DIGITAL RIGHTS MANAGEMENT

TOPICS TO BE COVERED

Introduction

- **Need for copyright protection & DRM**
- **Watermarking and Encryption**
- **Case studies**

What is watermarking –

- **History and motivation**
- **Comparison to Steganography**
- **Uses of water marking**
- **Desirable qualities of watermarks**
- **State of the art algorithms for text, images, video, audio**

What is encryption –

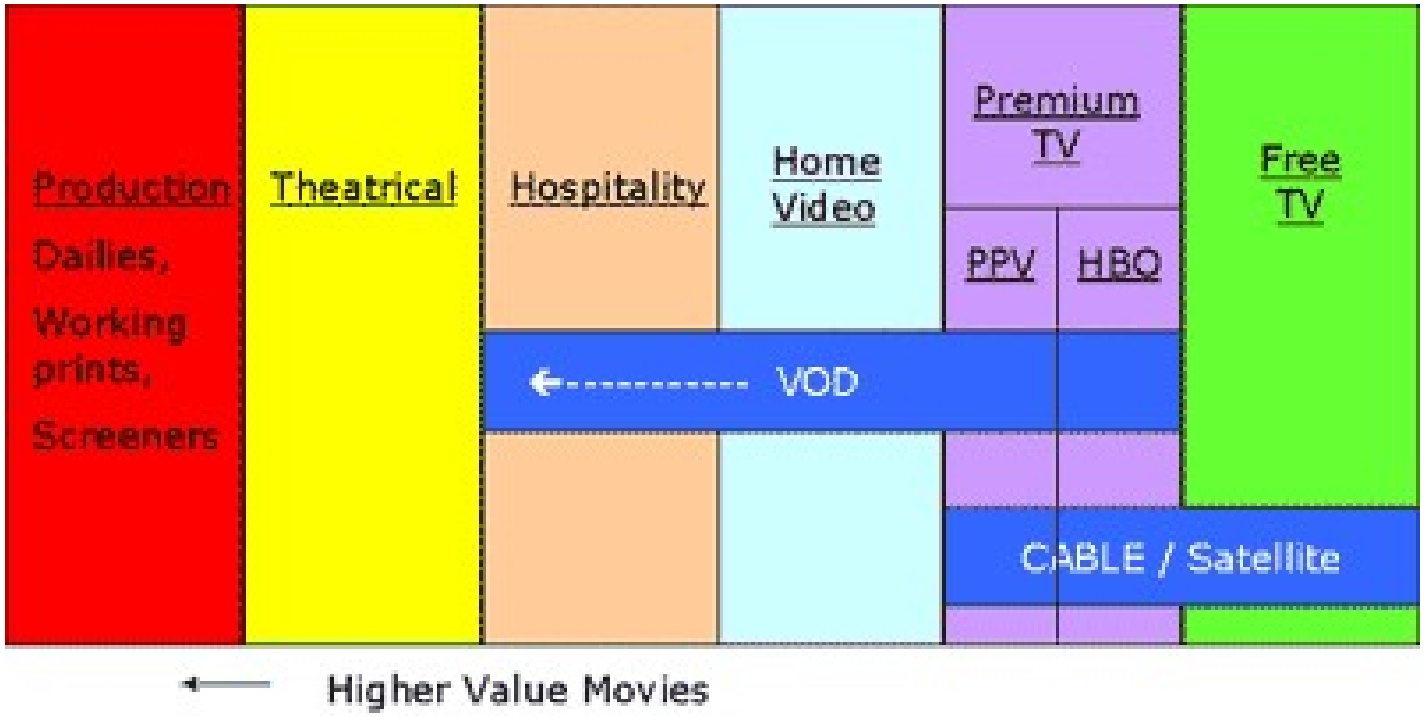
- **Definition**
- **Comparison to Cryptography**
- **State of the art algorithms**

EXAMPLES

Cable / Satellite distribution

Video on Demand

Movie Distribution



DIGITAL RIGHTS MANAGEMENT

Who owns it?

Who can modify it?

Who can distribute it?

Who can access/consume it?

How do you prevent unauthorized access? Can you catch and trace unauthorized distribution?

Comes under a general framework of DRM

- **Watermarking**
- **Encryption**

This not an easy problem! – especially in a distribution pipeline that has established standards

