9. Digital Watermarking

This chapter is based on transparencies originally provided by Prof. Dr. Jana Dittmann. Her support is gratefully acknowledged.

9.1 Security Aspects

Security

Measures that prevent intentional attacks on computers, stored data and data in transfer over a communication network.

Safety

Measures that prevent the effects of unintended events that would lead to loss or damage of computers, stored data or data in transfer over a communication network.

Privacy

Protection of personal data from unauthorized access.

Example

A photographer finds pictures he took in a digital image database on the Internet where they are offered for sale. He is not able to prove his copyright since the digital pictures do not contain a reference to him as the author.

Security Aspects : Digital Watermarks

Security aspect	Short description
access protection	control of access to the system
authenticity	proof of identity of the author and authenticity of the data. An authentification is performed and authenticity confirmed.
confidentiality	prevents access to data by unauthorized persons
integrity	proves that data has not been altered
provability	examination of authenticity and integrity, recording even of authorized access, to guarantee liability of communication

Copyright

Objects

Works of literature, science and art.

The copyright protects intellectual property and its implementation from

- unauthorized commercial use
- violation of intellectual interests in the work.

Rights

- author's personality right (mention of his/her name, authenticity)
- rights of utilization (replication, distribution and broadcasting)
- Limits of copyright: where the public interest might be violated

Protection by copyright also applies to software and technical documentation.

9.2 Watermarks: History, Types und Applications

History

Watermarks on paper, carpets, banknotes ...

Digital Watermarks are based on a steganographic procedure:

- Insert visible, invisible robust or invisible fragile markings into the document
- Goals:
  - Authenticity: copyright protection
  - Integrity: proof that the document has not been manipulated.

Types of Watermarks

- **Visible watermarks**
  for the annotation of documents with meta data such as the name of the author
- **Invisible robust watermarks**
  A manipulation of the document should *not* spoil the watermark.
  - insertion of hidden messages
  - insertion of copyright information, authenticity (“copy control watermark“)
  - insertion of meta data that should not be visible
- **Invisible fragile watermarks**
  A manipulation of the document *should* spoil the watermark.
  Used to prove the integrity of the document (proof that nothing has been faked or manipulated)

Steganography

Steganography: use of invisible watermarks for secret messages

Hiding of secret messages in other messages, such that their presence is not recognizable by a third party.

Example 1 for a Steganographic Message

A vacation postcard:

Liebe Kolleginnen! Wir genießen nun endlich unsere Ferien auf dieser Insel vor Spanien. Wetter gut, Unterkunft auch, ebenso das Essen. Toll! Gruß, J. D.

Algorithm

- count characters up to the next space
- odd number represents a binary 0, even number a binary 1
- interpretation of the resulting binary numbers in groups of eight as ASCII code

Result

- first 8 words 01010011, ASCII ‘S‘
- next 8 words 01001111, ASCII ‘O‘
- last 8 words 01010011, ASCII ‘S‘

The vacation greeting contains the hidden message “SOS“.

Example 2 for a Steganographic Message

An example of a message containing a so-called null cipher:

Fishing freshwater bends and saltwater coasts rewards anyone feeling stressed. Resourceful anglers usually find masterful leapers fun and admit swordfish rank overwhelming anyday.

Taking the third letter of each word, the following message is decoded:

“send lawyers guns and money“

Steganographic Methods

Substitutional Steganography

Replacement of a noisy component of the digital message by an encrypted secret message.

Constructive Steganography

Reproduction of noisy signals, based on a model of the original noise.

Digital Watermarks for Multimedia Documents

Additional information in a digital document, intended to prove the copyright, to trace every single commercial copy or to integrate meta data in pictures, videos, audio, 3D models or software.

