} \otimes \otimes I_0$$

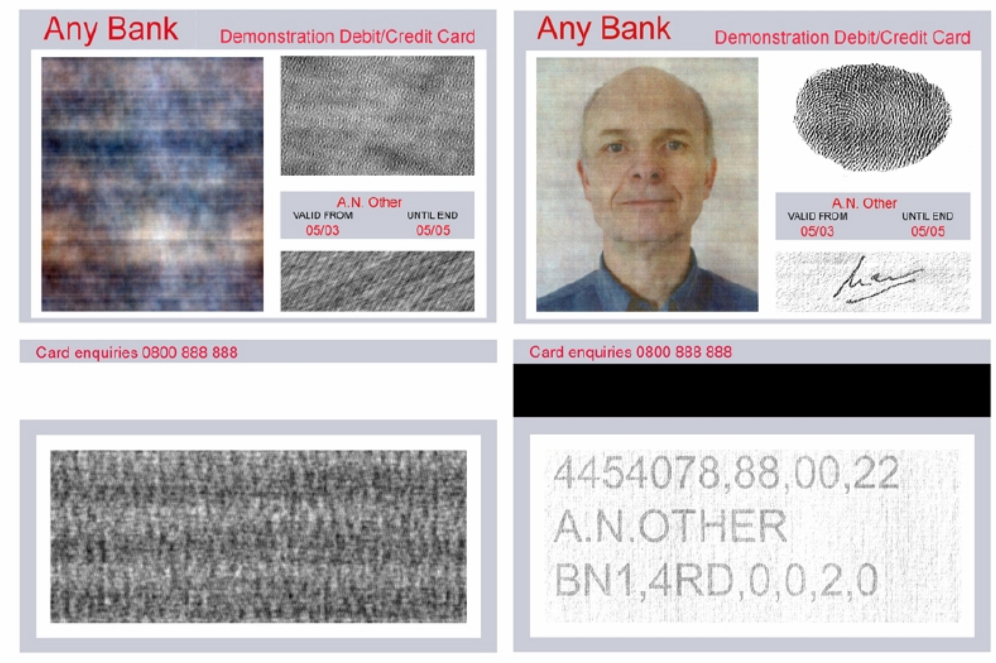
Conditions Required for Hidden Data Retrieval

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

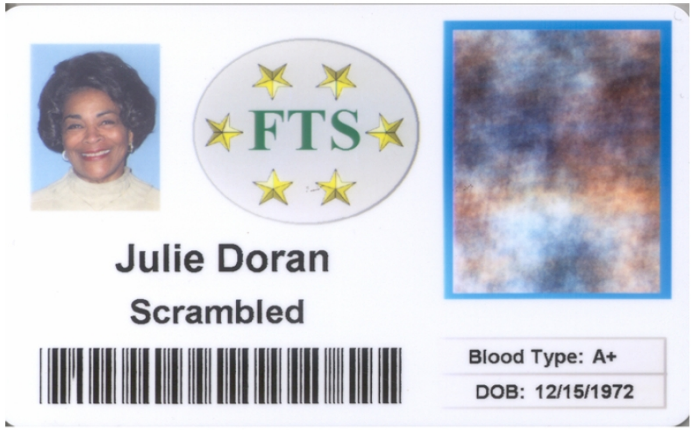
- Fidelity of the reconstruction critically depends on:
  - orientation
  - cropping