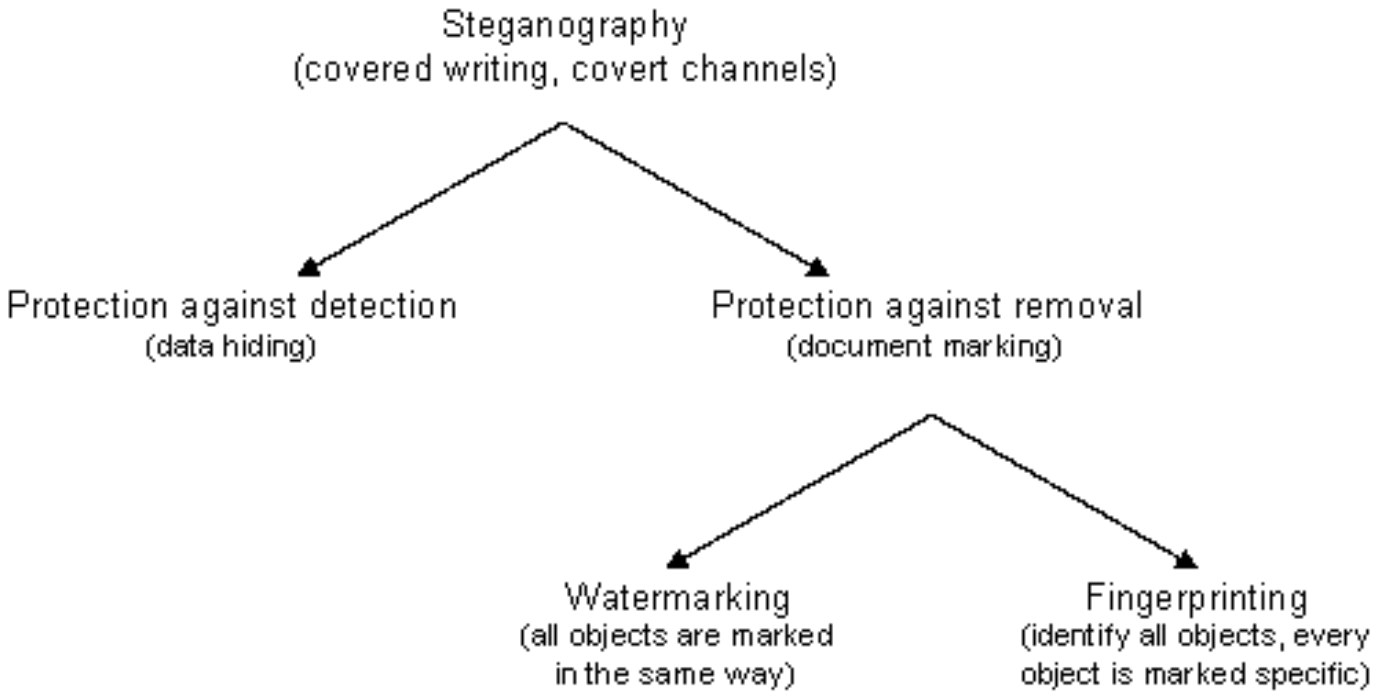
WATERMARKING

Digital Media Watermarking is the art/technique of embedding information in a media type. The information is called a watermark and is used to attest the media data in some manner -

- **Who owns it? *(Lawful owner)***
- **Who can access/consume it? (*Intended recipient*)**
- **Who can distribute it? *(Protected Distribution)***
- **Who can modify it?**
- **Other miscellaneous information - ?**

Is this the same as Steganography?

STEGANOGRAPHY



EXAMPLE OF DATA HIDING

What is the hidden message in this paragraph?

MPEG4 was established in 2000 but is recently getting wider acceptance. One definitive reason for this is a market ready for deploying applications, which are good and useful. However, the level of piracy today is a grade higher than it was in the previous years. As a result in today's market, digital content is easily copied and this is the very reason, which has forced a necessary course of action on the part of content owners. One method is the use of watermarking and encryption, which is not only helpful to curb piracy but now it is also not difficult to catch the perpetrators using digital forensics. So, content industries are hopeful that virtually everyone involved in piracy will be caught. The responsible party will hopefully always be brought to justice.