Technical challenges

- development of watermarking algorithms
- testing of their robustness
- development of efficient watermarking tools for different types of multimedia documents

9.3 Robust Watermarks

Goal

Design watermarks that remain intact in the document even if it is manipulated (e.g., scaled)

Robust Watermarks for Digital Images

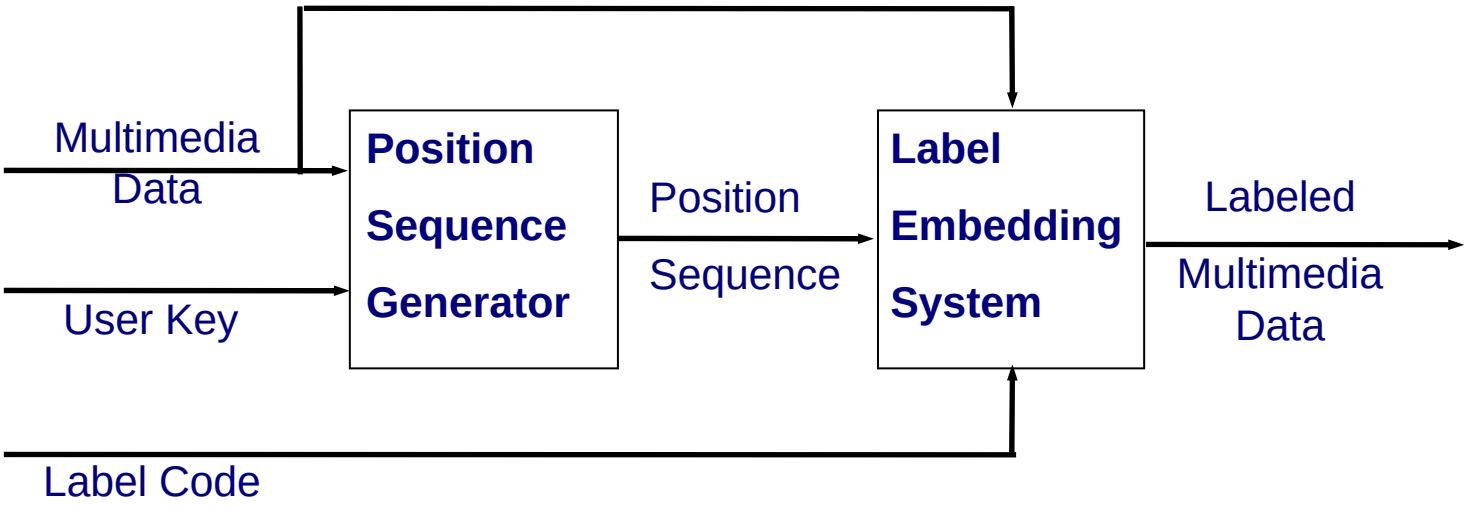
Method

- Modification of a single pixel in the image domain. Example: amplitude modulation in the blue channel
- Modification in the transformed domain: alteration of a DCT coefficient