- Method is robust to ***hardcopy soiling***

Applications of Texture Coding 1:
Identity Cards

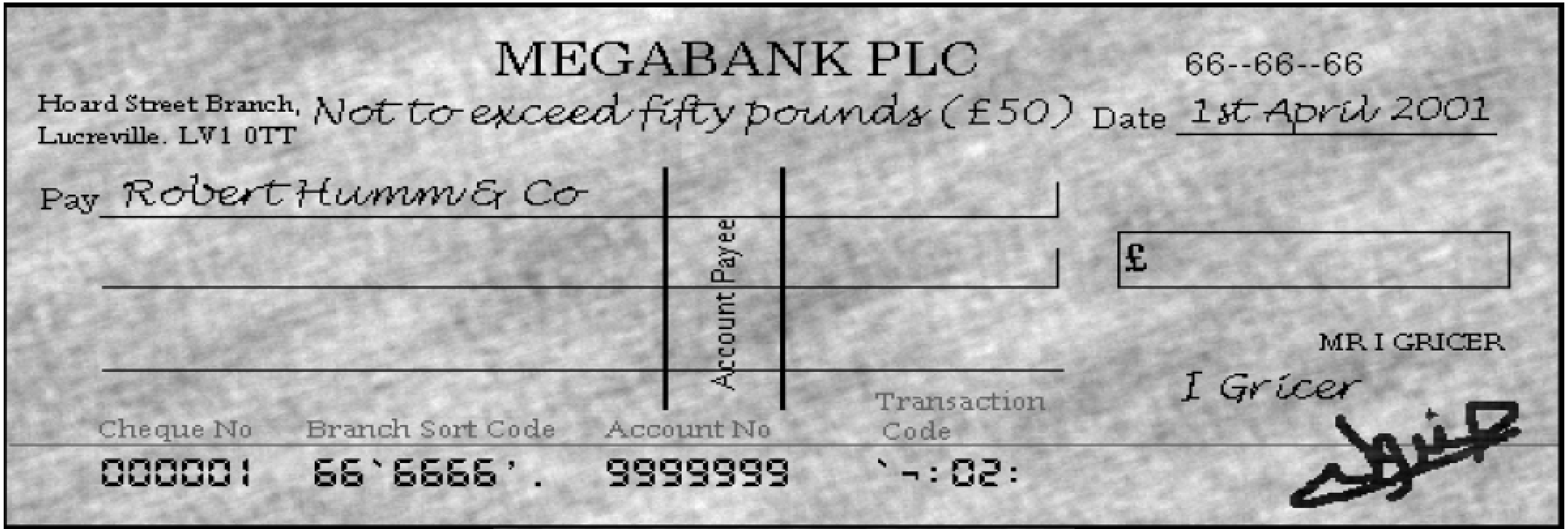


Printed at 600dpi; scanned with flat-bed scanner at 300dpi

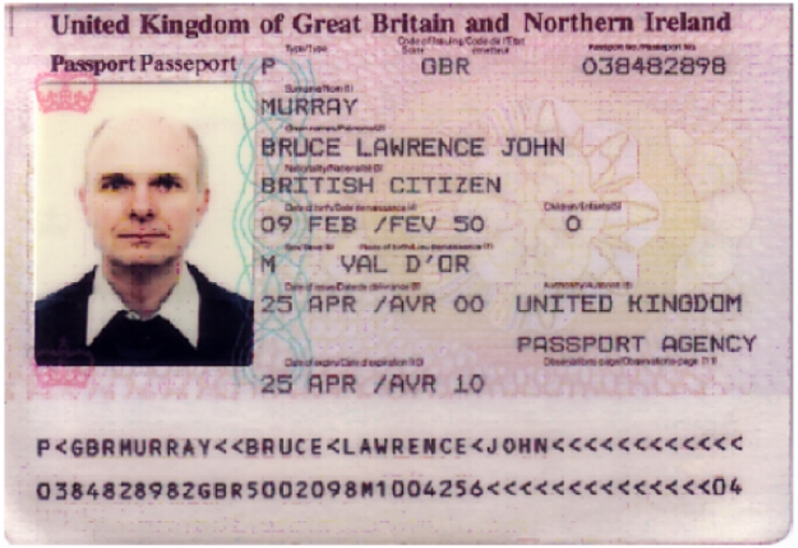


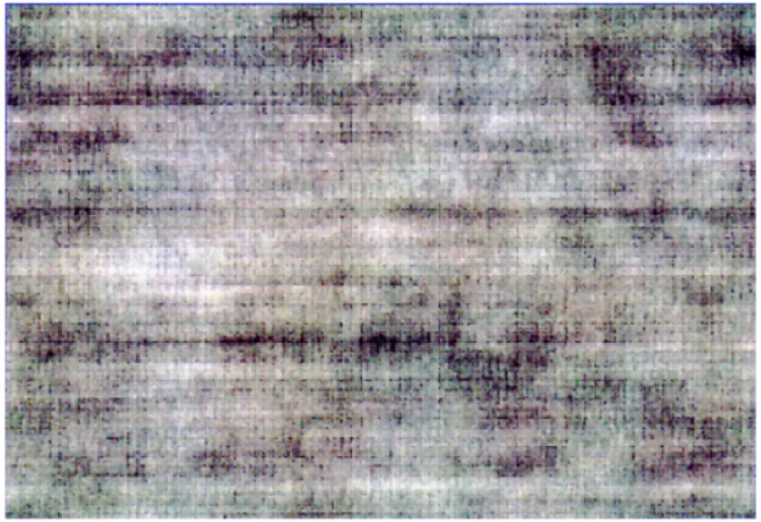
Printed at 600dpi; scanned with mobile phone camera

Applications of Texture Coding 2:
Signature Authentication



Applications of Texture Coding 3: ***Passport Authentication***

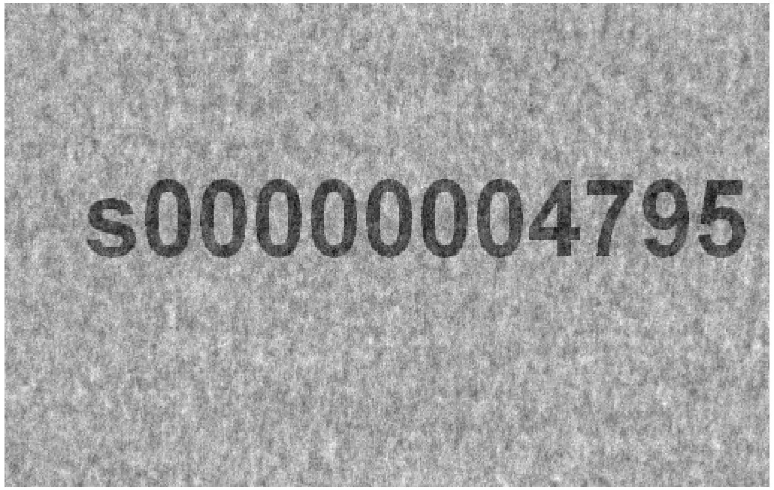