APPLICATIONS OF DIGITAL WATERMARKING

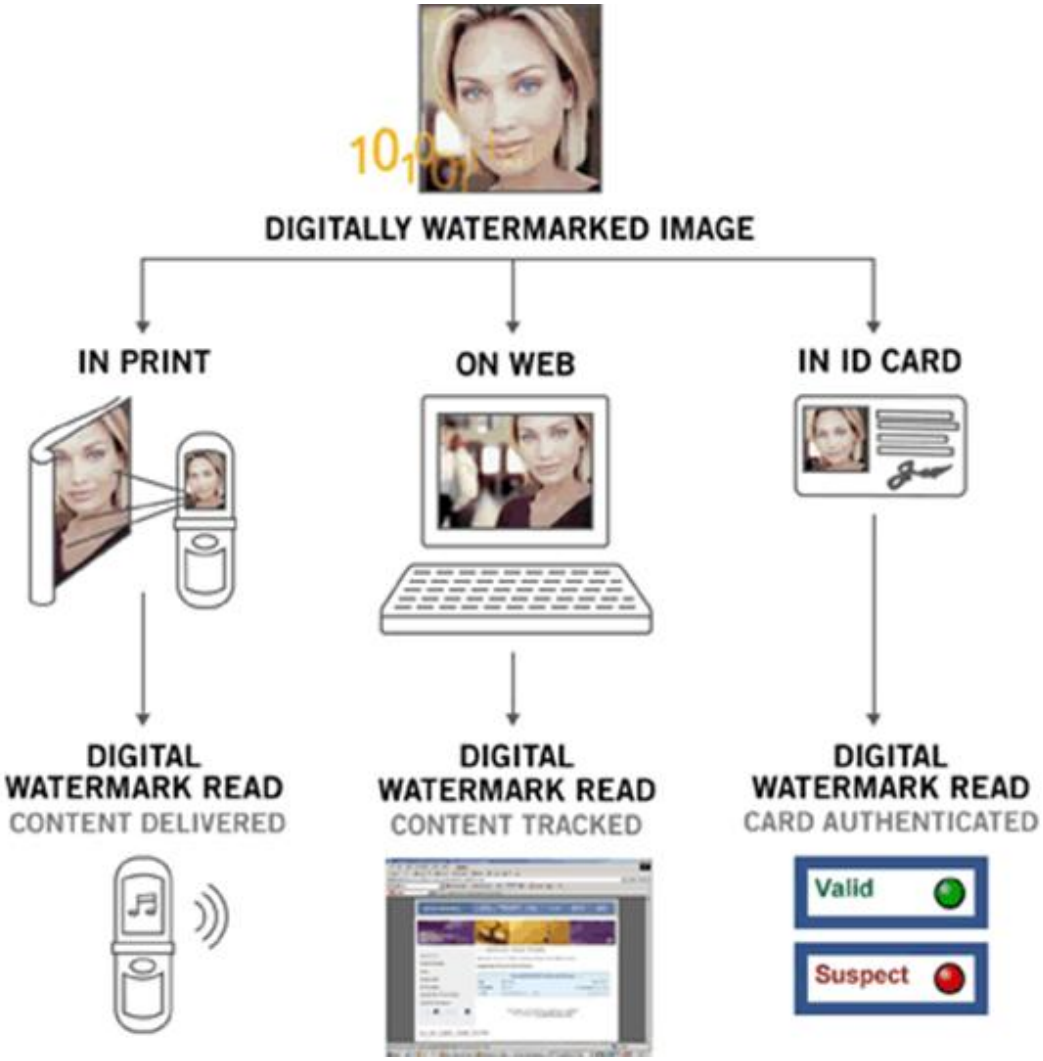
Copyright protection

Tracking and tracing media objects – creation, manipulation and modification history

Identify the intended recipient - Embedding of control, descriptive or reference information eg: pay-per-use application (audio, video, broadcasting, electronic commerce, digital media)

Providing different authentication and access levels to the data

APPLICATIONS OF DIGITAL WATERMARKING



CLASSIFICATION OF WATERMARKS

There are various ways of classifying watermarks depending upon applications and usage

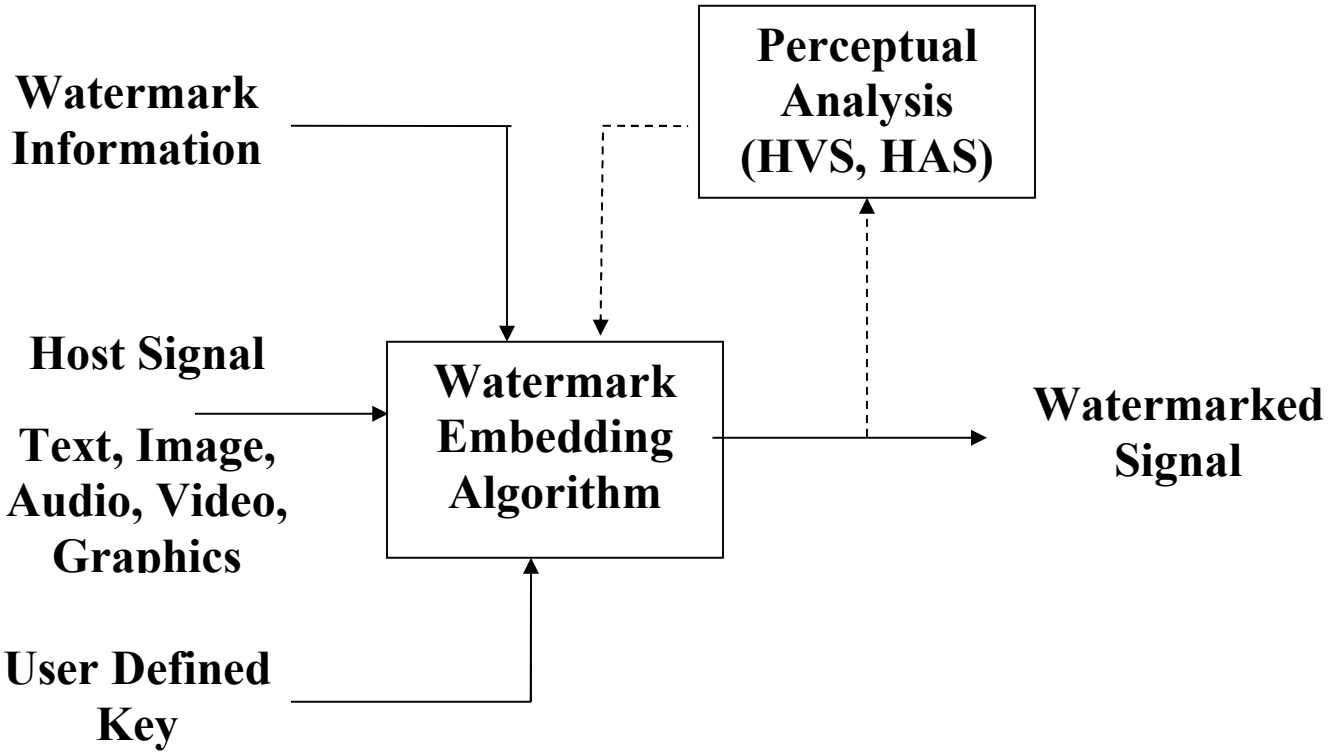
- **Visible Vs Invisible watermarks**
- **Public Vs Private watermarks**
- **Fragile Watermarks**
- **Perceptible or Transparent Watermarks**
- **Bit-stream Watermarks**

Invisible watermarks - More desirable and useful, Used for identifying source, owner, distributor or authorized consumer, Can be permanent also, unalterably mark the media

VISIBLE/INVISIBLE WATERMARKS

Purpose	Visible	Invisible
Deterrence against theft	*Primary*	*Secondary*
Digital notarization and authentication	*Secondary*	*Primary*
Diminish Commercial Value	*Primary*	*Primary*
Discourage Unauthorized Duplication	*Primary*	*Secondary*
Identify Source	*Primary*	*Secondary*

WATERMARK INSERTION



DESIRABLE QUALITIES OF WATER MARKING

Useful watermarking techniques need good understanding of signal processing, communication theory and HVS/HAS.

Desirable Qualities for watermarking digital data

- **Perceptual Transparency -**
- **Security – watermark must survive attacks**
- **Payload of Watermark – the embedded information must be a minimal set**
- **Detection & Recovery – should be detected easily, possibly without original image**
- **Removal – must be difficult, if not impossible to remove, at least without perceptibly degrading the media type.**

SECURITY – ATTACKS ON MEDIA

Attacks correspond to manipulations on media. Attacks may be deliberate or unintentional.

