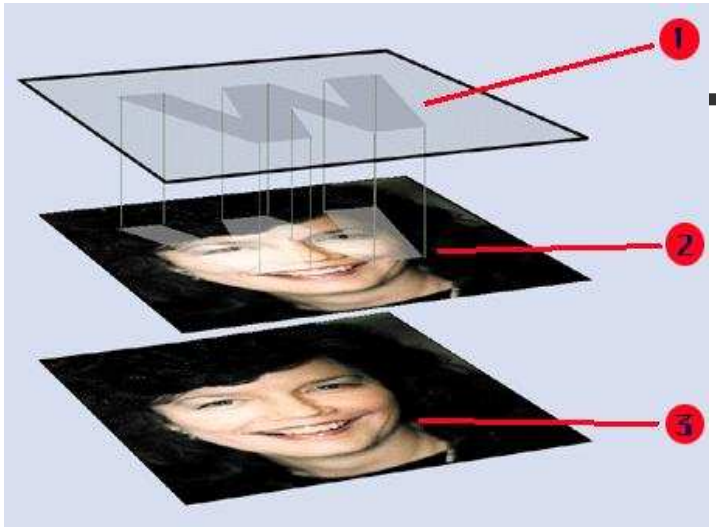
Networks security

Jean-Yves Antoine
LI - Université François Rabelais de Tours
Jean-Yves.Antoine AT univ-tours.fr



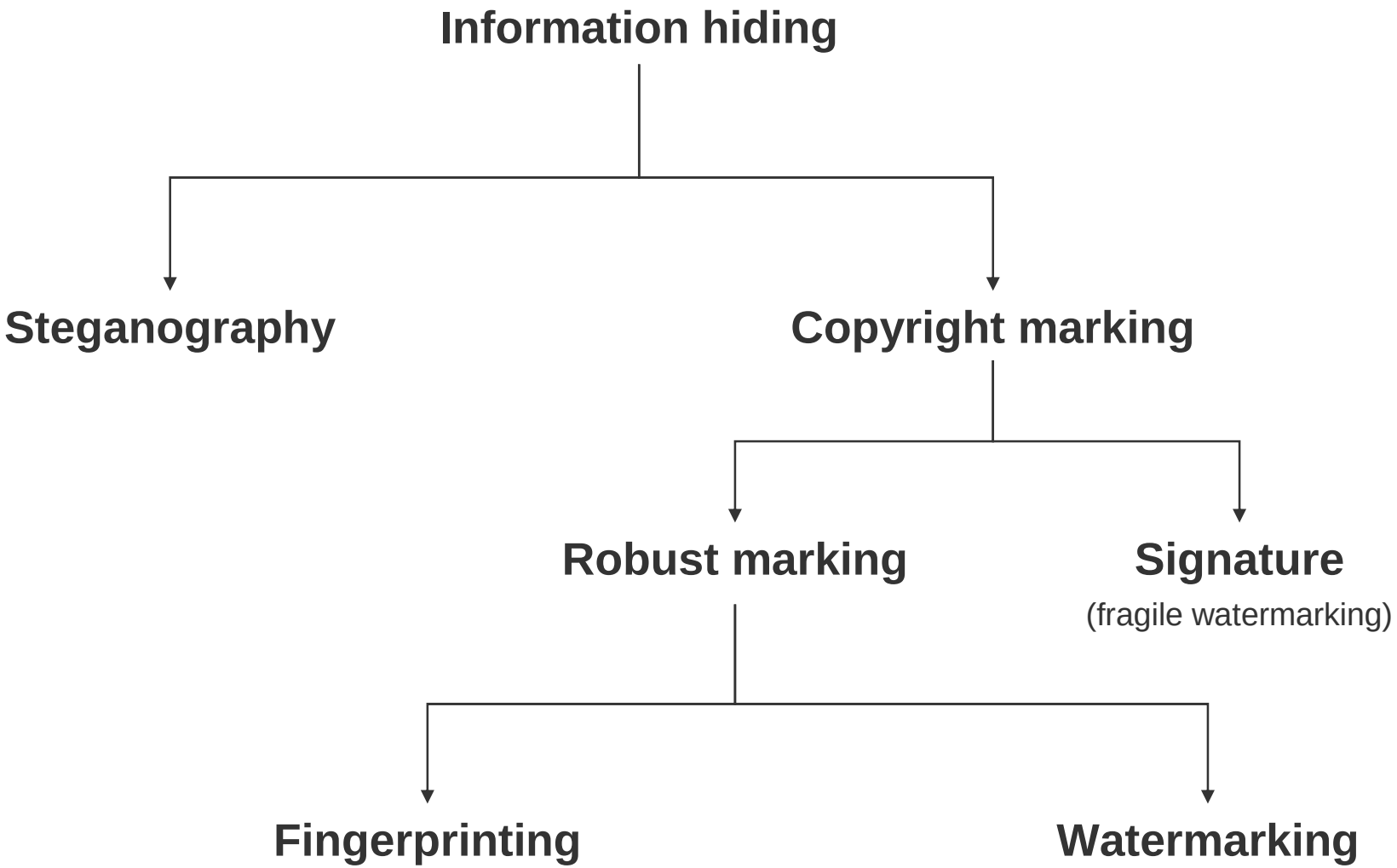
Source : Byte

Networks security

Information hiding : steganography and watermarking

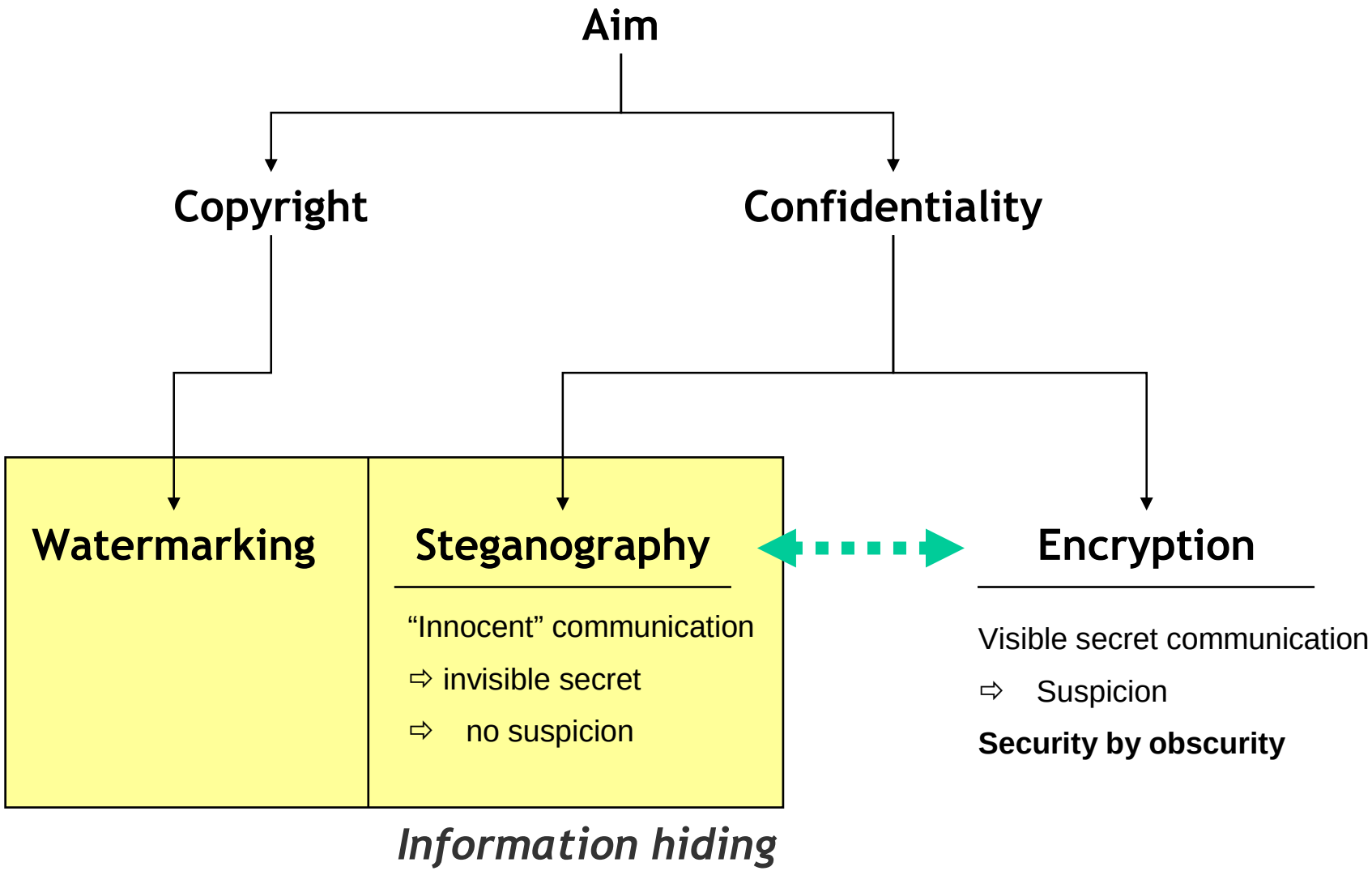
UNIVERSITÉ FRANÇOIS - RABELAIS TOURS

Introduction



Source: adapted from [Pfitzmann 1996]

Information hiding vs. encryption



An old history…

Camouflage (physical steganography)

Antic Greece (from Herodotus)

- Histiaeus shaved the head of his slave and tattooed it with a message which disappeared after the hair had regrown ⇨German spies during WW1
- Demeratus warned Sparta of an invasion by Xerxes (Persian king) by removing the wax from a writing tablets, wrote his message on the wood underneath and then covered it with wax again.

Rennaissance

- Discovery of the perspective rules (Alberti, Brunelleschi) ⇨**anamorphosis**

  Example : *Vexierbild* (Shö, 1530s)

Modern times

- Invisible inks (WW1 & WW2 : invisible ink to print very small dots on letters)

  ↳ **current** : bank notes marking

- Microphotography : Brewster (1857), René Dragon (1870 : Paris siege) were able to print messages “in spaces no larger than a small dot”

  ↳ **current** : microfilms

An old history…

Linguistic steganography

Acrostics

– Giovanni Boccacio (1313-1375) : *Amorosa visione*

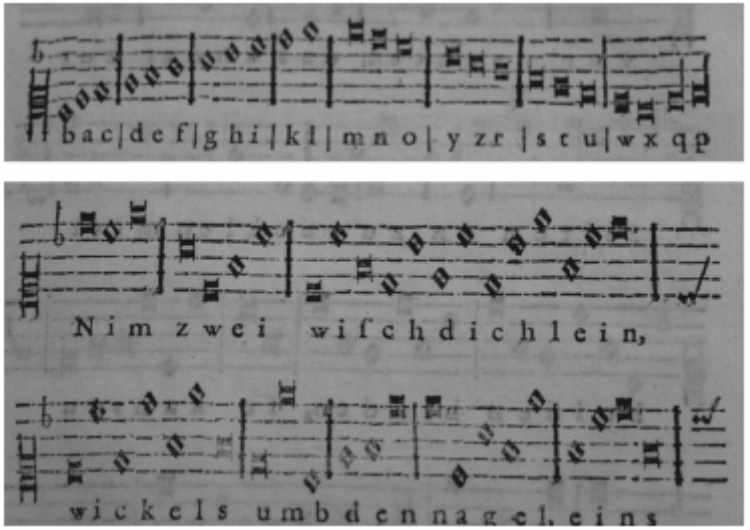
Renaissance

– Johannes Trithemius (1462-1516) : *Steganographiae*

  Corresponding tables between letters and words

– Gaspar Schott (1608-1666) : *Schola Steganographia*

  Corresponding tables between letters and music notes



… but a recent technologies

Nowadays : digital steganography

Recent area of research

- First academic conference in 1996 [Anderson, 1996]
- Increasing number of publications
- Numerous different approaches