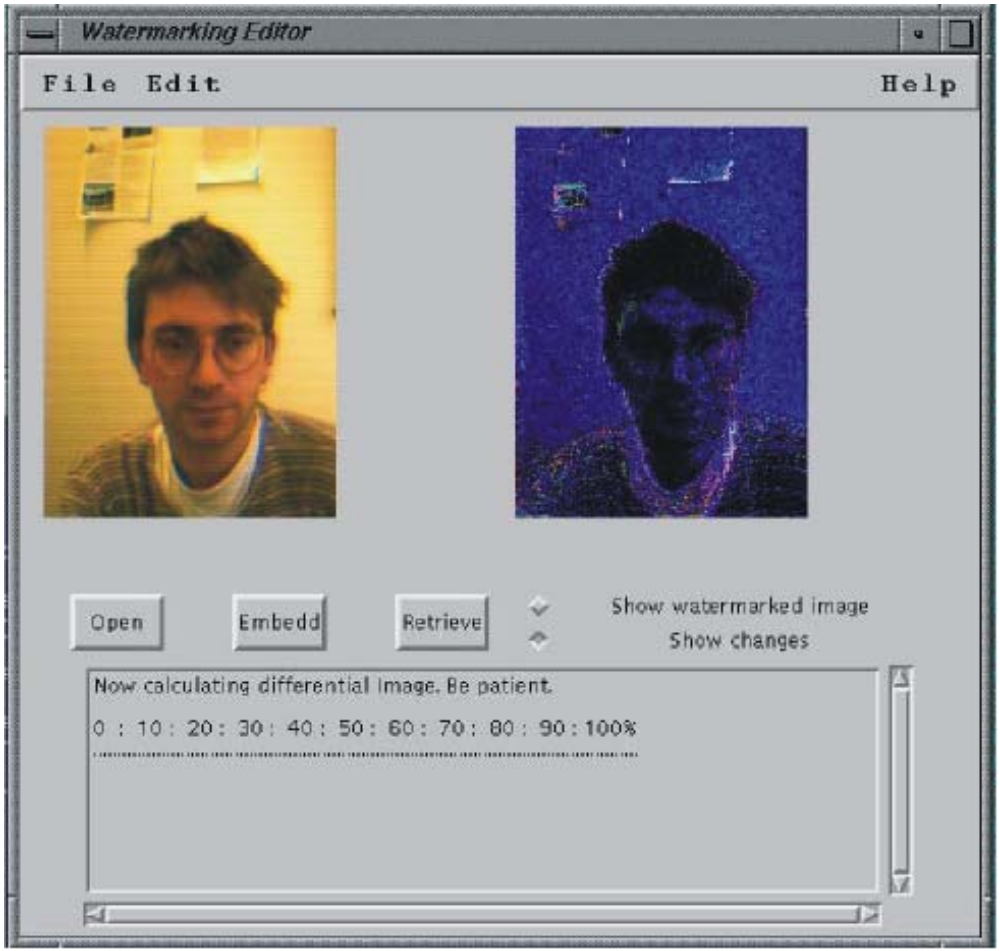
Commercial Products

- e.g. Signum Technologies, Digimark Technologies (Adobe Photoshop)

Insertion of Digital Watermarks



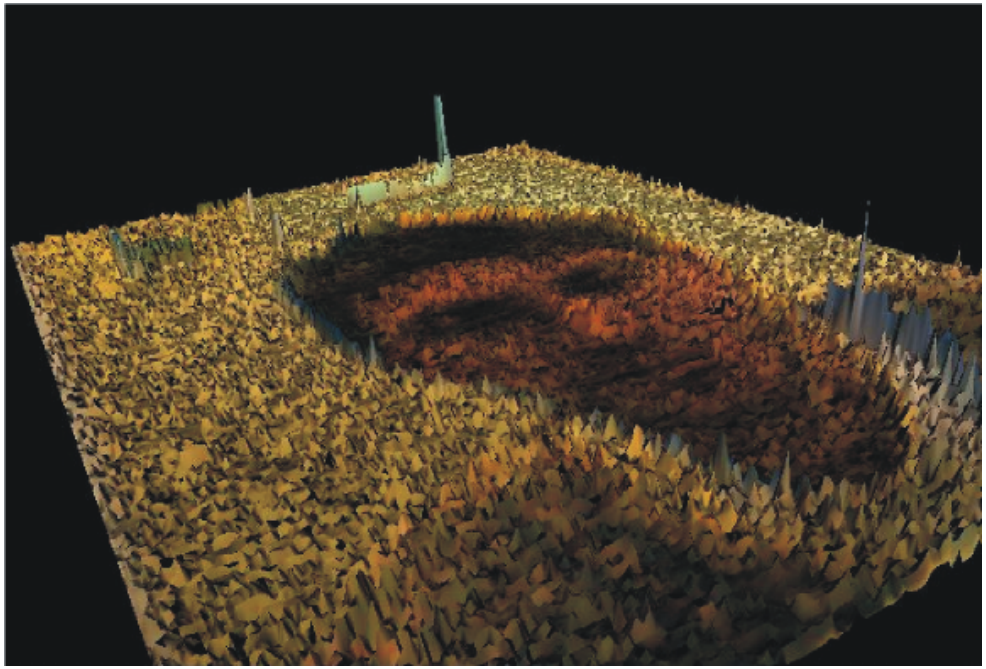
Blue Channel Method (1)



Blue Channel Method (2)

3D-Watermark

A method of analyzing image watermarking algorithms developed by FhG/IPSI in Darmstadt.



Frequency Domain Method by Zhao/Koch (1)

Embedding of watermarking data into a JPEG image

Bit sequence c_i, i = 1,...,n is to be embedded into the image.

Bit c_i is represented by the relationship between three frequency coefficients located in a specific diagonal region of a DCT block.