Intentional attacks – these operations are purposefully applied to either remove/detect/replace already in place watermarks. The operation would depend on the media type and embedding scheme.

Unintentional attacks – these operations happen as a result of creating and distributing content. Eg compression/decompression, transmission, filtering etc.

CLASSIFICATION OF MALICIOUS ATTACKS

Basic Attacks - take advantage of limitations in the design of the embedding techniques

Robustness Attacks - attempt to diminish or remove the presence of a watermark eg random geometric distortions. *Stirmark* is a standard to benchmark robustness

Presentation Attacks - modify the content of the file in order to prevent the detection of the watermark

Interpretation Attacks - involve finding a situation in which the assertion of ownership is prevented

Implementation Attacks – the vulnerability of the implementation technique/software may make it possible for attackers to deceive the process.

ALGORITHMS

In order to embed watermark information in host data, watermark embedding techniques apply minor modifications to the host data in a perceptually invisible manner

There are various classifications of watermarking algorithms depending on whether or not original data is needed to extract the watermark.

Algorithms can be also classified depending on domain of operation/embedding

- Spatial Domain watermarking
- Frequency Domain watermarking

WATERMARKING FOR TEXT

Text documents are discrete information sources! – Algorithms are divided into hiding information into the semantics, or into the text format

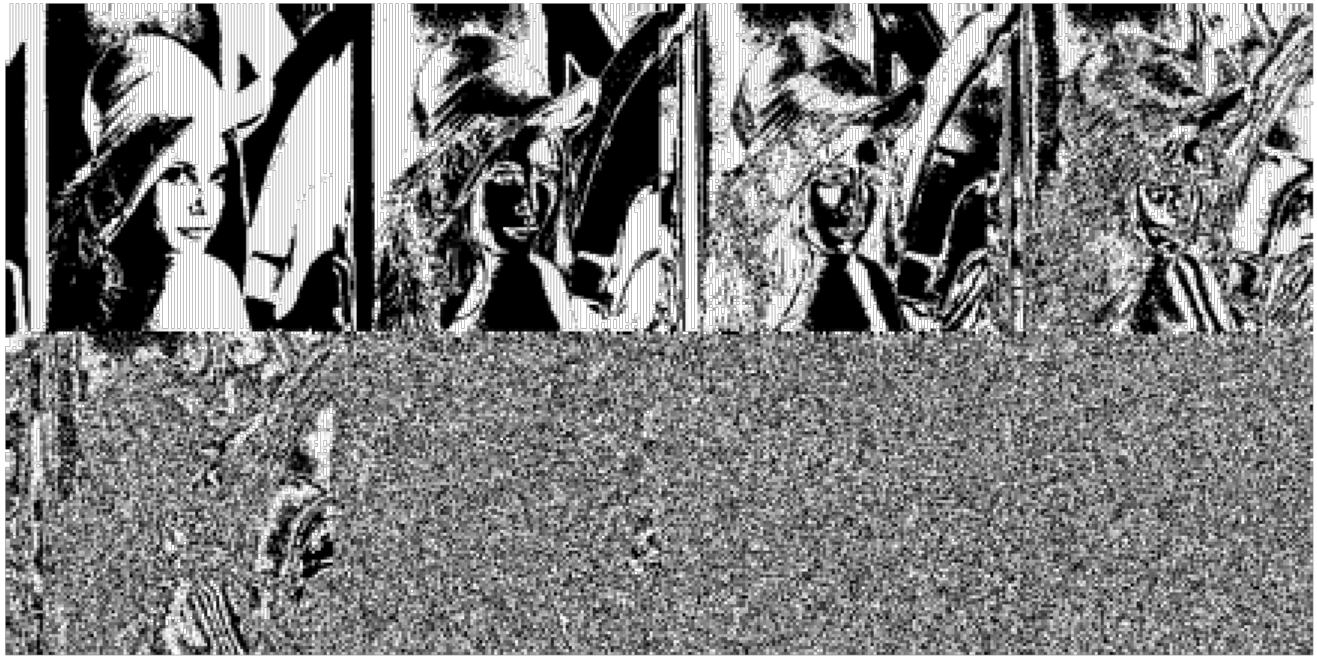
In semantic-based watermarking, the text is designed around the message to be hidden. Thus, misleading information covers watermark information.