Industry : copyright marking

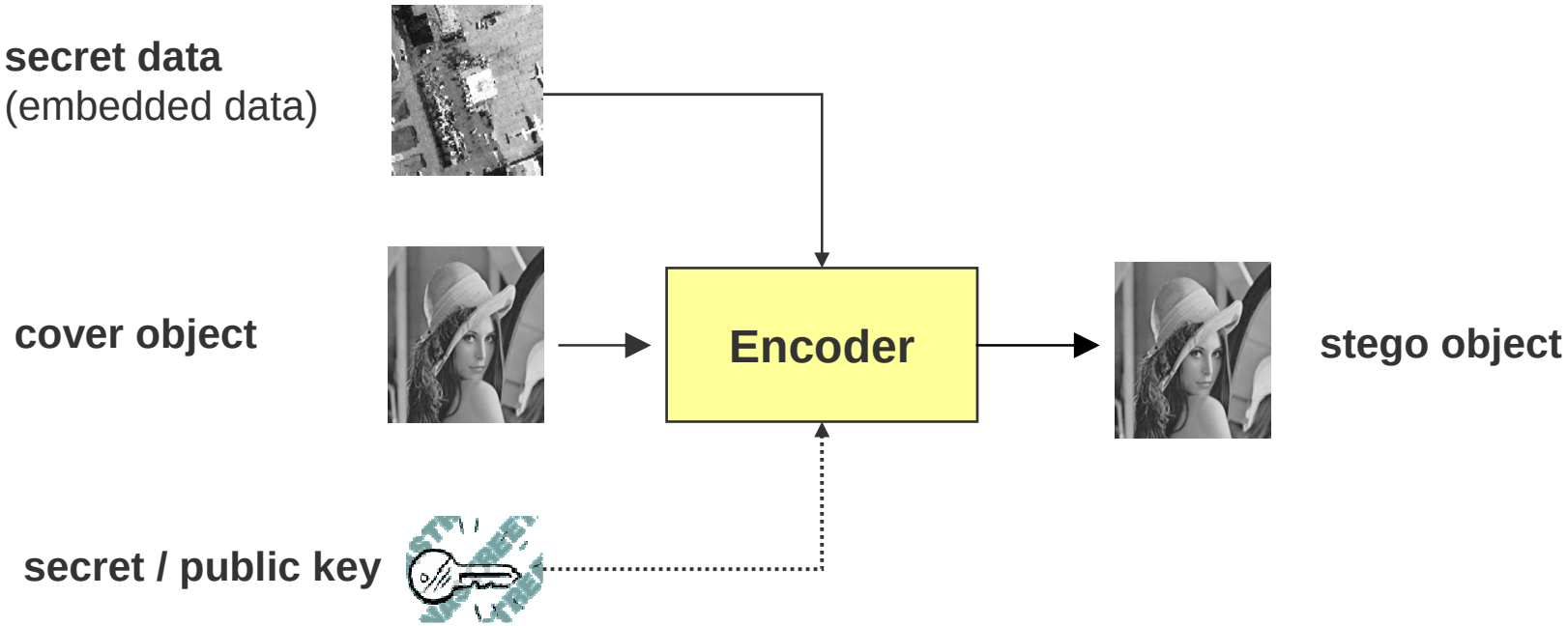
- Copyright marking (watermarking)
- Document marking (fingerprinting)

Army, intelligence agency … and criminal: steganography

- Unobstrusive communication
- No suspicion / secret identity

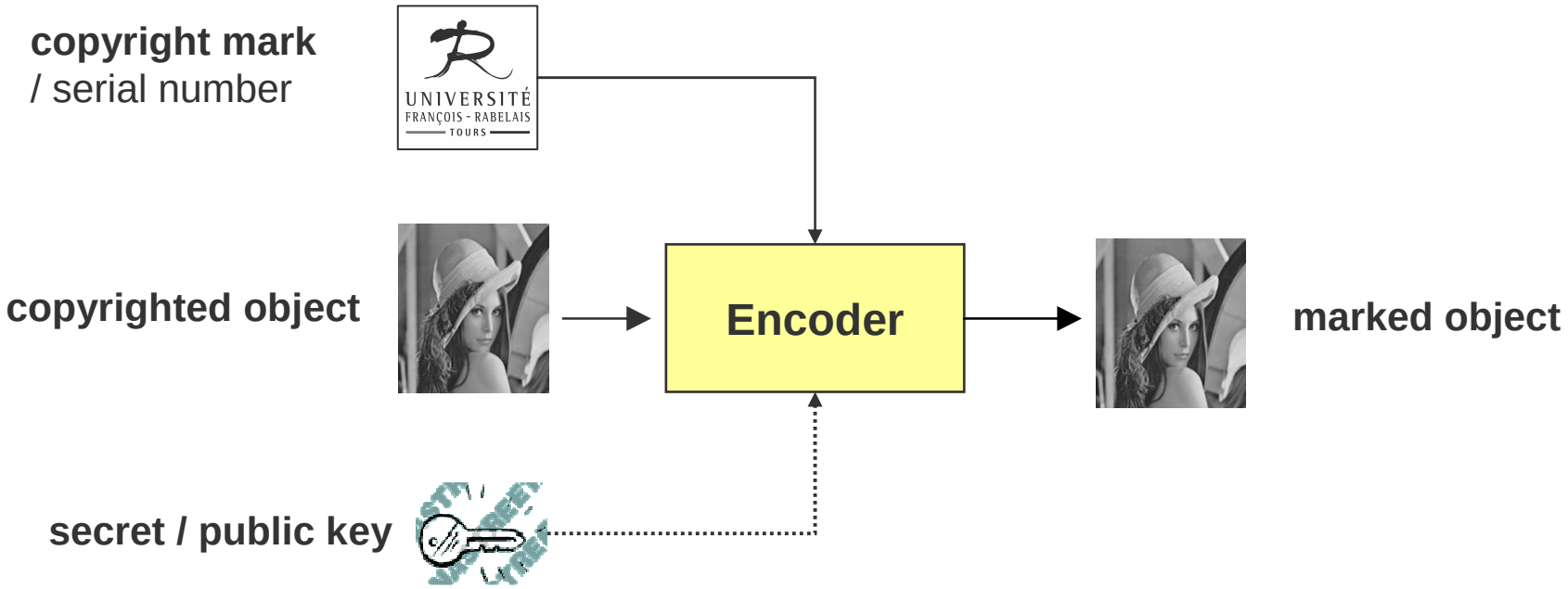
Data embedding scheme

Steganography



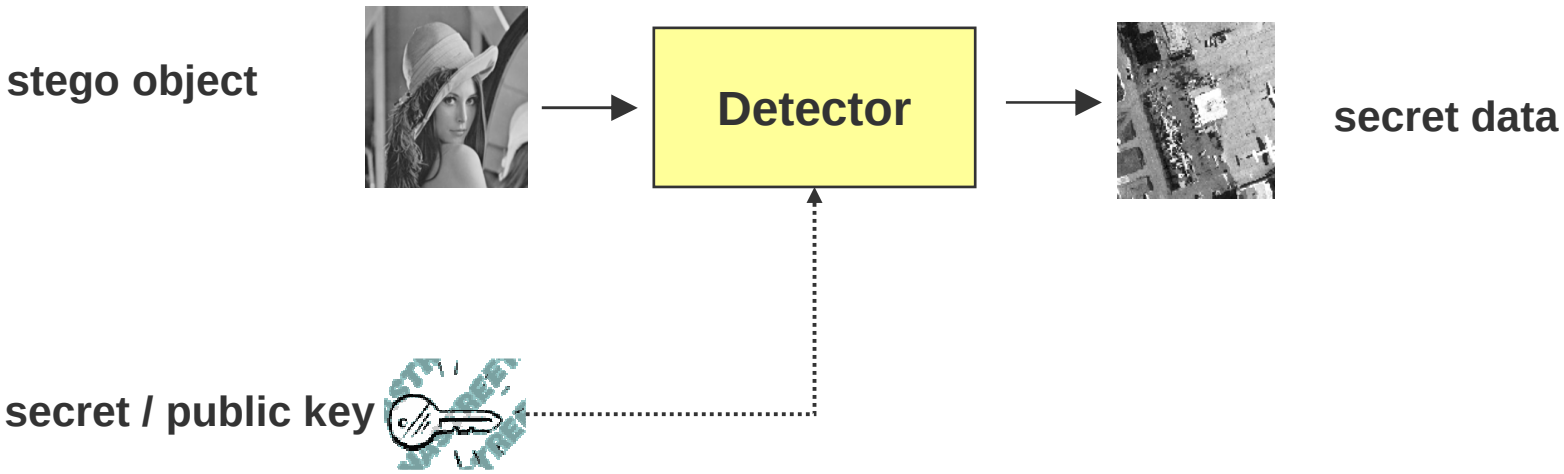
Data embedding scheme

Digital marking



Data recovery scheme

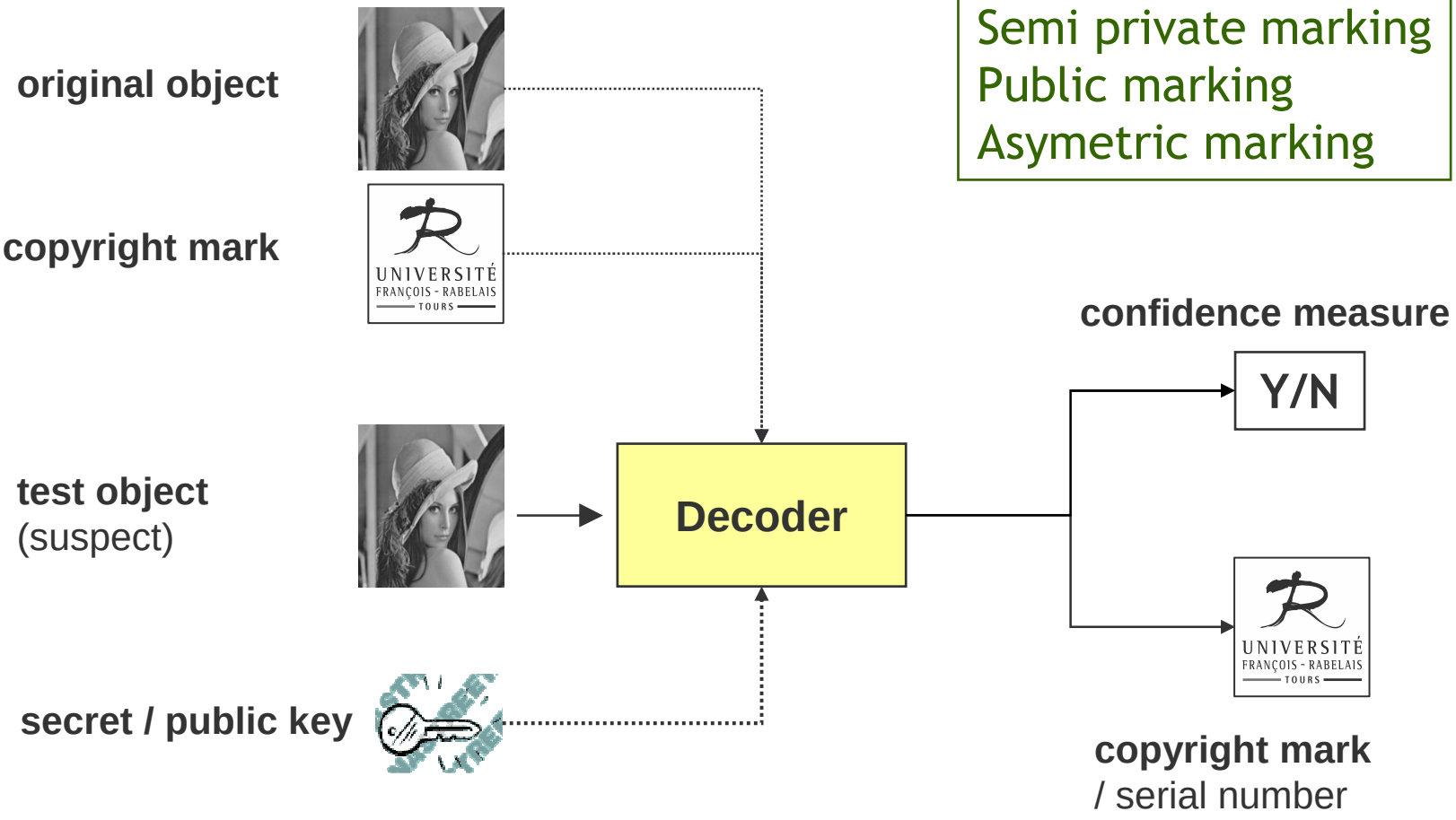
Steganography



Data recovery scheme

Copyright marking

Private marking
Semi private marking
Public marking
Asymetric marking



Attacks : steganalysis

Aims (steganography)

