Lecture 8. (Part 2.) Digital watermarks

Definition. Digital watermarking (WM) is invisible practically changing of cover object (CO) for the purpose of embedding an additional message about this CO. Usually , an addition message is identification code of CO owner. Sometimes the fact of embedding should be kept in secret for illegal users. Typically WM have to be resistant to any natural and deliberate transforms.

Models of WM and classification :

- known CO for legal decoder (*informed decoder*),
- unknown CO for legal decoder *(«blind» decoder*),
- using CO fro legal encoder (*informed encoder*),
- *private WM* (it is allowed to extract WM for authorized users only),
-*public WM* (it is allowed to extract WM for any user),
- *«0»-bit WM* (the embedding means the fact of presence an identification owner's code only),
- *multiple bit WM* (the embedded message consists of several bits).

The main attacks on WM:

1. Detecting of WM embedded into CO (for private WM).
2. Extraction of the embedded WM (for secret WM).
3. Removal of WM *without significant distortion of CO*.
4. Unauthorized embedding of WM into CO without its significant distortion .

Kerckhoff's assumption for WM :

Attacker knows everything about algorithms of embedding and detecting with exception of CO and possibly stegokey . (In fact the knowledge of CO by an attacker simply allows him to "remove" WM .)

Criteria of WM system efficiency :

- the probability P_{fa} of false alarm WM detection (for 0-bit WM),

- the probability P_m of WM missing (for 0-bit WM),

- the probability P_e of incorrect bit extraction by legal users (for multi bit WM), including WM under natural and deliberate transforms which do not corrupt CO significantly ,

- CO quality after WM embedding that as a first approximation is estimated by signal –to-noise ratio but more precisely it is estimated by experts with the use of special criteria depending on type of CO and its application ,

- date embedding rate (for multi bit WM) as a ratio of the number of embedded bits to total size of CO; typically it is calculated in bit/sample of signal or in bit/pixel of the image.

The main types of CO which are used in WM applications:

- motionless images,
- motion images (video and TV),
- audio WM (speech and music),
- graphical presentations of text and schemes ,
- source codes (for soft ware),
- topology of micro chips,
- description of chemical formulas,
- internet-protocols.

The main distinction of SG and WM. SG require undetectability by unauthorized users whereas it is not necessary always to be resistant against unauthorized removal. WM are not necessary to be undetectable but as a rule they should be resistant against unauthorized removal and inserting .

Natural and deliberate transforms (attacks) on signals containing WM *:*

- addition of noise,

- filtering,

- scaling,

-cropping,

- requantization,

- insertion and deletions of samples,

- compression and decompression,

- estimation and subtraction of WM,

- geometrical transforms of the images,

- and so on.

The main problems of WM design:

1. It is difficult to describe theoretical model of attacks on WM which do not produce corruption of CO (audio and video) noticeable for individuals .

2. Statistical distributions of CO are known not completely that makes hardness to design legal decoders of WM under the presence of different attacks .

3. In order to remove WM adversaries may form a coalitions among users that results in a new setting of WM design-resistance against coalition attack known as *fingerprinting problem .*

The main applications of WM [19]:

1. Broadcast monitoring.
2. Owner identification.
3. Proof of ownership.
4. Transaction tracking (Fingerprinting).
5. Content authentication.
6. Copy control.
7. Device control.

Let us consider these applications one by one.

1.Broadcast monitoring.

Advertisers want to sure that they receive all of the air time they purchase from broadcaster.

A passive monitoring system consists of computer that monitors broadcast and compares the received signals with a database of known Works. When the comparison locates a match , the song , film ,TV program , or commercial being aired can be identified.

Active monitoring is to place the identification information in a separate area of the broadcast signal that can be automatically extracted later.

For digital Works , there are similar active techniques that store identification codes in file headers. *Watermarking* is an obvious alternative method of coding identification information for active monitoring .It has the advantage of existing within the content itself , rather than exploiting a particular segment of broadcast equipment , including both digital and analog transmission.

This type of WM should be resistant to unauthorized embedding only.

2. Owner identification

This function serves in order to specify the identity of the creator or person whose permission must be obtained. When decoder recognizes WM , it contacts a central database over the Internet , and uses the watermark message as a key to find contact information for the Work owner.
In such WM application nothing deliberate attacks are considered as a rule in order to remove or to embed false WM .

Example. You can see in the next slide a picture of resort area in which is embedded information about the tourist company that offers a packet of service to visit this area.

Picture of resort area

Picture of resort area
with embedded logo

Logo of tourist company
to be embedded

Extracted logo of tourist
company

3. Proof of Ownership.

Difference with previous case – WM is necessary to prove *ownership in the court*.
The owner owing to WM can avoid a registering of Works with the Office of Copyrights and Patents.
Such application of WM should be resistant both to unauthorized removal and unauthorized embedding (see for the last case ambiguity attacks in the sequel).