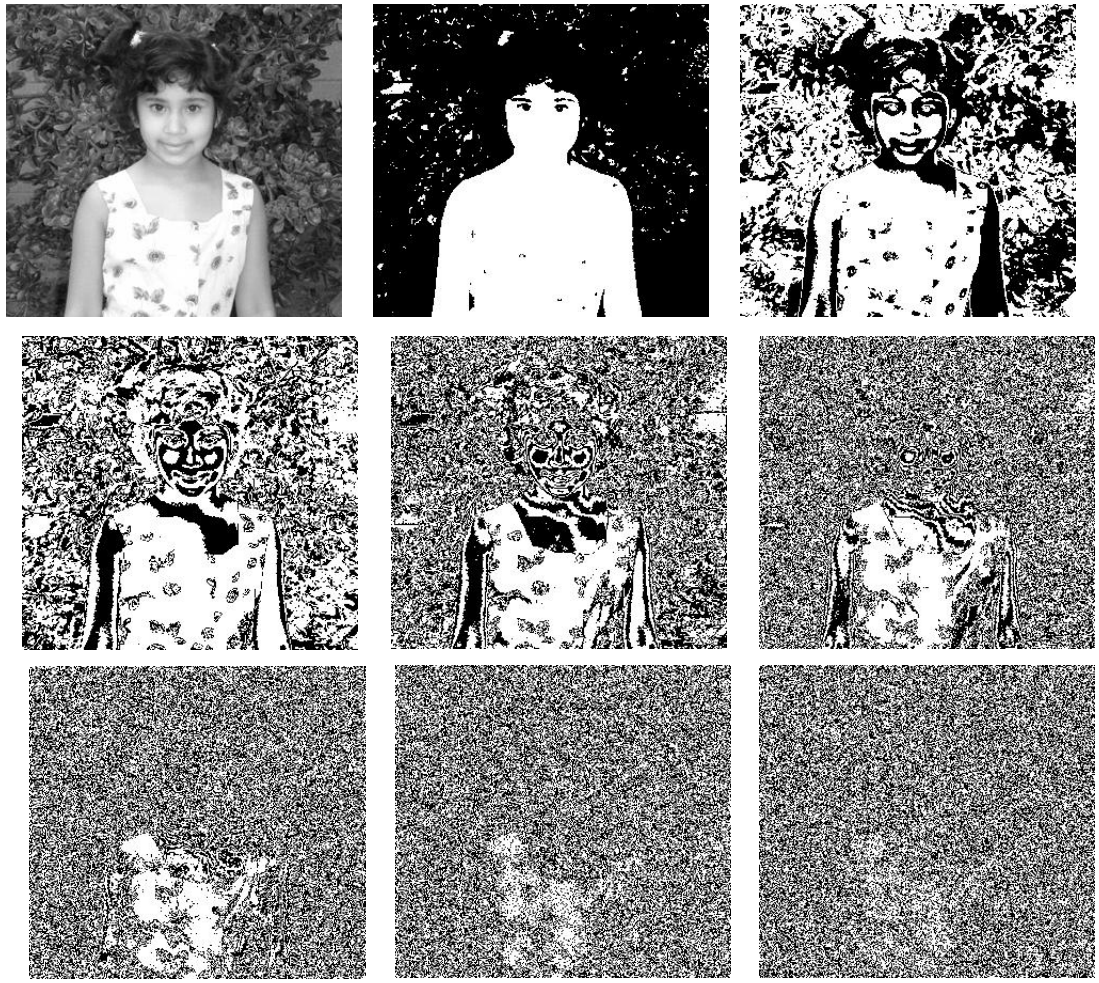
By text format modification, the layout and appearance or both are modified. Commonly used techniques to hide watermark information are

- **Line shift coding,**
- **Word shift coding**
- **Feature coding**

WATER MARKING FOR IMAGES

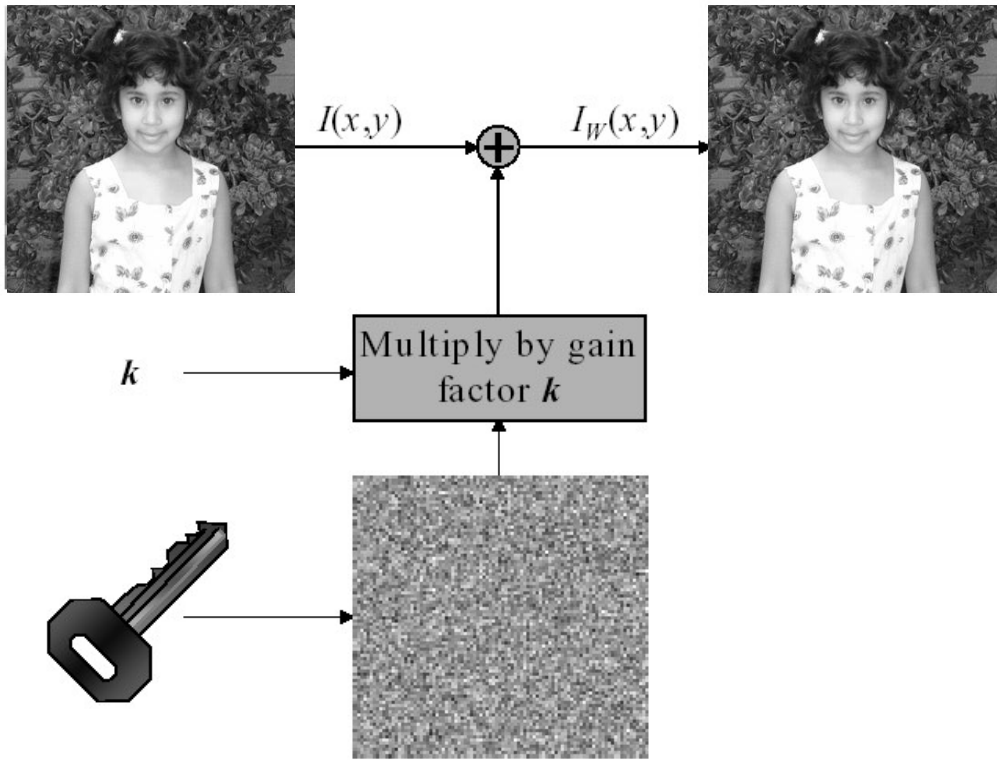
Least Significant Bit Insertion - Modifies the low order bit of pixels. If you see the "regional" distribution of pixels, the low order bit planes are more random than the higher order ones.