- Detecting the secret nature of the communication
- Recovering secret data
- Modifying secret data

Passive attacks

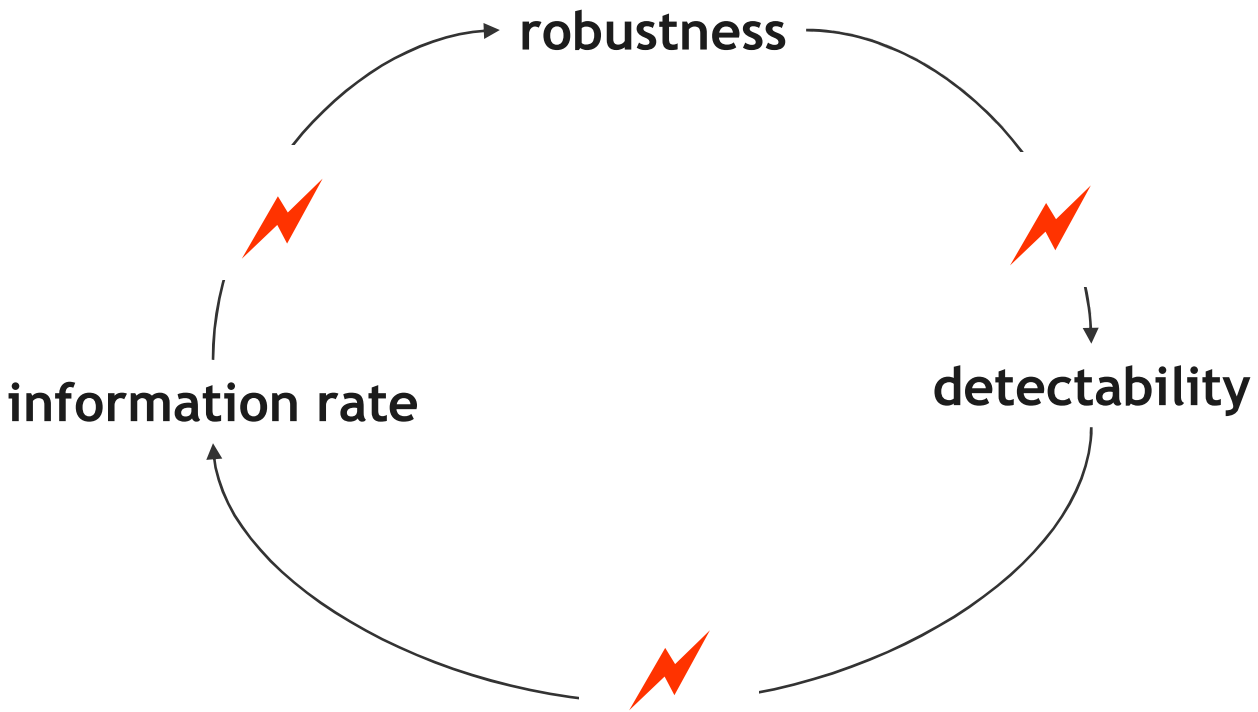
Active attacks

Aims (digital marking)

- Detecting the presence of a copyright mark
- Removing or modifying the copyright mark
- Adding false copyright mark

Information hiding : vicious circle

- Secret data integrity must remain after being embedded
- Stego object must remain (almost) unchanged to naked eye / ear
- Changes in stego object have no effect on watermark (compression !)



Hiding techniques

Medium : *compression* or not

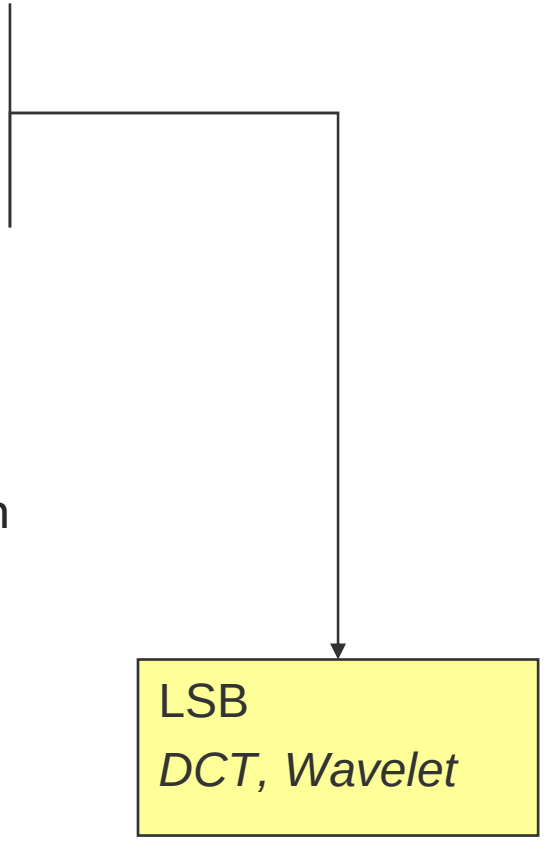
Image	bitmap, GIF, *JPEG (compression)*
Audio	Raw, WAV*, MP3 (compression)*
Video	*MPEG (compression)*
Text	document, XML, program

Cognitive principles

masking properties of the human perceptual system

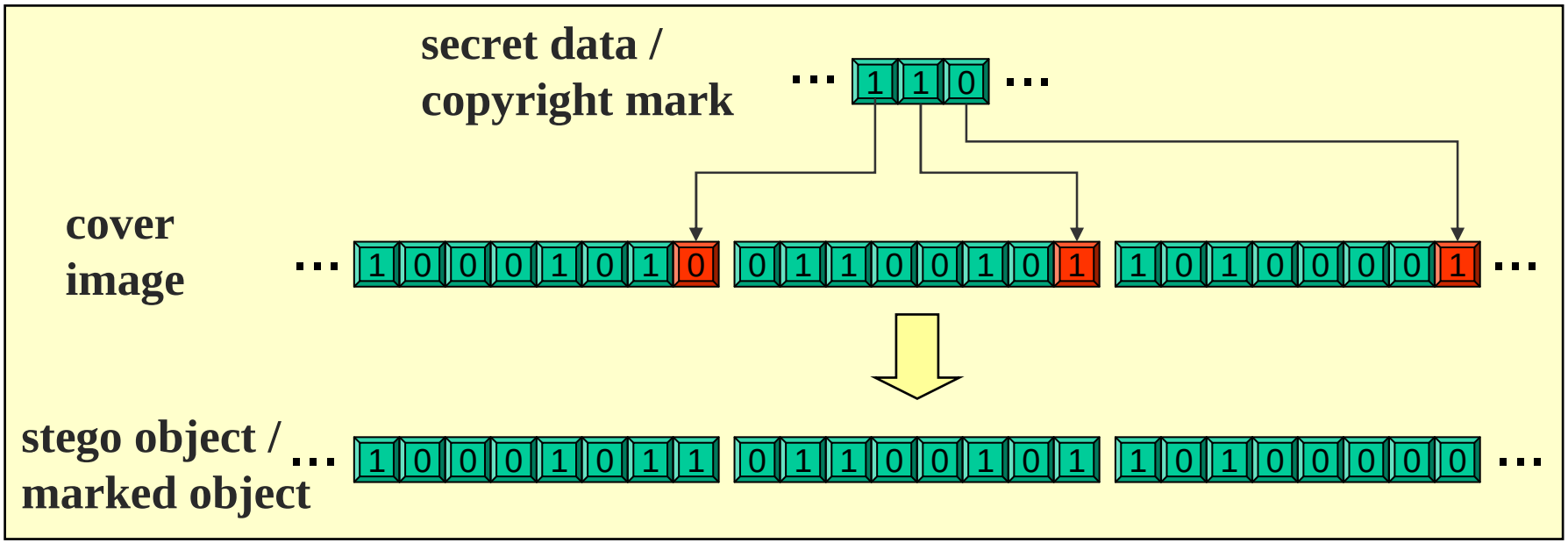
Techniques

- Direct embedding
- *Embedding in a transform space*
- Linguistic steganography



LSB - Least Significant Bit (public marking)

The least significant bits (LSB) of the cover object are used to hide the most significant bits (MSB) of the hidden object