4. Transaction tracking

WM in such application has an information about legal buyers (“fingerprinting”), that allows to trace illegal distributers of Works (*traitors (or pirates*) .
(In a particular case WM protects DVD against their illegal distribution.)
WM should be multi bit and resistant against removal attack .

5. Content authentication.

It is well known authentication in cryptography (digital signature (DS) for example)
But if DS is appended to Work it can be lost in normal usage and then Work can no longer be authenticated.
WM allows to embed DS into Work itself without its significant distortion.

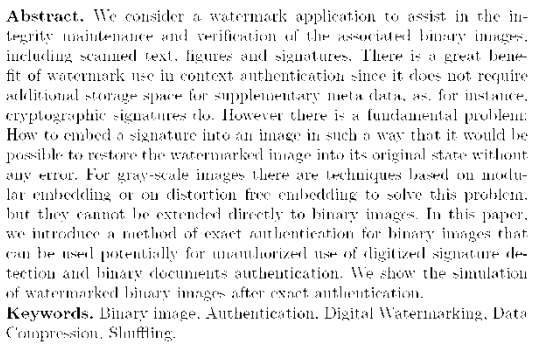
Two types of authentication based on WM:

- *exact authentication* (if a corruption even one bit in Work is not allowed)
- *selective authentication* (if some corruptions of Work (like transform to JPEG format or an addition of small noise) are allowed whereas others (like image contour transforms) are not allowed and should be detected.

In such application of WM there are no attacks if cryptographic resistance of authentication (DS) is taken for granted.

Remark. The main problem to design exact WM is to provide its *reversibility* after WM extraction .It seems to be difficult (and even unsolved problem at single glance !) because embedding procedure results as a rule in corruption of CO. How to resolve this seeming contradiction will be shown in the lecture devoted to WM authentication.

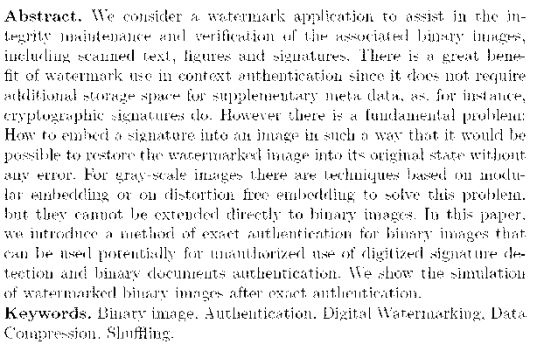
Example of exact authentication for binary image



Abstract. We consider a watermark application to assist in the integrity maintenance and verification of the associated binary images, including scanned text, figures and signatures. There is a great benefit of watermark use in context authentication since it does not require additional storage space for supplementary meta data, as, for instance, cryptographic signatures do. However there is a fundamental problem: How to embed a signature into an image in such a way that it would be possible to restore the watermarked image into its original state without any error. For gray-scale images there are techniques based on modular embedding or on distortion free embedding to solve this problem, but they cannot be extended directly to binary images. In this paper, we introduce a method of exact authentication for binary images that can be used potentially for unauthorized use of digitized signature detection and binary documents authentication. We show the simulation of watermarked binary images after exact authentication.

Keywords. Binary image, Authentication, Digital Watermarking, Data Compression, Shuffling.