Eight positions of the DCT block, known to contain not much grey scale variance, are used for the method:

k \ l	0	1	2	3	4	5	6	7
0			2	3				
1		9	10	11				
2	16	17	18					
3								
4								
5								
6								
7								

Frequency Domain Method by Zhao/Koch (2)

Used combinations of three frequency coefficients

	A	B	C
1	2 (0,2)	9 (1,1)	10 (1,2)
2	9 (1,1)	2 (0,2)	10 (1,2)
3	3 (0,3)	10 (1,2)	11 (1,3)
4	10 (1,2)	3 (0,3)	11 (1,3)
5	9 (1,1)	2 (0,2)	10 (1,2)
6	2 (0,2)	9 (1,1)	10 (1,2)
7	9 (1,1)	16 (2,0)	2 (0,2)
8	16 (2,0)	9 (1,1)	2 (0,2)
9	2 (0,2)	9 (1,1)	16 (2,0)
10	9 (1,1)	2 (0,2)	16 (2,0)
11	10 (1,2)	17 (2,1)	3 (0,3)
12	17 (2,1)	10 (1,2)	3 (0,3)
13	10 (1,2)	3 (0,3)	17 (2,1)
14	3 (0,3)	10 (1,2)	17 (2,1)
15	9 (1,1)	16 (2,0)	17 (2,1)
16	16 (2,0)	9 (1,1)	17 (2,1)
17	10 (1,2)	17 (2,1)	18 (2,2)
18	17 (2,1)	10 (1,2)	18 (2,2)

Frequency Domain Method by Zhao/Koch (3)

Embedding of watermarking data

Pseudo-random selection of a combination of three out of the eight frequencies (selection from Y_A, Y_B, Y_C)

Comparison with a maximum allowable distance D; if exceeded mark as “invalid“.

Otherwise insert the frequency pattern (Y_A, Y_B, Y_C) for 0 or 1 into the positions of the matrix.

Bit	**1**	**1**	**1**	**1**	**0**	**0**	**0**	**0**	**invalid**		
Y_A	H	H	M	M	L	L	M	M	H	L	M
Y_B	H	M	H	M	L	M	L	M	L	H	M
Y_C	L	L	L	L	H	H	H	H	M	M	M

152	0	4	0	0	0	0	0
0	0	23	0	0	0	0	0
0	0	0	0	0	0	0	0
5	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

Frequency Domain Method by Zhao/Koch (4)

Embedding of bits into the three coefficients:

- If c_i=1: modify (Y_A, Y_B, Y_C) such that $Y_A > Y_C + D$ and $Y_B > Y_C + D$.
- If c_i=0: modify (Y_A, Y_B, Y_C) such that $Y_A + D < Y_C$ and $Y_B + D < Y_C$.

For a higher D, the embedded bit is more reliable but also more visible!

Bit	**1**	**1**	**1**	**1**	**0**	**0**	**0**	**0**	**invalid**		
Y_A	H	H	M	M	L	L	M	M	H	L	M
Y_B	H	M	H	M	L	M	L	M	L	H	M
Y_C	**L**	**L**	**L**	**L**	**H**	**H**	**H**	**H**	**M**	**M**	**M**

152	0	**4**	0	0	0	0	0
0	0	**23**	0	0	0	0	0
0	0	0	0	0	0	0	0
5	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

Frequency Domain Method by Zhao/Koch (5)

Reading out watermarking data

- pseudo-random selection of n blocks from the picture and a combination of three coefficients in the blocks
- Read Y_A, Y_B and Y_C
- Check for “invalid“
- If $Y_A >= Y_C + D$ and $Y_B >= Y_C + D$ return $c_i = 1$
- If $Y_A + D <= Y_C$ and $Y_B + D <= Y_C$ return $c_i = 0$

Bit	1	1	1	1	0	0	0	0	invalid		
Y_A	H	H	M	M	L	L	M	M	H	L	M
Y_B	H	M	H	M	L	M	L	M	L	H	M
Y_C	L	L	L	L	H	H	H	H	M	M	M

152	0	4	0	0	0	0	0
0	0	23	0	0	0	0	0
0	0	0	0	0	0	0	0
5	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