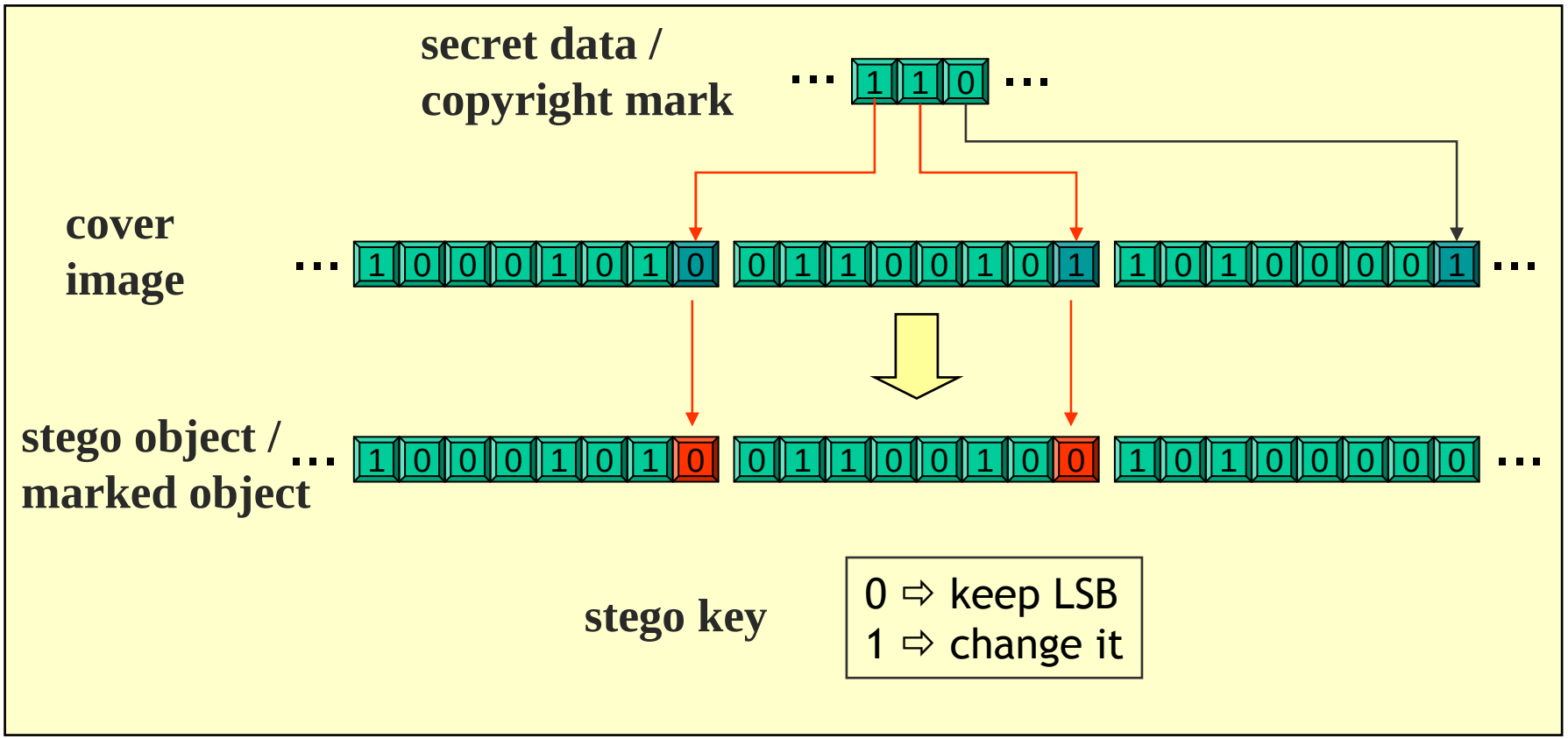


Medium

- Bitmap image (BMP)
- Raw audio (SND) or without compression (optional : .AU, .AIFF, .WAV)

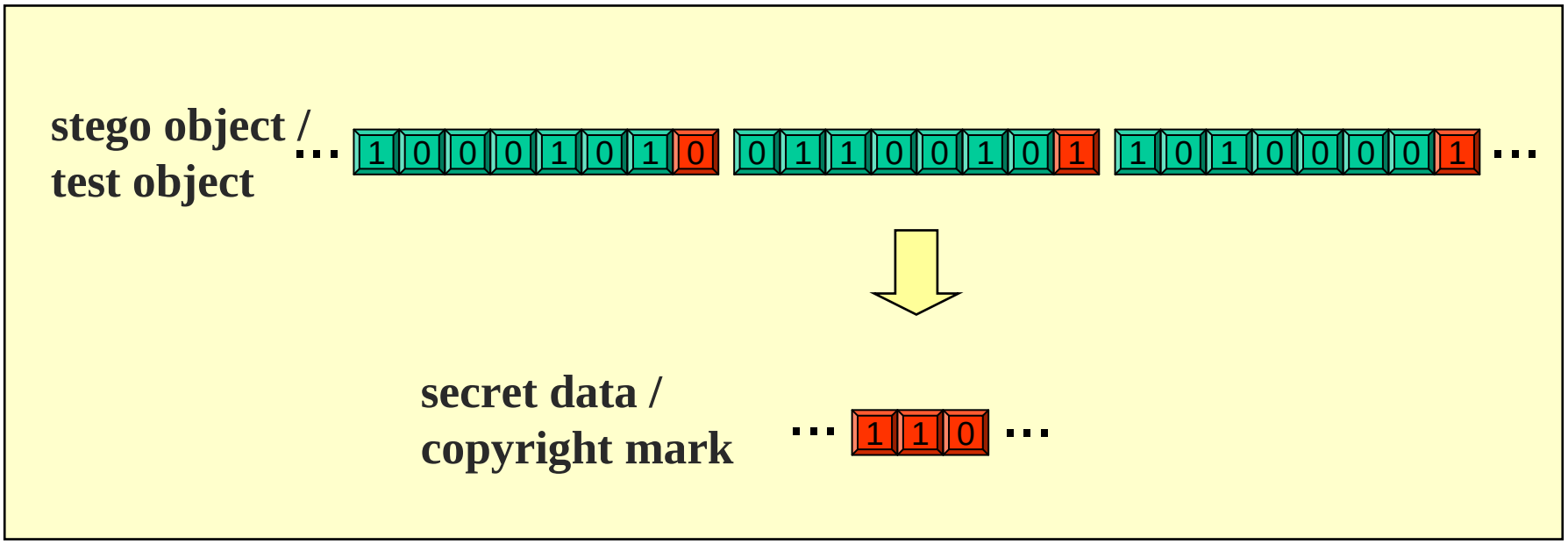
LSB - Least Significant Bit (private marking)

Modification of the LSB according to a stego key depending of the MSB of the hidden object



Recovery

- **Public marking** – To extract the hidden image, you only have to take out the N first LSB's from the stego object
- You need the stego key in case of pseudo-random marking



Recovery

- **Private marking** – Original image is needed

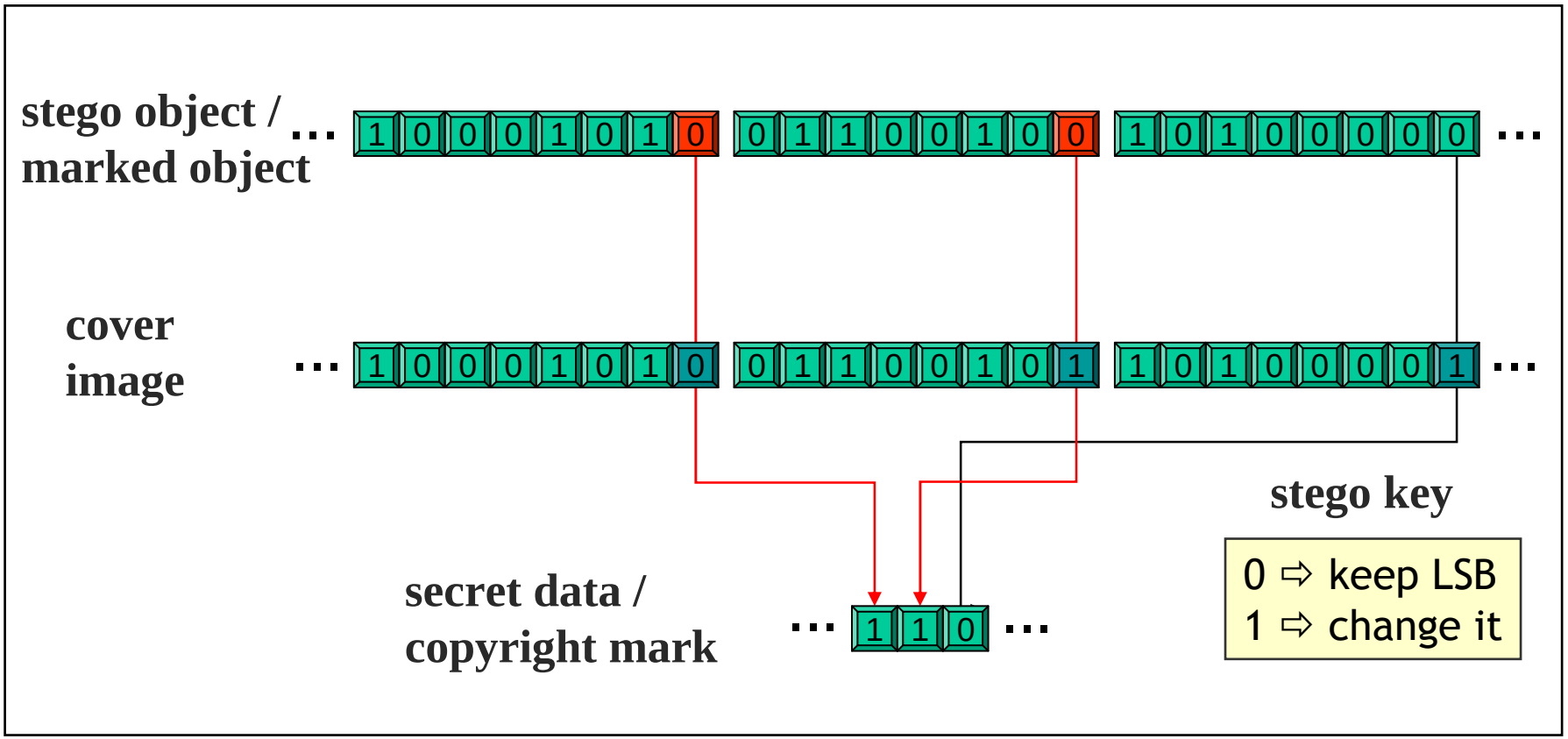


Image : LSB

Information rate

Bit Level 7

Source : Cummins, Diskin,_ Lau & Parlett

- Trade off : information rate vs. confidentiality vs. robustness
- Easier for digital marking than steganography … but problems of robustness

Image : LSB

Confidentiality

- do not modify pixels in large expanses of flat colour (low variance of luminosity)
- do not modify pixels that are lying on a sharp edge (high variance of luminosity)

- pseudo-random selection of the pixels of the cover object (stego key)

Robustness

↳ by definition, LSB do not resist to filtering or compression techniques

Basic solutions

- repetition code to survive filtering
- primitive spectrum modulation : *Patchwork*-like techniques [Bender et al 1996]

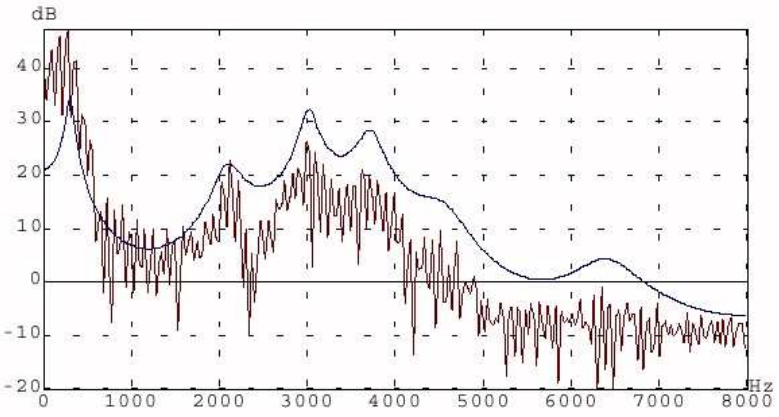
Embedding in a transform space

- DFT, DCT, Wavelets

Transform spaces

DFT (Discrete Fourier Transform)

- ⇨ frequencies space
- ⇨ audio signal : spectrum

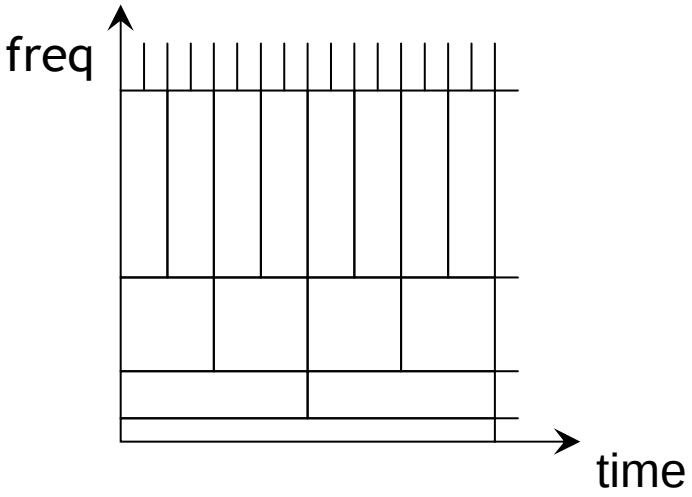


DCT (Direct Cosine Transformation)