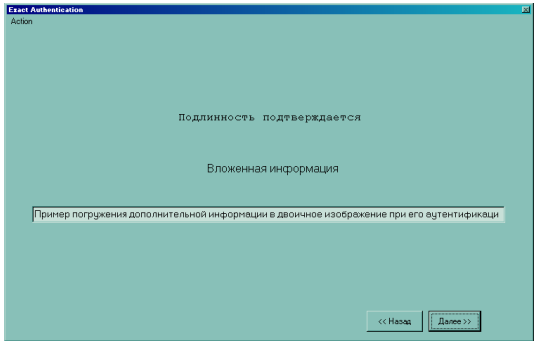
a) Original CO



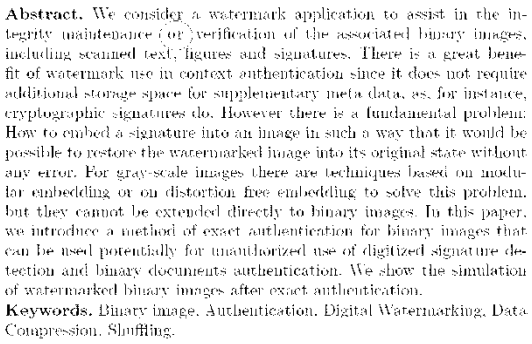
Abstract. We consider a watermark application to assist in the integrity maintenance and verification of the associated binary images, including scanned text, figures and signatures. There is a great benefit of watermark use in context authentication since it does not require additional storage space for supplementary meta data, as, for instance, cryptographic signatures do. However there is a fundamental problem: How to embed a signature into an image in such a way that it would be possible to restore the watermarked image into its original state without any error. For gray-scale images there are techniques based on modular embedding or on distortion free embedding to solve this problem, but they cannot be extended directly to binary images. In this paper, we introduce a method of exact authentication for binary images that can be used potentially for unauthorized use of digitized signature detection and binary documents authentication. We show the simulation of watermarked binary images after exact authentication.

Keywords. Binary image, Authentication, Digital Watermarking, Data Compression, Shuffling.

b) CO after embedding of 64 bits of authenticator and 7864 bits of additional information



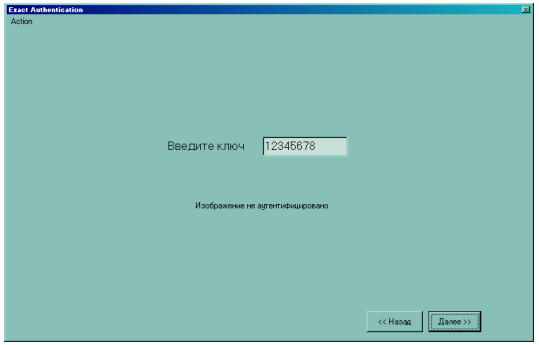
c) Verification of authentity



Abstract. We consider a watermark application to assist in the integrity maintenance (or) verification of the associated binary images, including scanned text, figures and signatures. There is a great benefit of watermark use in context authentication since it does not require additional storage space for supplementary meta data, as, for instance, cryptographic signatures do. However there is a fundamental problem: How to embed a signature into an image in such a way that it would be possible to restore the watermarked image into its original state without any error. For gray-scale images there are techniques based on modular embedding or on distortion free embedding to solve this problem, but they cannot be extended directly to binary images. In this paper, we introduce a method of exact authentication for binary images that can be used potentially for unauthorized use of digitized signature detection and binary documents authentication. We show the simulation of watermarked binary images after exact authentication.

Keywords. Binary image, Authentication, Digital Watermarking, Data Compression, Shuffling.

d) CO after corruption



e) Verification of authentity after some corruption of CO

Types of medical images :

- **EPS** - Cardiac Electrophysiology;
- **DX** - Digital Radiography;
- **ECG** - Electrocardiography;
- **ES** - Endoscopy;
- **IVUS** - Intravascular Ultrasound;
- **MR** - Magnetic Resonance;
- **US** - Ultrasound;
- **XA** - X-Ray Angiography;
- **BI** -Biomagnetic imaging ctr.;

Formats and parameters of medical images :

- Conventional plain (Magnetic Resonance , computer tomography);
- Color **CMYK** and **RGB** (- Ultrasound; positronic-emission tomography);
- Luminance and contrast (Window Level, L and Window width, W) of the image) , where :

L- the averaged value of image luminance for all images,

W - the number of quantization levels

- The main formats : conventional BMP, JPEG and special ones
  - **DICOM** (The Digital Imaging and Communications in Medicine standard committee)
  - **HL7** (Health Level Seven)
  - **IHE** (Integrating the Healthcare Enterprise)

The main features of DICOM :

DICOM embraces both image and text information about patient and results of investigations.

- **PACS** (*Picture Archiving and Communication System*) — it is assumed a creation of special remote files on DICOM Server and DICOM Server, which are very fast accessible for a viewing on DICOM network

Problems of DICOM Format:

- DICOM files have significant sizes and require high quality communication channels - this format cannot be read by conventional applications and requires special ones, - require specially educated personal .
- Company Agfa Health Care has been created unique product Xero (Impax Data Center Viewer) for a viewing of medical images which embrases two Worlds of standards – "conventional" and medical ones. Digital images can be available through any web-browser .
- Great defect : Design of medical date centers connecting tens hospitals is very hard and costly problem.

Important problems :

1. Transmission of digital medical images between hospitals ctr.

2.Verifivcation of image authentity.

3.Information about patients should be sent jointly with digital medical images.

Solution to these problems:

- p. 1 is solved by convergence of special formats to BMP or to JPEG
- p. 2 is solved by authentication or digital signature.

Defects of conventional authentication :

- There are needed extra size for digital signature (for strong DS about 1000 bits).
- Loss of DS in image transmission or its corruption.