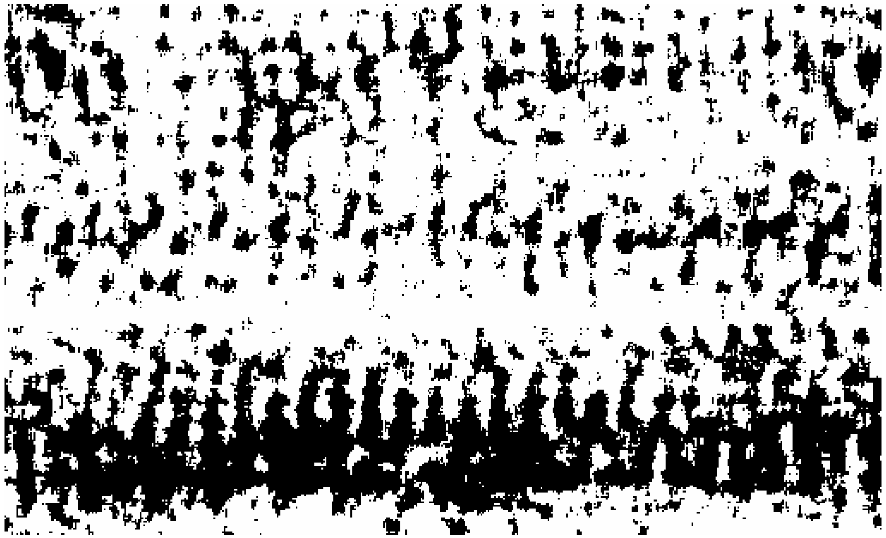


Printed at 400dpi;

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 at 300dpi under UV lamp

Applications of Texture Coding 5: *Statistical Authentication*

0010000 680009162602 00 000000

ANY UNITED STATES PERSON WHO HOLDS THIS OBLIGATION WILL BE SUBJECT TO LIMITATIONS UNDER THE UNITED STATES INCOME TAX LAWS, INCLUDING THE LIMITATIONS PROVIDED IN SECTIONS 165(j) AND 1287(a) OF THE INTERNAL REVENUE CODE, AS AMENDED.