- ⇨ frequencies space
- ⇨ image compression : JPEG

Wavelets

- ⇨ image compression (JPEG2000)
- ⇨ digital signal processing (MP3)



Transform spaces

JPEG compression

139	144	149	153	155	155	155	155
144	151	153	156	159	156	156	156
150	155	160	163	158	156	156	156
159	161	162	160	160	159	159	159
159	160	161	162	162	155	155	155
161	161	161	161	160	157	157	157
162	162	161	163	162	157	157	157
162	162	161	161	163	158	158	158

pixels

DCT transform on 8x8 blocks →

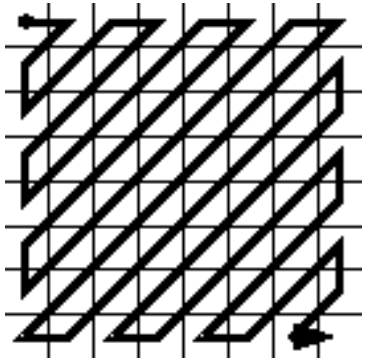
1260	-1	-12	-5	2	-2	-3	1
-23	-17	-6	-3	-3	0	0	1
-11	-9	-2	2	0	-1	-1	0
-7	-2	0	1	1	0	0	0
-1	-1	1	2	0	-1	1	1
2	0	2	0	-1	1	1	-1
-1	0	0	-1	0	2	1	-1
-3	2	-4	-2	2	1	-1	0

DCT coefficients

↓ *Quantization (high frequency filtering)*

79	0	-1	0	0	0	0	0
-2	-1	0	0	0	0	0	0
-1	-1	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0

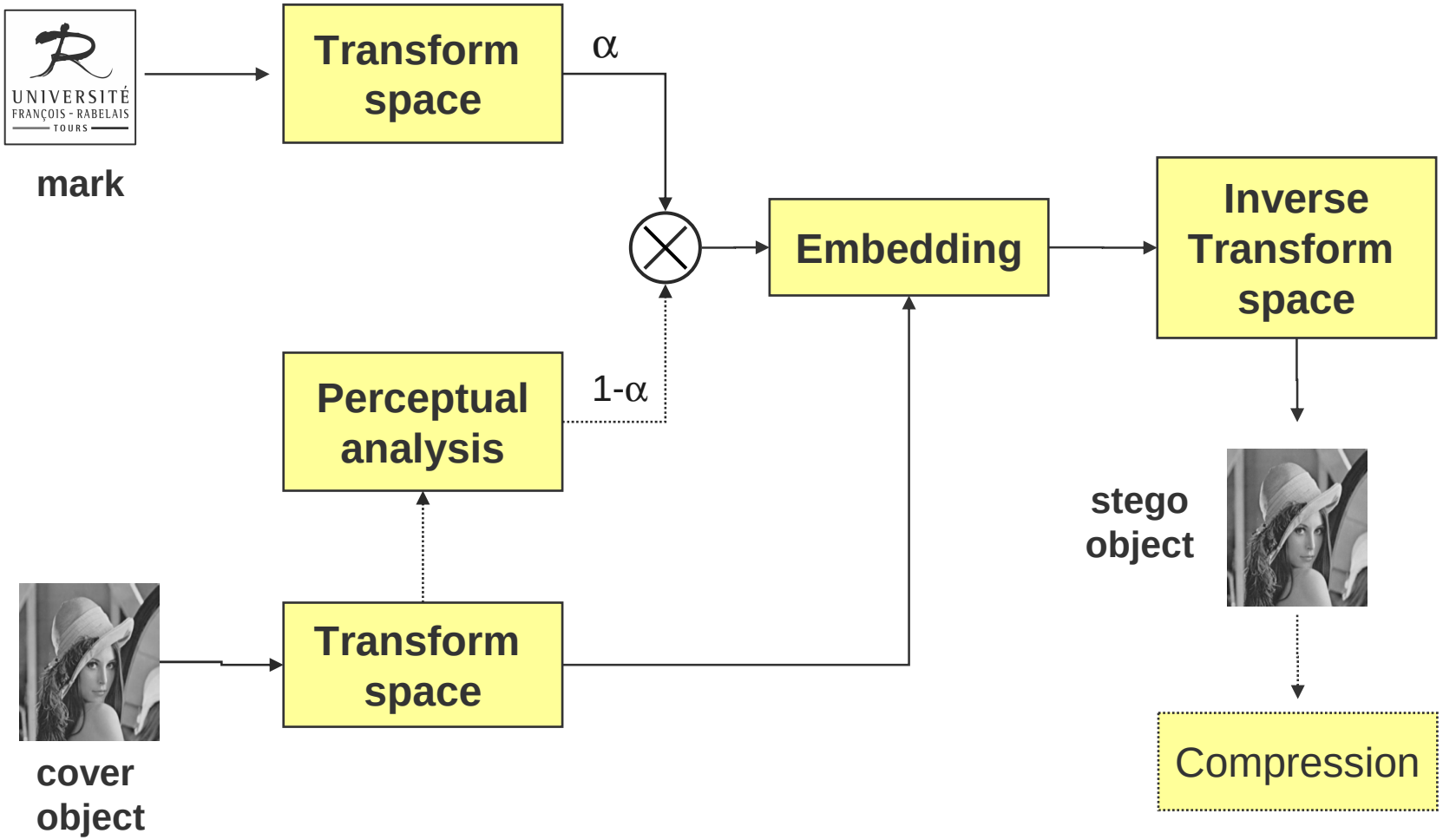
Zig-zag compression ←



← **JPEG**

Embedding in a transform spaces

Embedding general scheme



Embedding in a transform spaces

Example : discrete cosine transform (JPEG) [Cox et al, 1996]

1. DCT transform of the cover image $V = \{V_i\}_{i=1..N}$
2. DCT transform of the watermark $W = \{W_i\}_{i=1..N}$
3. Embedding on the DCT coefficients $V'_i = V_i\ (1 + \propto W_i)$
   or simply LSB shift on the DCT coefficients

Practically
N = 1
(most significant frequency)

Original

Watermarked

JPEG compressed

Embedding in a transform spaces

Recovery

Private marking : original image needed

1. DCT inverse transform of the tested image
2. DCT inverse transform of the original image
3. Inversion of the embedding formula
4. Detection if comparison > Threshold

Robustness additional markings
rescaling, JPEG compression, printing, scanning…

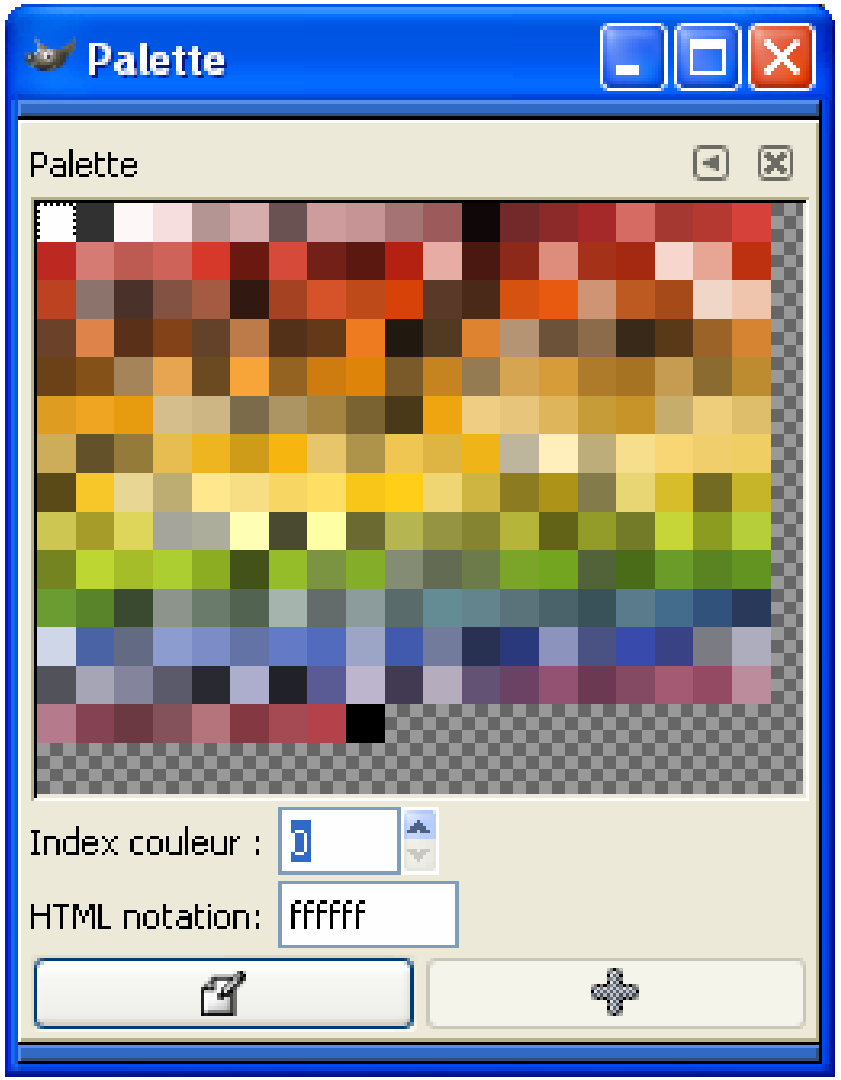
Information rate

- DCT performed on 8x8 blocks ⇨ 1 bit per block
- Limited rate ⇨watermarking rather than fingerprinting or steganography

GIF images

GIF format

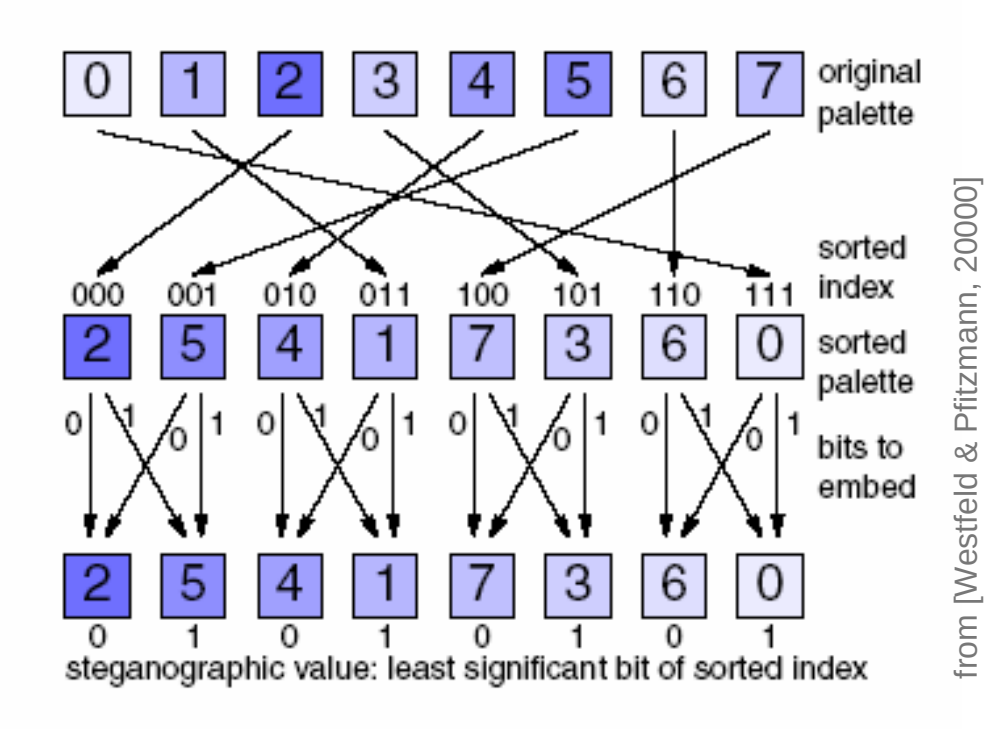
- **Indexed colours** : every pixel refers to a position in a colours palette
- **image** = **specific** colours palette
- basic compression algorithm