Solution of defects above:

- Embed DS into image itself jointly with extra information.
- (Watermarking –WM)

The main requirements to authentication based on embedding into the image :

1. After WM extraction image has to be recovered
2. Corruption even one bit results in a detection of this fact.
3. Deliberate corruption of the images is possible only after braking of DS.
4. Image has to be recognized before WM extraction.

Remark: It is possible to verify CO integrity even after JPEG compression.

6. Copy control

This application do not serve to trace traitors (or pirates) . It aims to prevent people from making illegal copies of copyrighted content.

Naïve approach: In every recording device is fitted with a WM detector. Then the devices could be made to prohibit recording whenever a “never-copy “ WM is detected at its input.
But how do we ensure that every recorder contains a WM detector? The direct solution to this problem would be to require WM detectors in recorders by law. However , no such law currently exists , and enacting one would be difficult at best.

More realistic approach (playback control): The customer has a choice between a compliant device that can play legal , purchased content but cannot play pirate content or a noncompliant device that can play pirated content but not purchased content. The hope is that most customers will choose a compliant option. The scheme of such method is shown in Fig.1 , next slide.

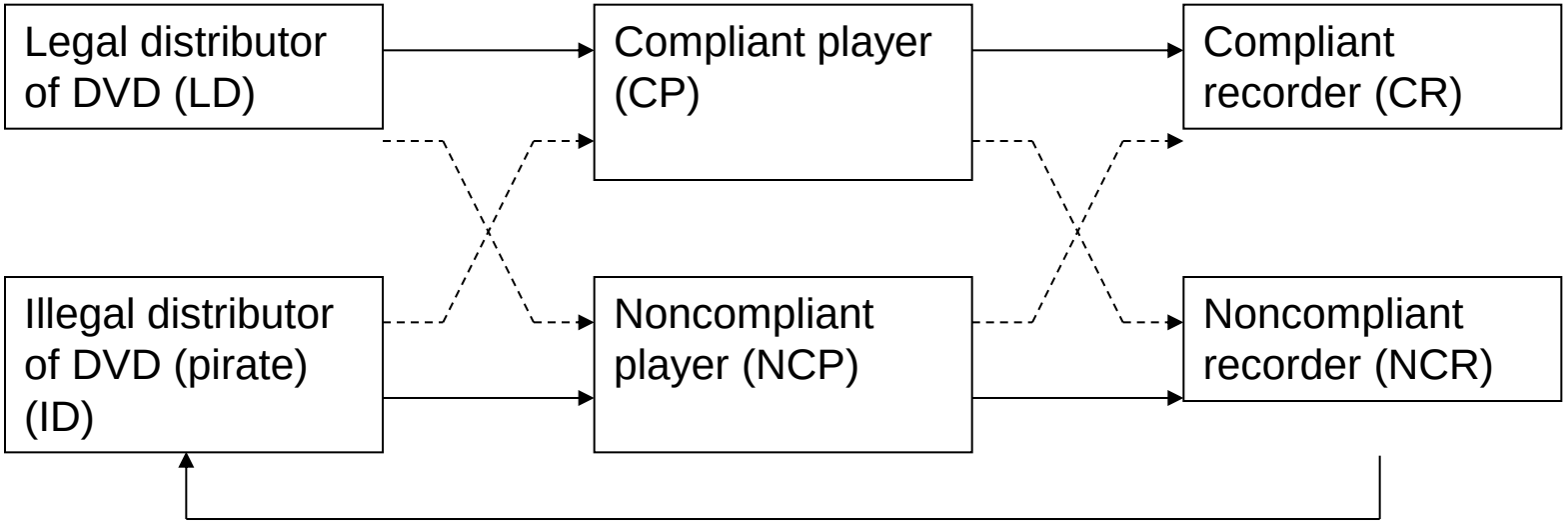


Fig. 1 – Copy control scheme

CP – plays only legal DVD ,
NCP – playas only illegal DVD,
CR – records only if WM is absent in DVD,
NCR – records any DVD,
«———» – means allowed operation,
«- - - - -» – means non-allowed operation

Legal DVD can be encrypted by LD and decrypted on CP, but not on NCP.
Decrypted DVD cannot be recorded on CR.
If legal client is «pirate», then he (or she) be able to record DVD on NCR.
Illegal copies of DVD, recorded on NCR, can be illegally distributed by ID to any clients but the last can play these illegal copies only on NCR.
Conclusion. Clients are free to buy either CP/CR or NCP/NCR.

7. Device control.

This is a generalization of “copy control” application when a device is able to detect WM and performs some operations..

Example. A unique identifier is embedded into printed and distributed images such as magazine advertisements ,packaging , tickets , and so on. After the image is recaptured by a digital camera , the WM is read by MediaBridge software on PC and the identifier is used to direct a web browser to an associated web site.