Frequency Domain Method by Zhao/Koch (6)

Advantages of the algorithm

- visual estimation when “invalid“ (would spoil visible image too much)
- parameter D determines robustness

Disadvantages of the algorithm

- shifting of blocks destroys the watermark
- scaling of the picture destroys the watermark, since in the original algorithm the pseudo-random sequence depends on the size of the picture (x- and y-dimension)
- security parameter (parameter D) is not adaptable to the content of the picture (edges!)
- sensitive to clipping
- sensitive to geometrical transformation: scaling, rotation, ...
- reproduction of the watermark possible

Reference: Jian Zhao and Eckhard Koch: Embedding robust labels into images for copyright protection. In: Proc. of the International Congress on Intellectual Property Rights for Specialized Information, Knowledge and New Technologies. Vienna, Austria, August 1995

Minimization of Visual Perception

Idea

Insertion of the watermark into areas of the image where the human eye notices the modification as little as possible.

In the example below the watermark is in the white background of the image.

Watermarks for Sound

Goals

- Tracking of illegal copies
- Assertion of the legitimate author resp. customer

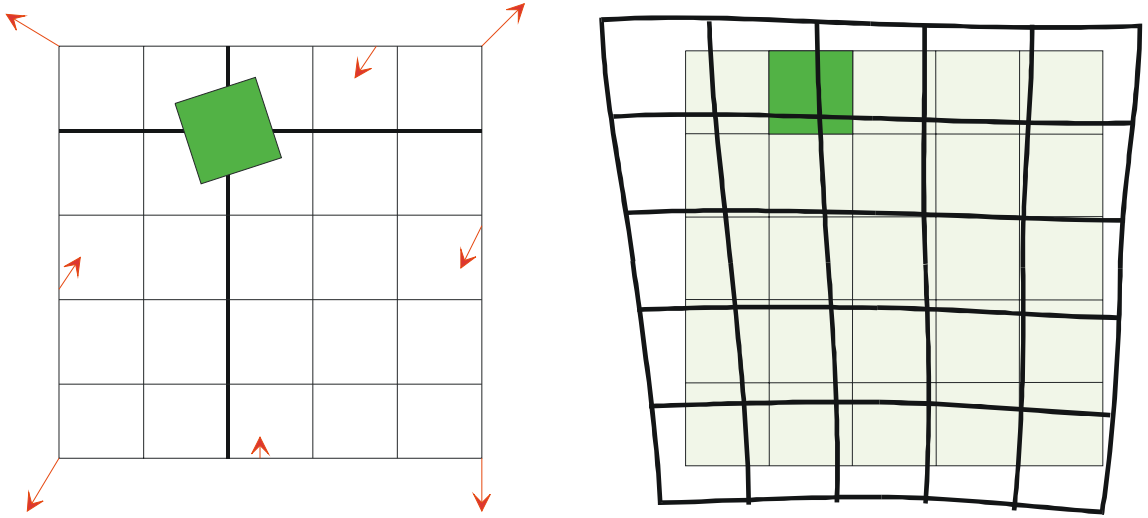
Methods

- Volume modulation
- Modulation of the noise signal
- Risk: compression captures and spoils watermark information (for example when exploiting psycho-physiological concealment effects in MP3)

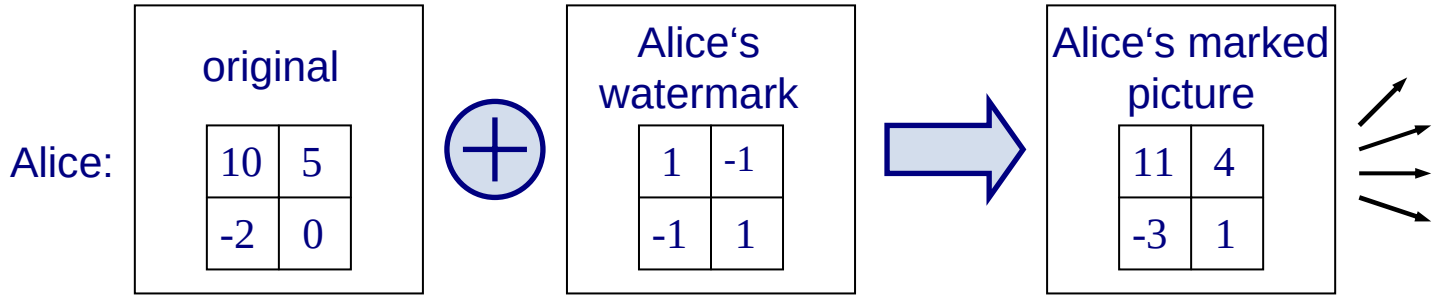
Unsolved Problems with Robust Watermarks