Hiding information in a GIF image

1. **Sorted colours palette** : unnoticeable differences between every pair of the sorted palette

2. **LSB Embedding**
   LSB shifts on the sorted indexes : unnoticeable colour shifts



from [Westfeld & Pfitzmann, 20000]

Sound techniques

General hiding techniques

- LSB
- Transform space (DFT, Wavelet)

Specific technique : echo hiding

[Gruhl et al., 1996]

- **temporal masking** : human perceptual system can not perceive short echoes
- two kinds of short echoes (delay τ, amplitude α) following the embedded bit
- systematic or pseudo-random location of the echoed sounds
- **transform space embedding** : cepstral transform ⇨resist to compression
- **detection** (public key marking is difficult)
  - ✓ detection – delay τ : autocorrelation of the cepstrum of the stego file
  - ✓ recovery is more difficult if you don't own the cover audio file

Sound techniques

Midi files

- Useless repetitions of the Program Change messages (fake changes) are used to hide information
- Embedding information in useless parts of a object is a common technique for basic steganography (see below)

MP3

– During compression, data is selectively lost depending on the bit rate the user has specified

– hidden data is encoded in the parity bit of this information

– **Recovery** : to retrieve the data all you need to do is uncompress the MP3 file and read the parity bits

Video

- Mixture of sound and images techniques

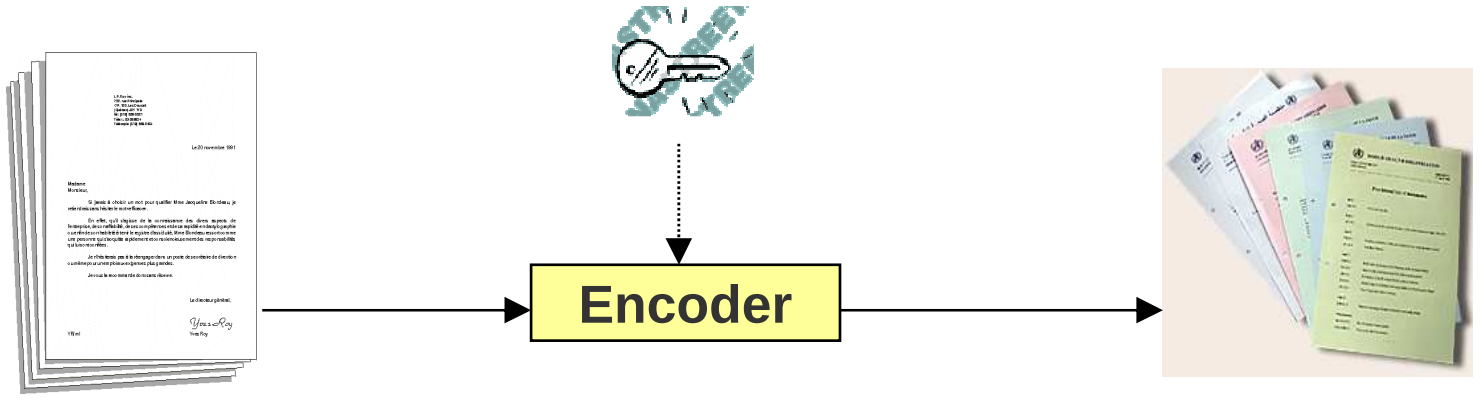
Information Hiding in Binary Files

- Divide program into n blocks.
- 0 = code left unchanged, 1 = two instructions are switched.
- To decode we need the original binary file.
- Recovery : comparing the original and marked binary files

Text / document techniques

Principles

- Differential encoding technique : invisible alterations of the form of the document
- Pseudo-random or systematic selection of the altered items
- Modification code (0 = … ; 1 = …)



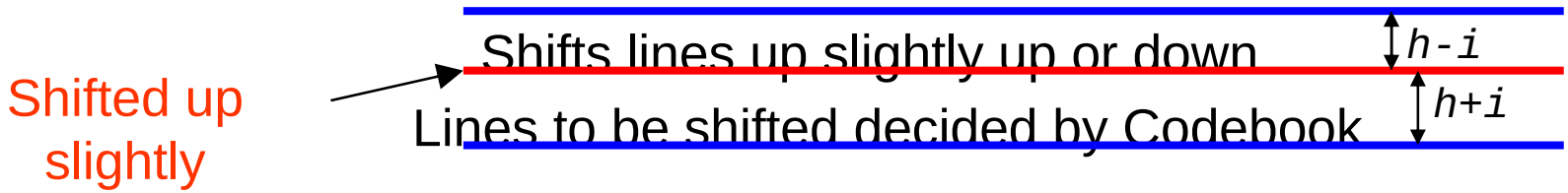
Original Document

Marked Documents

Text / document techniques

Alteration techniques

Line Shift Coding - Vertical shifting of lines



Word Shift Coding - Horizontal spacing between each word

Shift of words slightly left or right, decided by codebook

White space manipulation

Useless and invisible white space at the end of lines.

Feature Coding - features changes e.g. text height

Text / document techniques

XML

- Different components in which data can be hidden – css, dtd, xsl
- Using tag structure to hide information
- Useless / optional tags : invisible alterations

stego code

```
0 ⇨ <img></img>
1 ⇨ <img/>
```

stego XML file

```
<img src="toto1.jpg"></img>
<img src="toto2.jpg"></img>
<img src="toto3.jpg"/>
<img src="toto4.jpg"/>
<img src="toto5.jpg"></img>
```

secret data

```
0
0
1
1
0
```

Other ideas

- White spaces in tags
- Tags order

```
0 ⇨ <usr><name>N</name><id>I</id></usr>
1 ⇨ <usr><id>I</id><name>N</name></usr>
```

Attacks : steganalysis

Passive attacks

Detecting the presence of a copyright mark / secret message

Active attacks (watermarking)

[Craver el al. 1998]

- **Robustness attacks** — image processing (geometric alteration, filtering…) to diminish or remove the watermark

  ↳ StirMark [Petitcolas, Anderson, Kuhn 1998]

- **Presentation attacks** — modify the content to prevent detection of mark.

  ↳ Mosaic [Petitcolas, Anderson, Kuhn 1999]

- **Interpretation attacks** — prevents assertion of ownership

  ↳ fake marks addition

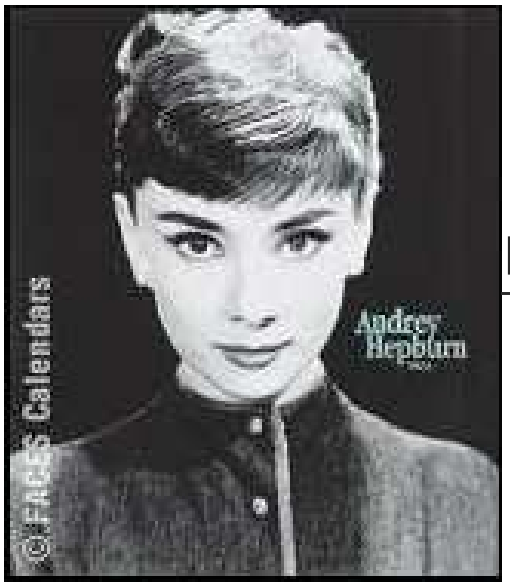
- Implementation attacks — take advantage of poorly implemented software.

Passive attacks

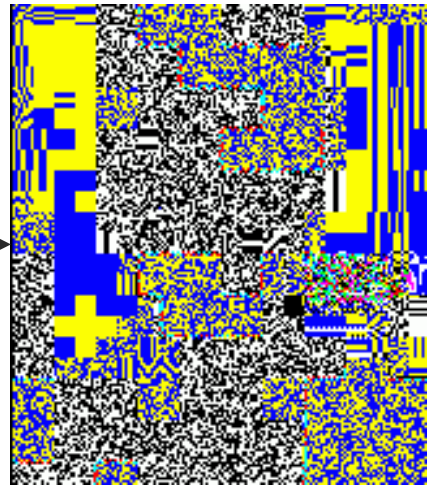
Statistical passive attack techniques

Natural data are not random !

LSB embedding — noisy nature of the LSB of the stego-object

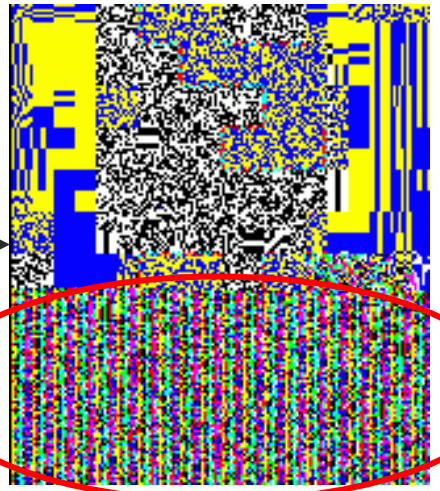


LSB extraction



Source : Guillermito

original image



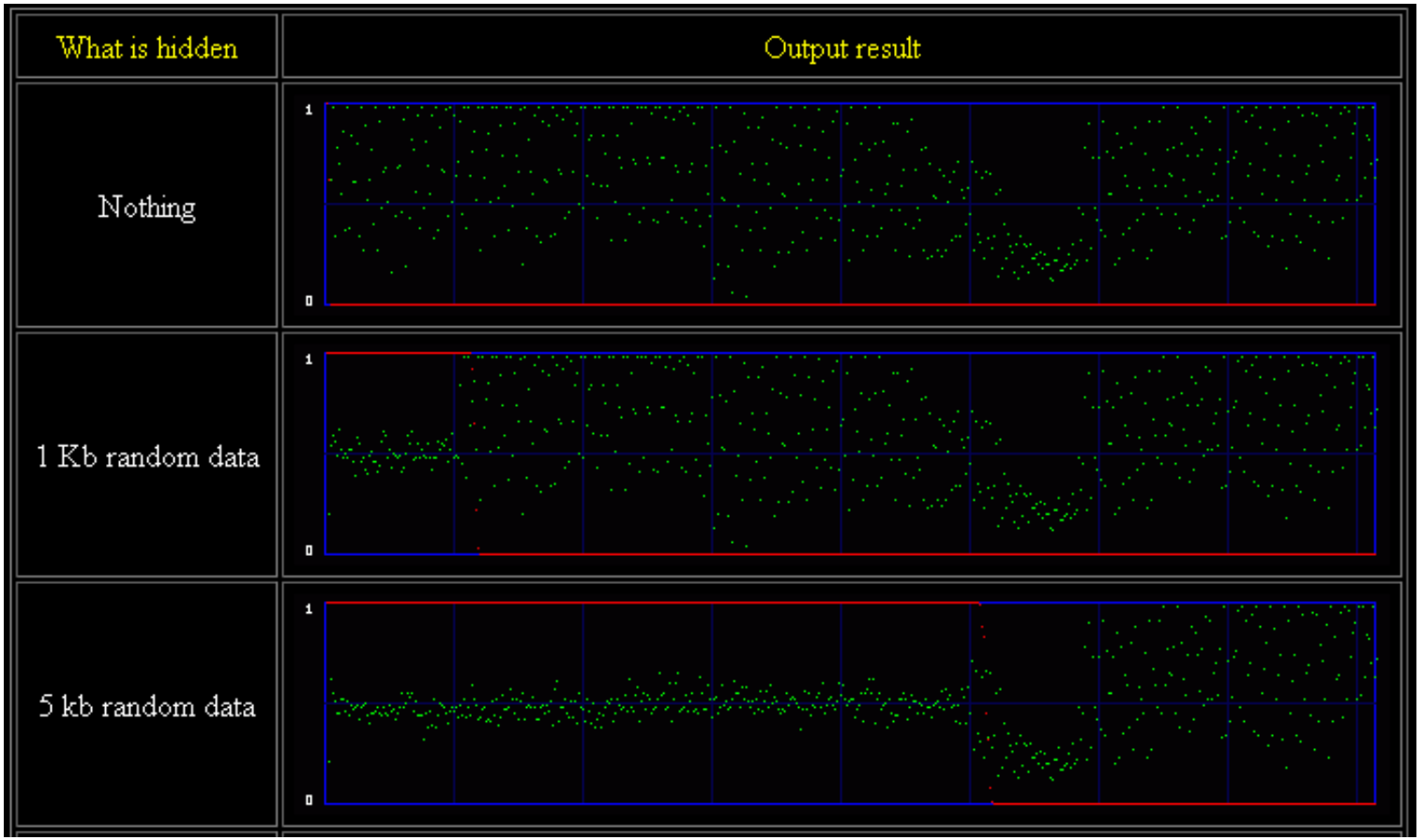
Visual attack

stego image

LSB : statistical passive attacks

LSB embedding detection with a statistical method [Westfeld, Pfitzmann, 2000]