U.S.$10,000

United Kingdom

U.S.$2,500,000,000 Floating Rate Notes Due 1992

SPECIMEN

This Note forms one of an issue of Floating Rate Notes [illegible] "Notes") in the aggregate principal amount of U.S.$2,500,000,000 [illegible] Paying Agency Agreement (the "Paying Agency Agreement") [illegible] and made between the Lords Commissioners of Her Majesty's [illegible] ("H.M. Treasury") on behalf of the Government of the United Kingdom [illegible] Northern Ireland, Morgan Guaranty Trust Company of [illegible], as [illegible] paying agent and the paying agents, registrar and transfer [illegible] The Notes are subject to, and have the benefit of, the [illegible] and the Terms and Conditions endorsed hereon.

H.M. Treasury, [illegible] promises to pay the bearer of this Note on the Interest Payment Date (as [illegible] Condition 4) falling in October 1992 or on such earlier date as the principal sum [illegible] mentioned may become repayable in accordance with the said Terms and Conditions, the principal sum of:—

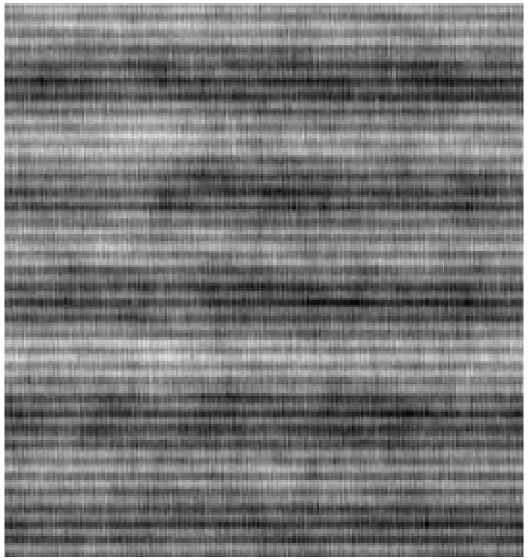
U.S.$10,000 (Ten thousand United States dollars)

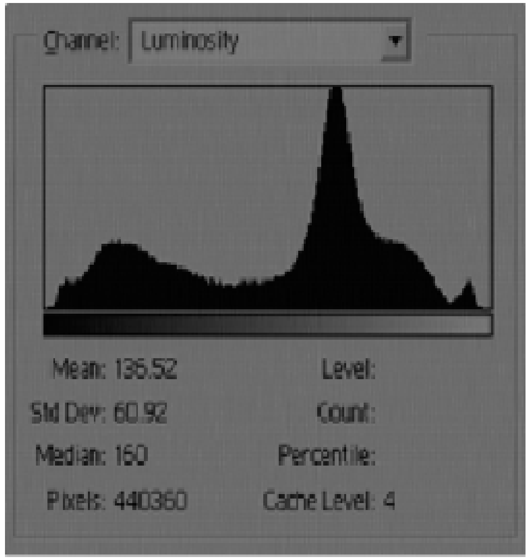
together with interest on the said principal sum from 7th October, 1985 calculated by reference to the rates from time to time applicable thereto, as determined in accordance with the provisions of Condition 4, and payable on each Interest Payment Date, subject to and in accordance with the said Terms and Conditions.

IN WITNESS whereof H.M. Treasury has caused this Note to be signed in facsimile on its behalf by Sir Peter Middleton, Permanent Secretary to H.M. Treasury.