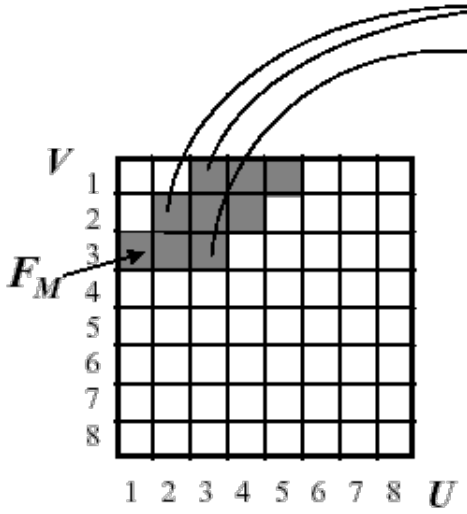
WATER MARKING FOR IMAGES

Correlation in the spatial domain



WATER MARKING FOR IMAGES

DCT Coefficient ordering



8x8 DCT block with possible locations for embedding a bit

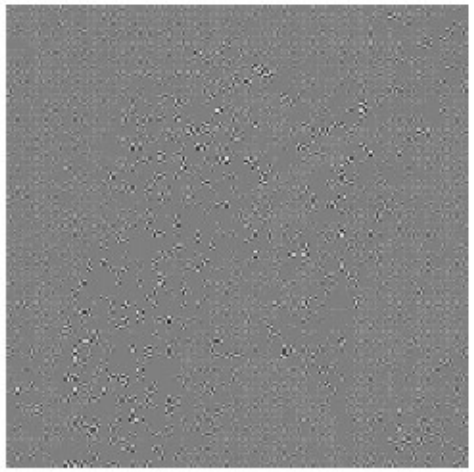
H M H	M H H	L L L	patterns for **1**
M L L	L M L	H H H	patterns for **0**
H L M	L H M	M M M	invalid patterns

Relationships among three quantized DCT coefficients

H: high
M: middle
L: low

WATER MARKING FOR IMAGES





WATER MARKING FOR VIDEO

A video sequence cannot simply be treated as an ordered collection of images:

- **Human perception of motion is not accounted for in visual models for still images**
- **Embed the "same watermark" in all the frames of a video sequence – this is not secure, an attacker can correlate across the entire sequence to estimate the watermark (temporal collusion)**
- **Embed "different watermarks" in successive frames of a video sequence- this is also not secure, as successive video frames are highly correlated**
- **The A/V synchronization may be a consideration for watermark protection.**

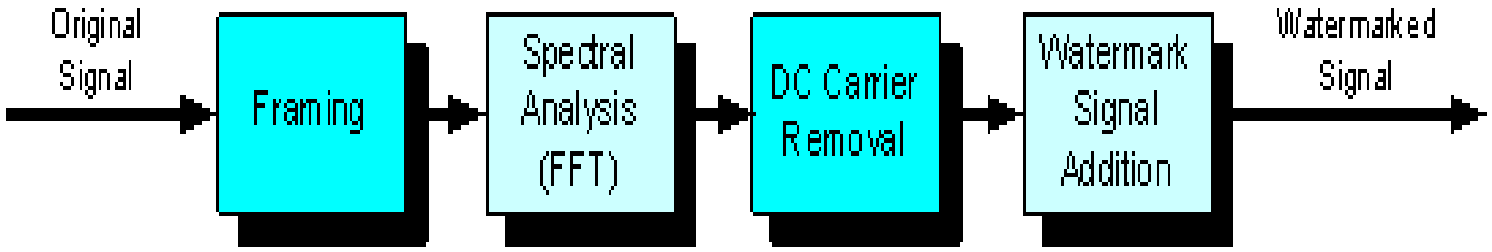
WATER MARKING ATTACKS IN VIDEO

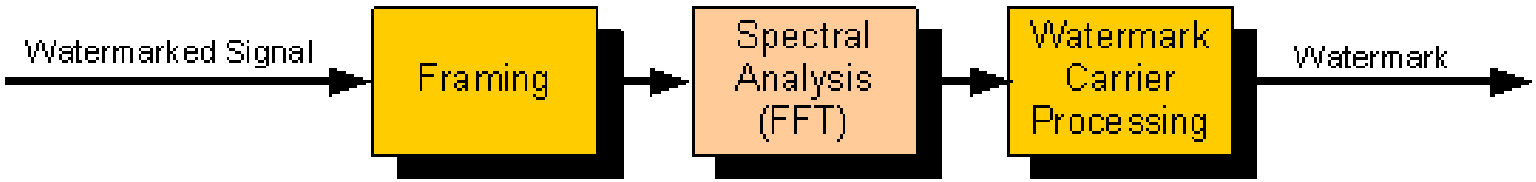
Different categories of video attacks are may be{
***Photometric* - noise addition, DA/AD conversion, gamma correction, transcoding and video format conversion, intra and inter-frames filtering, chrominance resampling (4:4:4, 4:2:2, 4:2:0)**

Spatial desynchronisation – Changes across display formats (4/3, 16/9, 2.11/1), Changes of spatial resolution (NTSC, PAL, SECAM), Positional jitter, Hand held camera attack

Temporal desynchronisation – Changes of frame rate, Video editing Cut-and-splice and cut-insert-splice, Fade-and-dissolve and wipe-and-matte, Graphic overlay (subtitles, logo)