χ2 test on the distribution of the LSBs (PoV) between stego image and a random one



χ2 test

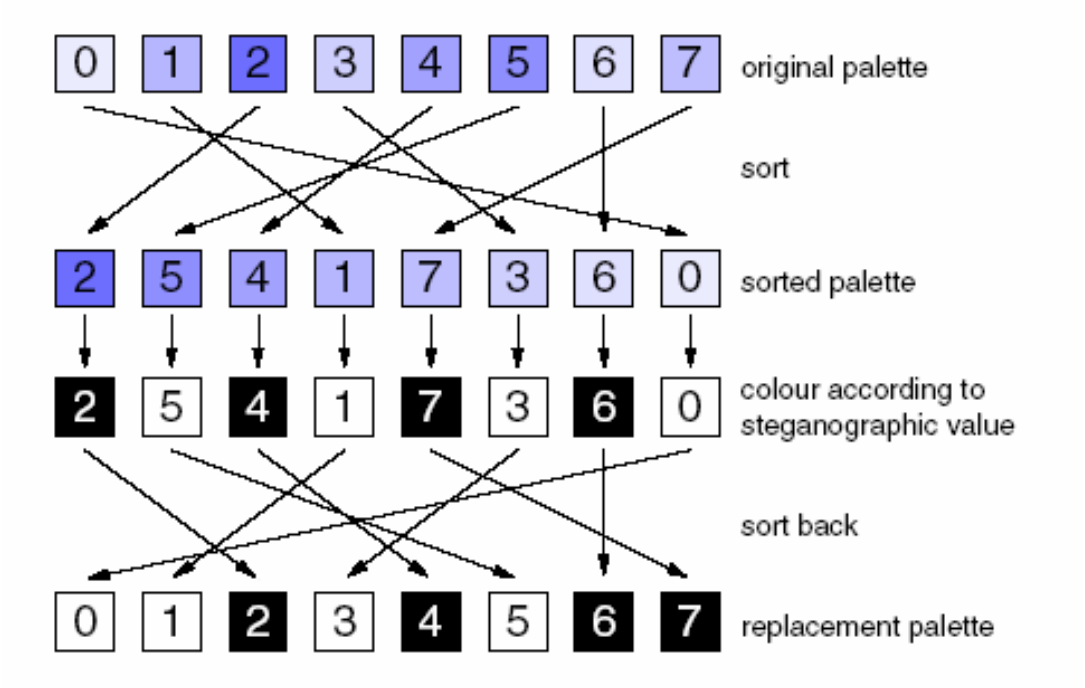
Source : Guillermito

GIF : passive attacks

GIF : colours palette modification

- Visible modification of the colour palette with the cover image
- **Visual attack**

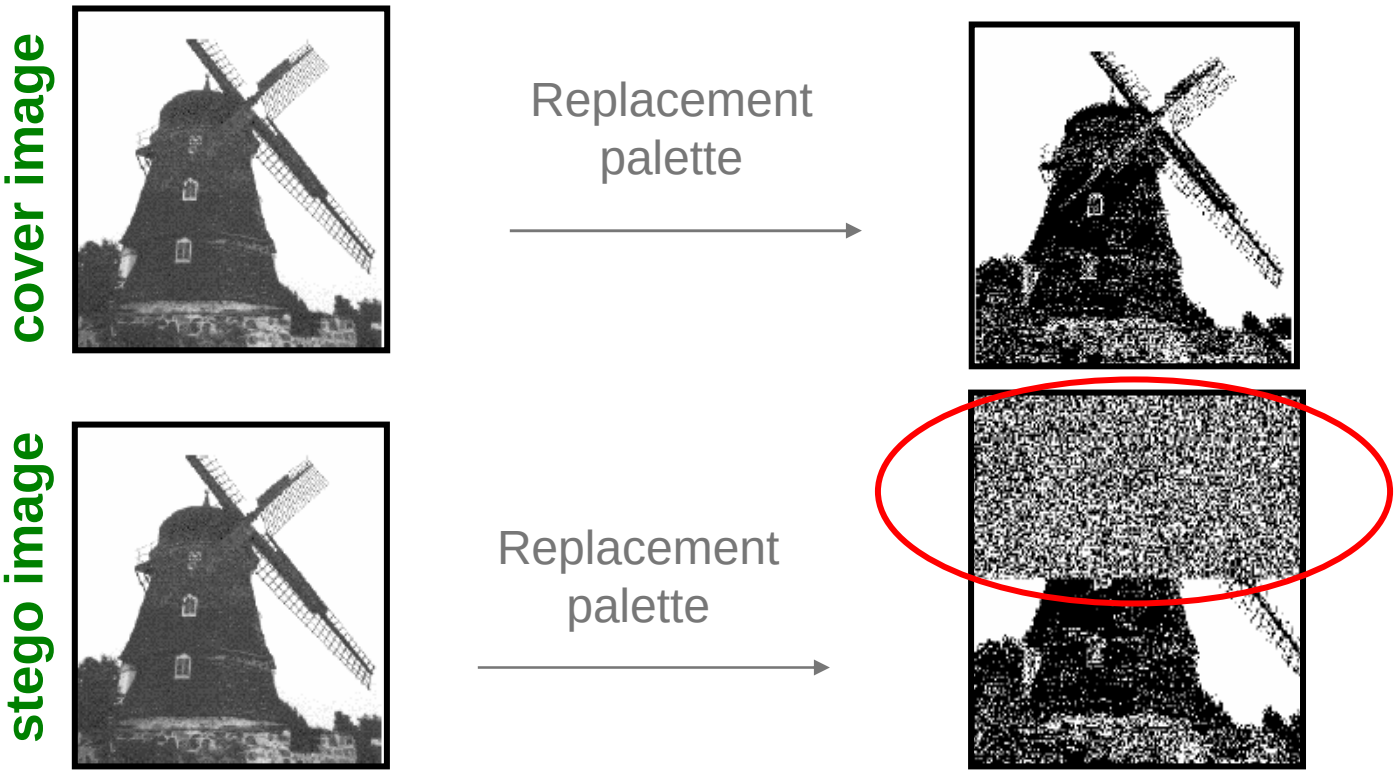
[Westfeld, Pfitzmann, 2000]



GIF : visual passive attacks

Visual attack : example

[Westfeld, Pfitzmann, 2000]



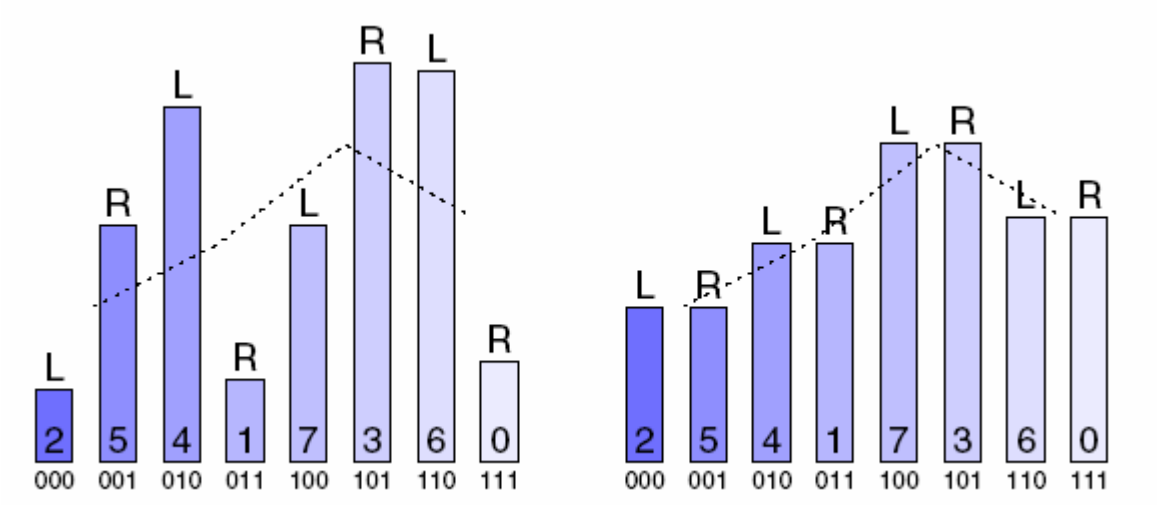
- LSB embedding on the indexes ⇨noticeable noisy nature of the LSB
- Pseudo-random vs. systematic embedding ⇨ statistical attack

GIF : statistical passive attacks

Statistical attack

[Westfeld, Pfitzmann, 2000]

LSB embedding ⇨ statistical influence on the colours histogram

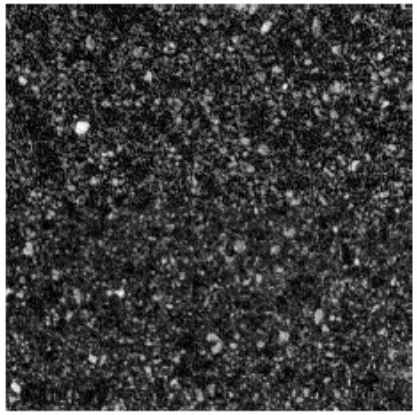


- visual observation of the histogram : not really noticeable
- $\chi 2$ test on the distribution of the LSBs (PoV) as seen previously with BMP

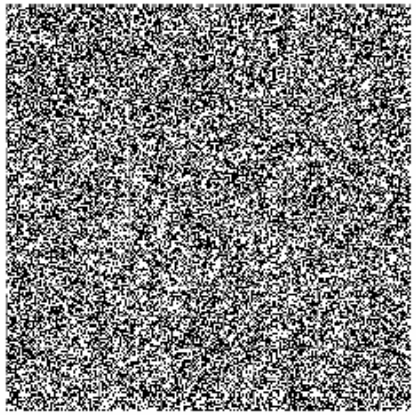
GIF : statistical passive attacks

Statistical attack : example

[Westfeld, Pfitzmann, 2000]