StirMark is an algorithm for the deletion of watermarks in documents. It simulates so-called re-sampling processes, similar to printing and re-scanning. Small, randomly chosen geometrical operations such as distortion, scaling, rotation or re-sampling with interpolation are carried out.

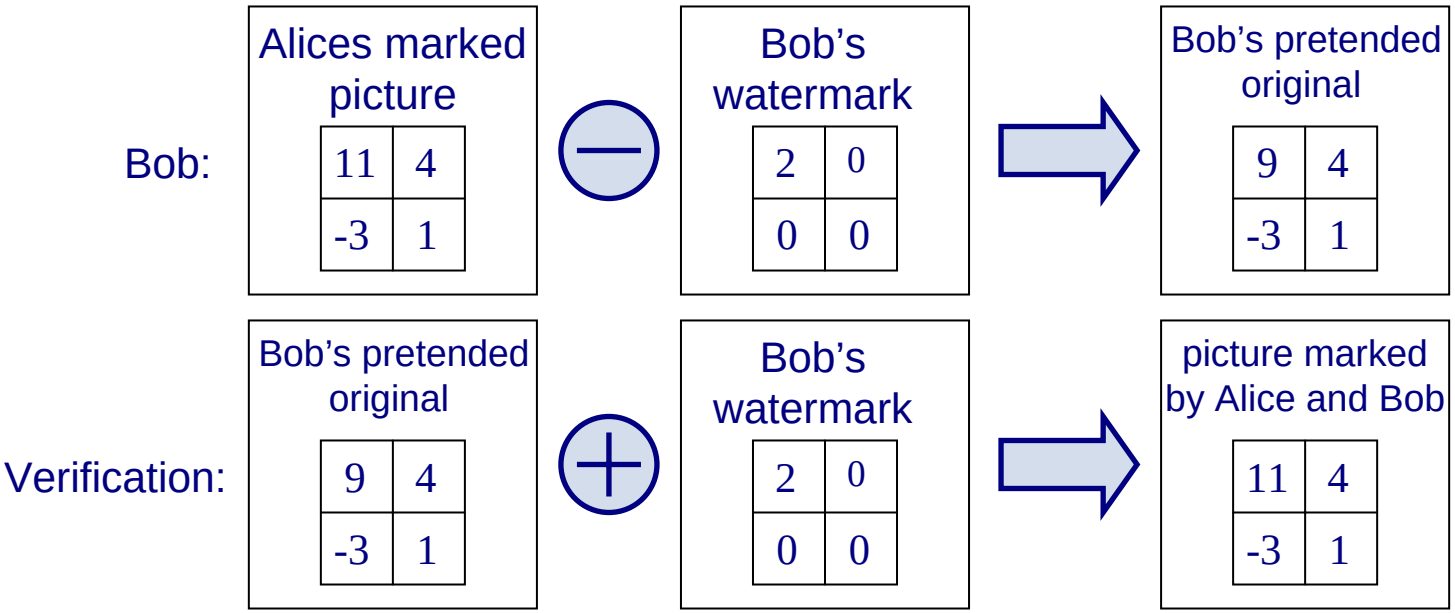
StirMark deletes almost all first-generation watermarks, without visibly damaging the document.



Secondary Marking to Fake Authorship



Here is a “multiple ownership attack“



Digital Fingerprinting

A different use of robust watermarking algorithms

Idea

Insertion of customer-specific information into every copy of the document.