WATER MARKING AUDIO





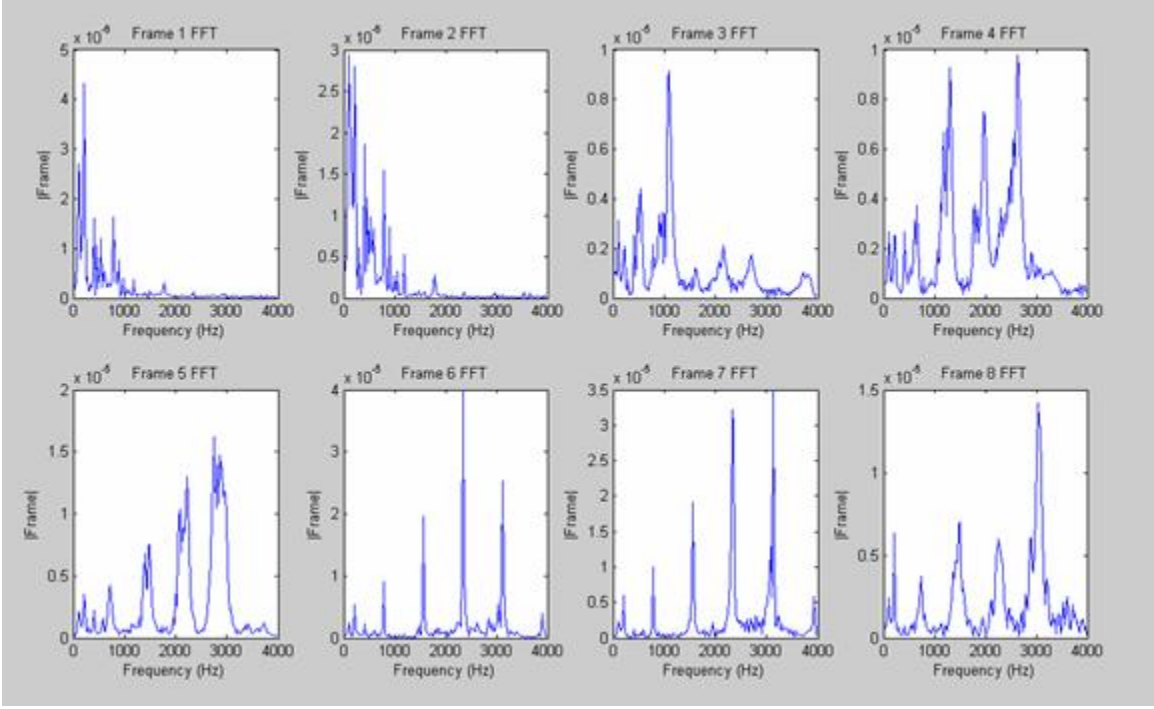
Example of framing : 90ms per frame. If every frame embeds 1 watermark bit, what is the watermark bitrate?

WATER MARKING AUDIO: SPECTRAL ANALYSIS

Example – CD Audio has 16 bits/sample and 44.1KHz. Each frame (at 90ms per frame) has 3969 samples.

An FFT on each window = 3969 Fourier Coefficients.

FFT for the first 8 windows is shown below:



WATER MARKING AUDIO

Low Bit Coding - Most digital audio is created by sampling the signal with a 16-bit quantizer. The rightmost bit, or low order bit, can be toggled without any perceptible change in the audio signal.

Spread Spectrum Coding: The watermarked signal is spread over the entire audible frequency spectrum such that it approximates white noise.

Phase Coding – humans are relatively less sensitive to phase changes. Substitute the initial phase of an audio signal with a reference phase that represents the data.

Echo Data hiding – Discrete copies of the original signal re mixed in with the original signal creating echoes of each sound. By using two different time values between an echo and the original sound, a binary 1 or binary 0 can be encoded.

ENCRYPTION

ENCRYPTION

Encryption is a technique to protect digital data during transmission from sender to a receiver.

- **Data is unreadable during transit; and virtually useless, unless you have a key to decrypt it.**
- **At the receiver, after decryption data is in the clear and no longer protected**

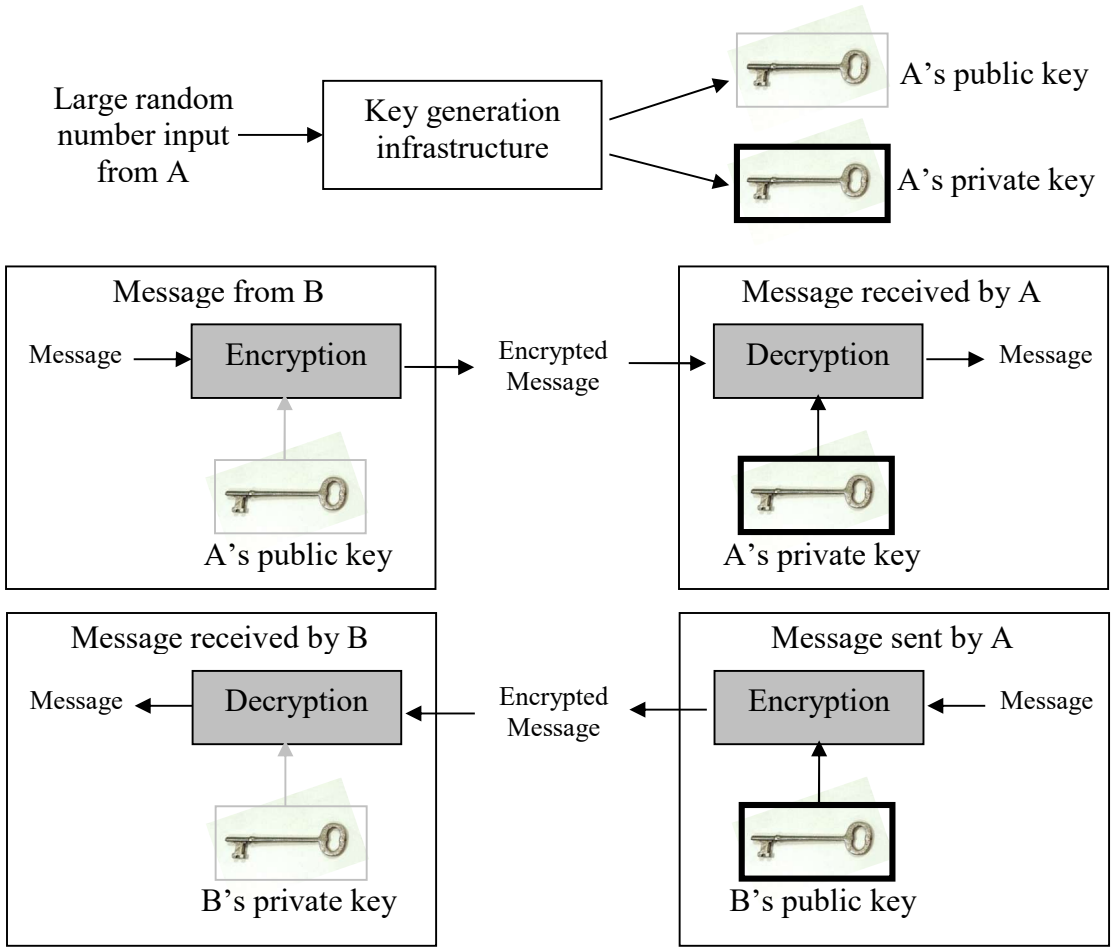
How is this different from Cryptography?