For THE LORDS COMMISSIONERS OF HER MAJESTY'S TREASURY

Dated as of 7th October, 1985

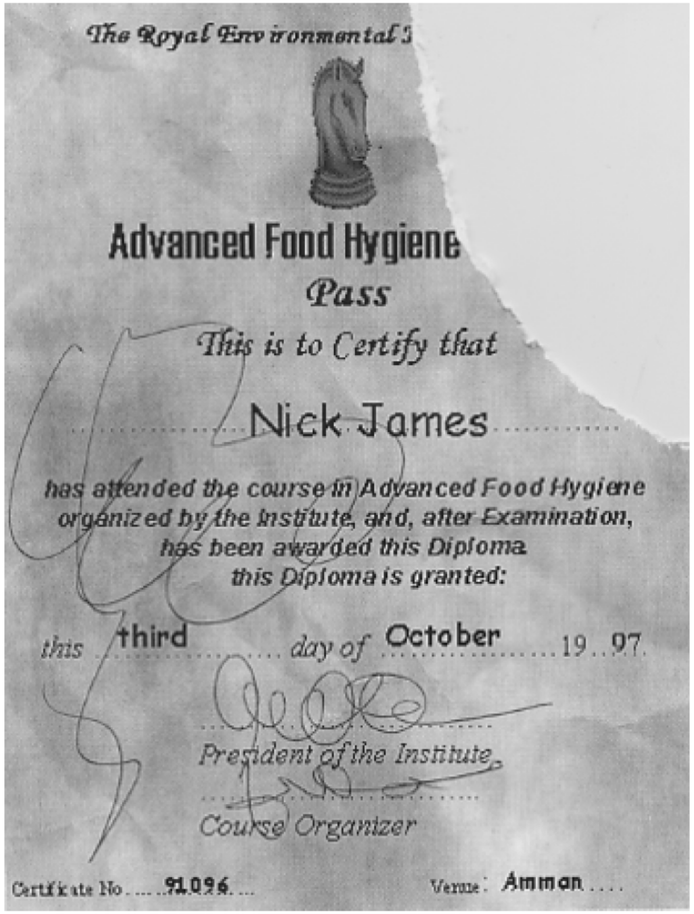




Texture code generated of basic statistics associated with a scan of a high value bank bond and printed on the back of the bond at 300dip; flat-bed scanned at 150dpi

Attack and Robustness Analysis

Printed Document Authentication using Texture Coding,
J M Blackledge and K W Mahmoud, International Society for Advanced Science and Technology, Transactions on Electronics and Signal Processing, No. 1, Vol. 4, 81-98, 2009; http://eleceng.dit.ie/papers/135.pdf


The Royal Environmental S

Advanced Food Hygiene

Pass

This is to Certify that

Nick James

has attended the course in Advanced Food Hygiene organized by the Institute, and, after Examination, has been awarded this Diploma
this Diploma is granted:

this third day of October 19 97

President of the Institute

Course Organizer

Certificate No ....91096....   Venue: Amman ....

Summary

- Fundamental steganographic model

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

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***

Summary (Continued)

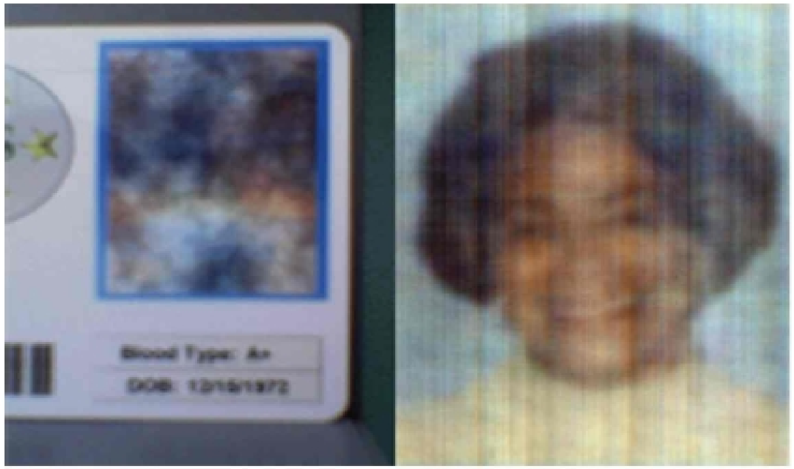
- ***Diffusion + Confusion*** model suitable for ***electronic-to-electronic (e-to-e)*** applications

- 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 CRYPTOMED



Q & A