- Allows the tracking of customer-specific copies
- Allows to trace back unauthorized distribution

Problem with conventional watermarking algorithms:

- The algorithms do not scale well for large numbers of customers.
- Customers may cooperate to attack watermarks by combining their different copies: “collusion attack“

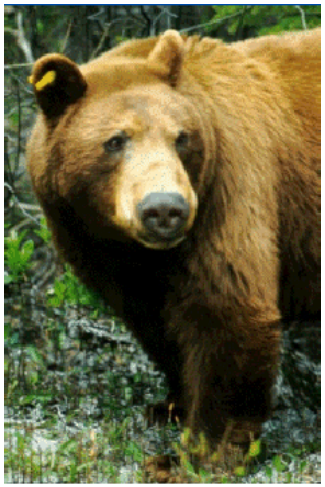
9.4 Fragile Watermarks

Goal

Protection of documents from alterations.

Example

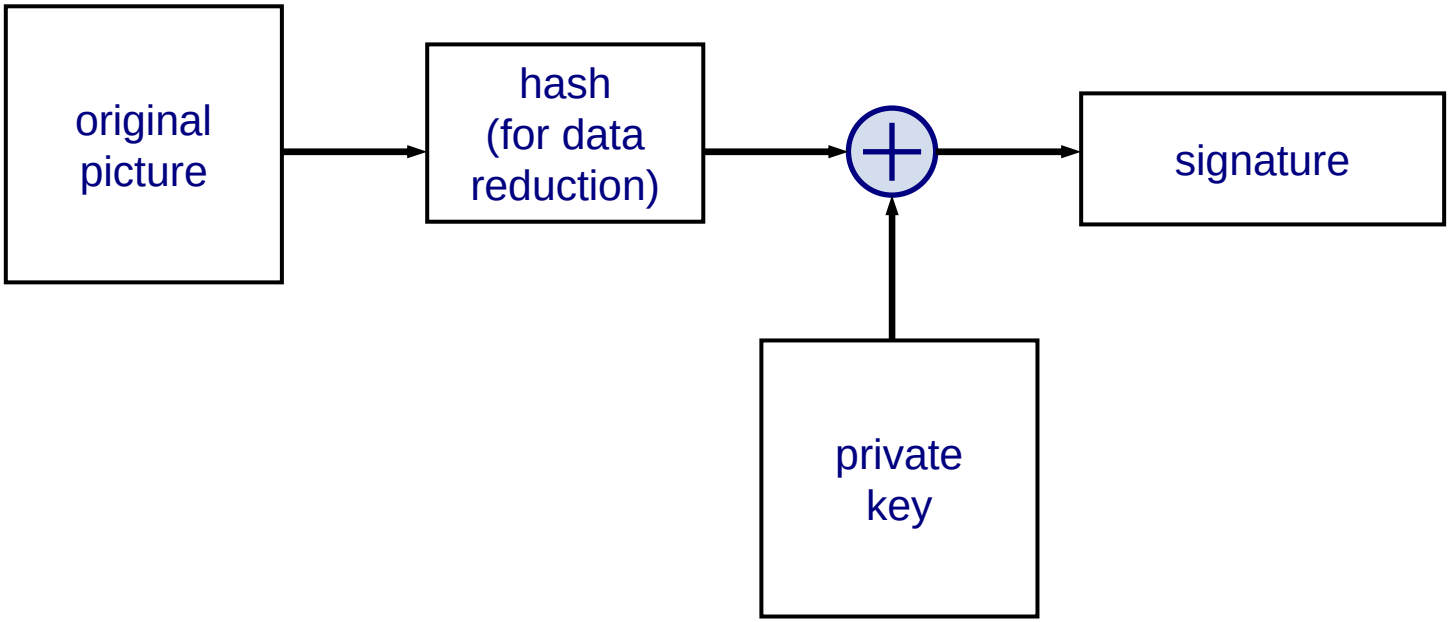
original



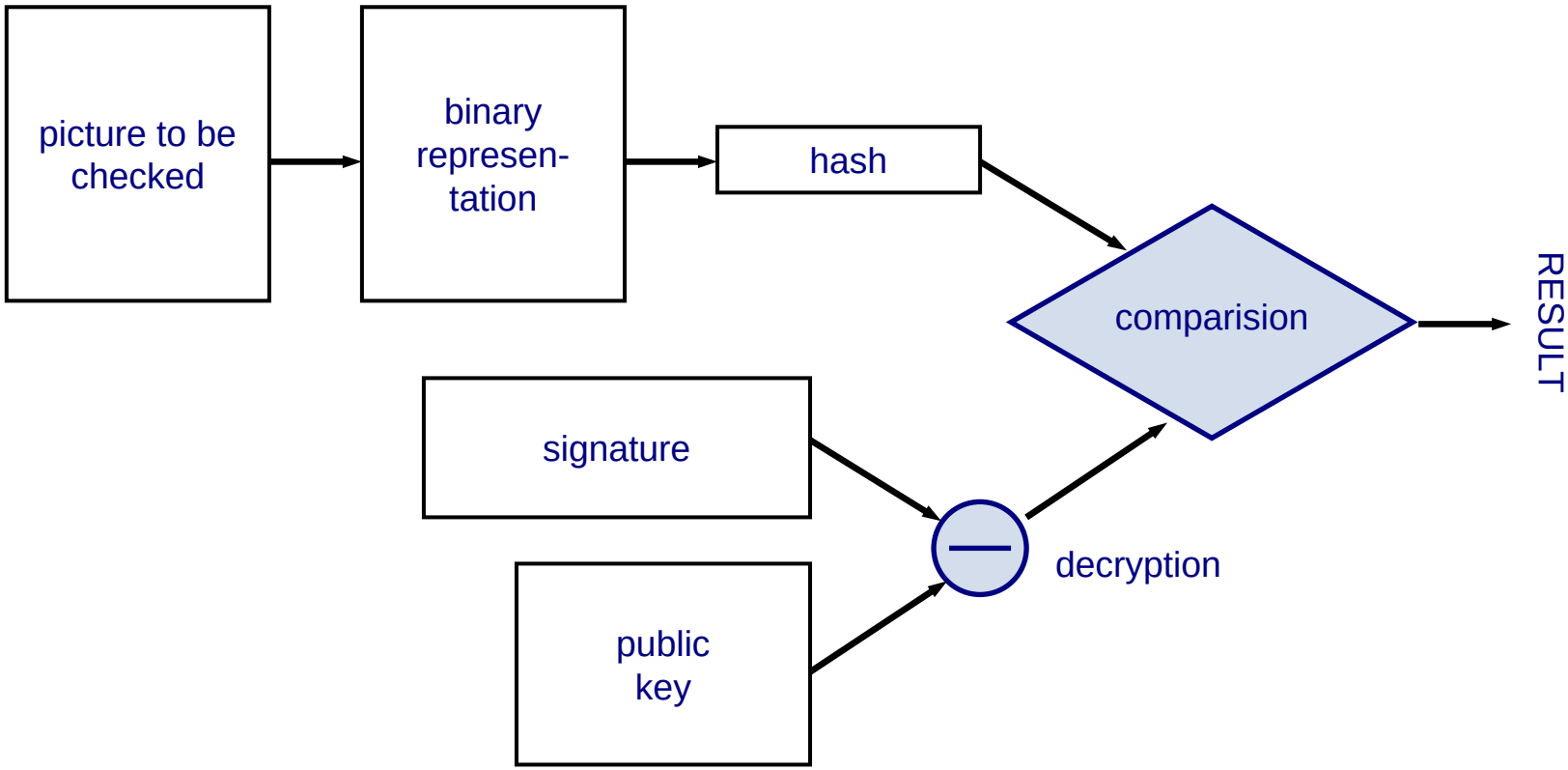
segment
bear

merge original and bear

First Approach: Digital Signature



Checking the Digital Signature



Summary

Watermarks

- A practical approach to copyright protection
- Allow to trace illegal reproduction, distribution or modifications
- Have significant importance for the Internet and in particular the WWW

Research Challenges

- Better robust watermarks needed to prove the origin of a multimedia document (not sensitive to StirMark)
- Better fragile watermarks needed to prove the integrity of multimedia documents
- Utilization for audio, 3D-scenes, software not yet well understood

Recommended reading: Jana Dittmann: Digitale Wasserzeichen. Grundlagen, Verfahren, Anwendungsgebiete. Springer-Verlag, 2000 (in German)