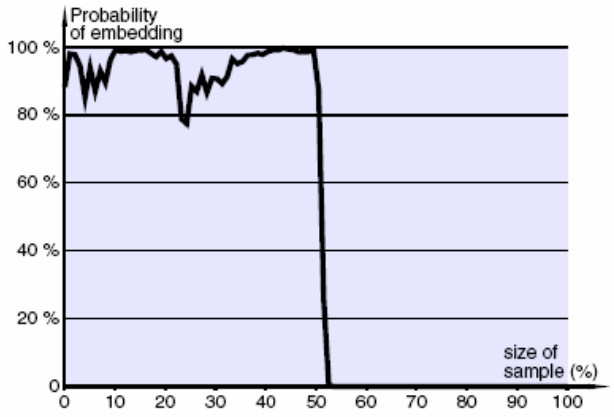


Stego image



Visual attack

χ2 test : half of the image is containing embedded data

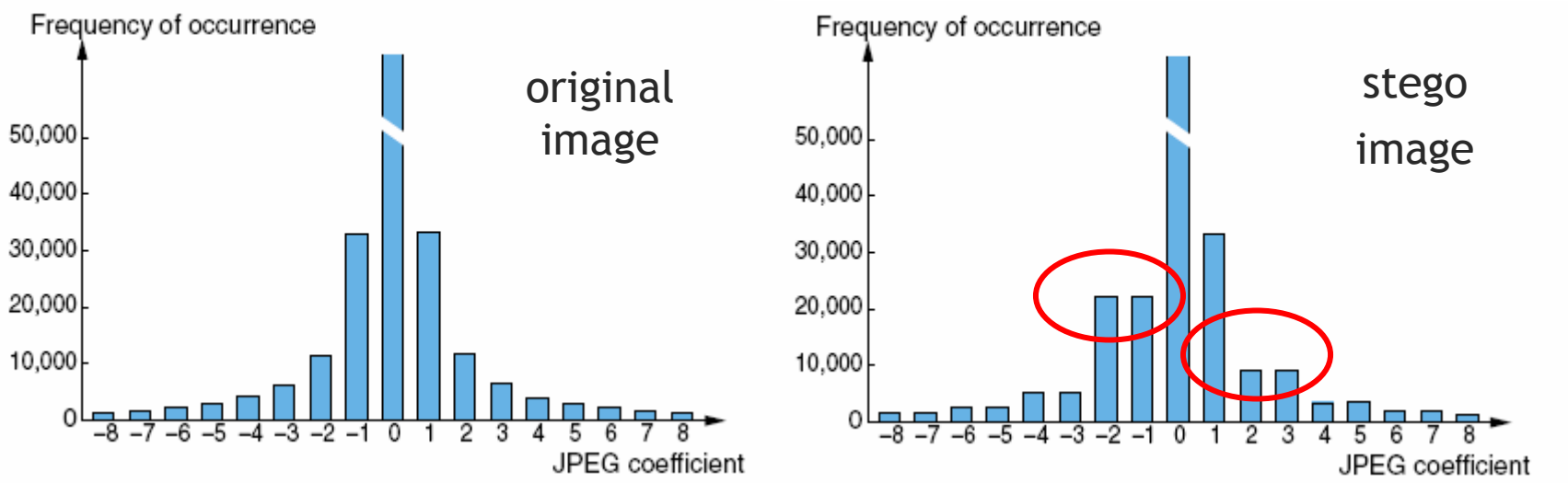


JPEG : statistical passive attacks

[Westfeld, Pfitzmann, 2000] [Fridirch et al, 2001]

Transform space

- No direct attack
- LSB embedding on the DCT coefficient : statistical influence
- asymmetric distribution of the DCT coefficients (differences reduced)



- **private marking** : $\chi 2$ test on DCT coefficients

Robustness Attacks

Robust hiding techniques

- Must be invisible
- Need to cope with common transformations to prevent accidental removal of the embedded data
- Direct embedding techniques are not robust ⇨ transform space
- Many techniques can survive individual transformations but are vulnerable to combinations of them ⇨ embedding multiple version of the mark with different transform techniques

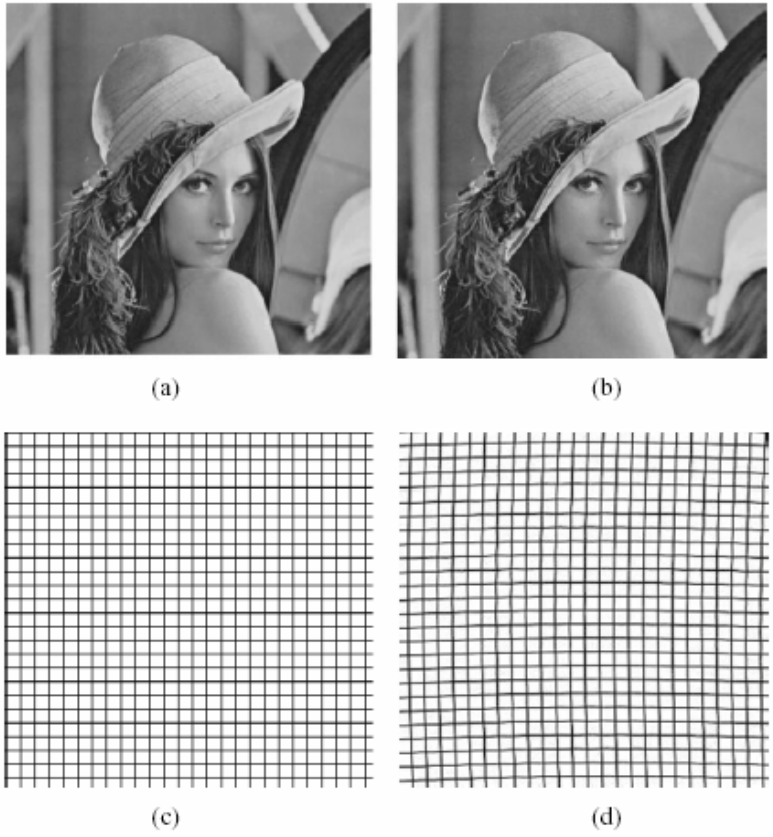
Robustness Attacks

StirMark

Series of unnoticeable distortions to remove mark

- Minor geometric distortion
- Random low frequency deviation
- High frequency displacement
- Transfer function to simulate noise (smoothly distributed error)
- Resampling (B-spline)

⇨ Benchmarking



Other techniques

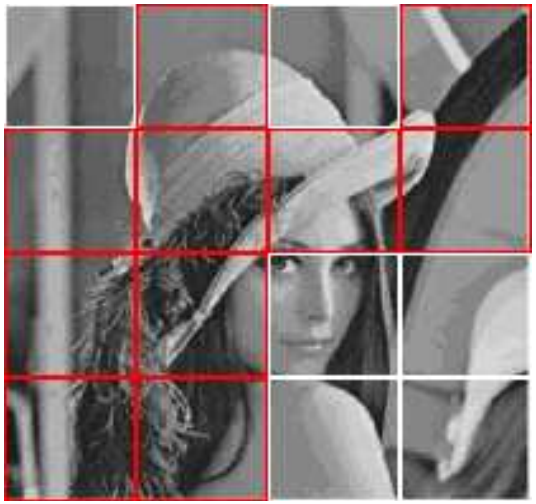
Many attack methods are tied to a specific embedding technique

http://www.cl.cam.ac.uk/~fapp2/watermarking/stirmark

Presentation Attacks - Mosaic

Principles

- Takes advantage of minimum size requirements for embedding
  (for instance: 8x8 DCT bloks)
- Split image into small subimages
- Unnoticeable recombination of the juxtaposed subimages when displaying by a Web crawler



Experiment

- Mark inserted by Digimarc.
- 6 over 16 subimages still contain the mark

Presentation Attacks - Audio

Echo hiding

- **Detection** — echo delay τ is detected through the auto-correlation of the cepstrum of the encoded signal
- **Blind echo cancellation** — Removing the echo signal without the original object is a complex problem in DSP
  - Obtaining the echo delay τ is easy (detection)
  - Removing an echo of delay τ with a random relative amplitude is not efficient : resistant watermark
  - Brute force approach : iterative search of the best α amplitude.

Implementation Attacks

Hacking vs. steganalysis

Unsecured marking software : direct attack is possible

Example : DigiMarc

- Digimarc requires users to register ID and password.
- Attacker broke into software and disabled password checks.
- Could then change the ID, affecting already marked images and bypassing checks for existing marks to overwrite them.

Conclusion

- Steganography will become increasingly important as more copyrighted material becomes available online

- Present techniques are not robust enough to prevent detection and removal of embedded data (e.g. anyone with the corresponding public key will be able to remove the digital mark)
- Techniques for public key steganography but not for digital marking

- By comparison with cryptography, we still need a real mathematical theory for steganography
- But new technologic domain with rapidly increasing developments

Bibliography

Main references

R.J. Anderson, F. Petitcolas (1998) On the limits of steganography, IEEE Journal of Selected Areas in Communications, 16(4), 474-481.

E. Cole (2003) *Hiding in plain sight : steganography and the art of covert communication*, Willey Publ. Inc.

F. Petitcolas (2000) *Information hiding for steganography and digital watermarking*. Artech House Inc., Norwood, MA.

F. Petitcolas, R. J. Anderson, M. G. Kuhn (1999) Information hiding : a survey, Proc. of the IEEE, 87(7), 1062-1078.

International Conferences

R.J. Anderson (Ed.) (1996) *Information hiding : 1st International Workshop*, Cambridge, England, *LNCS* 1174, Springer-Verlag, Germany

D. Aucsmith (Ed.) (1998) *Information hiding : 2nd International Workshop*, Portland, Oregon, *LNCS* 1525, Springer-Verlag, Berlin, Germany.

IHW'99, Information hiding : 3rd International Workshop, LNCS 1768, Springer-Verlag, Berlin, Germany 2000

Bibliography

Other works

F. Petitcolas, R.J. Anderson, G. Kuhn (1998) Attacks on copyright marking systems. *In* [Aucsmith, 1998] 218-238.

W. Bender, D. Gruhl, N. Morimoto, A. Lu (1996) Techniques for data binding. *IBM Systems Journal*. 35(3-4), 313-336.

S. Craver, B.L.. Leo, M. Yeung (1998) Technical trials and legal tribulations. *Communications of the ACM*. 41(7). 44-54.

I.J. Cox, J. Killian, T. Leighton, T. Shamoon (1996) A secure robust watermark for multimedia, *In* [Anderson,1996], 183-206.

J. Fridrich, M. Goljan and R. Du (2001) Reliable Detection of LSB Steganography in Grayscale and Color Images, *Proc. of the ACM Workshop on Multimedia and Security*, Ottawa, 27-30

D. Gruhl, W. Bender, A. Lu (1996) Echo hiding, *In* [Anderson,1996], 295-315

B. Pfitzmann (1996) Information hiding, *Proc. 1st International Workshop on Information hiding*, *LNCS* 1174, Springer-Verlag, 347-350.

A. Westfeld and A. Pfitzmann (2000) Attack on Steganographic Systems*, IHW'99 : Information hdiing : 3rd International Workshop*, *LNCS 1768,* Springer-Verlag, Berlin, 2000, pp. 61-75

Bibliography

Internet links

- J. Cummins,P. Diskin, S. Lau, R. Parlett, *Steganography and Digital Watermarking*, http://www.
- Guillermitto, *Analyzing steganography softwares*, http://www.guillermito2.net/stegano/
- F. Hartung (1999) References on multimedia watermarking and data hiding research and technology. www-nt.e-technik.uni-erlangen.de/~hartung/watermarkinglinks.html
- N. Provos, P. Honeymann (2003) Hide and Seek : an introduction to steganography. IEEE Security and Privacy. http://www.computer.org/security
- Stego Archive http://www.stegoarchive.com/