Classical Encryption Techniques have traditionally been known as hard encryption

- **Credit Card**
- **Banking**
- **Email**

Standards include the Data Encryption Scheme (DES) and Advanced Encryption Scheme (AES)

ENCRYPTION USING PKI



MEDIA ENCRYPTION

Media Encryption cannot encrypt the entire stream unlike DES and AES – too expensive and time consuming

- **Huge Data Stream**
- **Real Time needs**
- **Ordered sequence of frames/packets etc**

Media Encryption trading speed for security

Media Encryption is termed as "Soft" or "Selective" Encryption, to differentiate it from classical hard encryption standards

HISTORY OF ENCRYPTION

Existed as long as writing was discovered and used

- **Greeks – writing on narrow strips of parchment around a cylinder.**
- **Writing on the scalp**
- **Numerical ciphers**

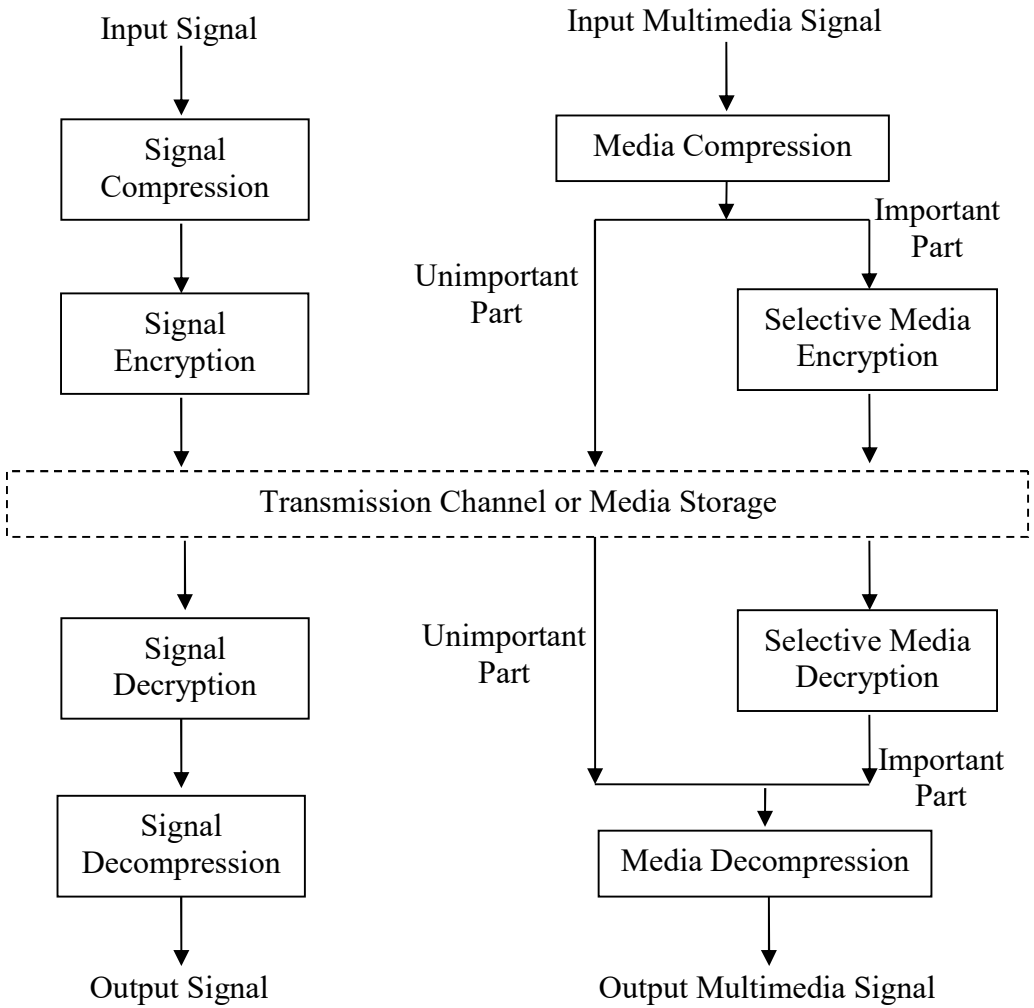
	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

This is a book about multimedia

44 32 42 34 42 34 11 21 43 43
52 11 21 43 54 44 23 54 13 44
42 23 51 41 42 11

- **Mechanical ciphers – Enigma machine**

SELECTIVE ENCRYPTION



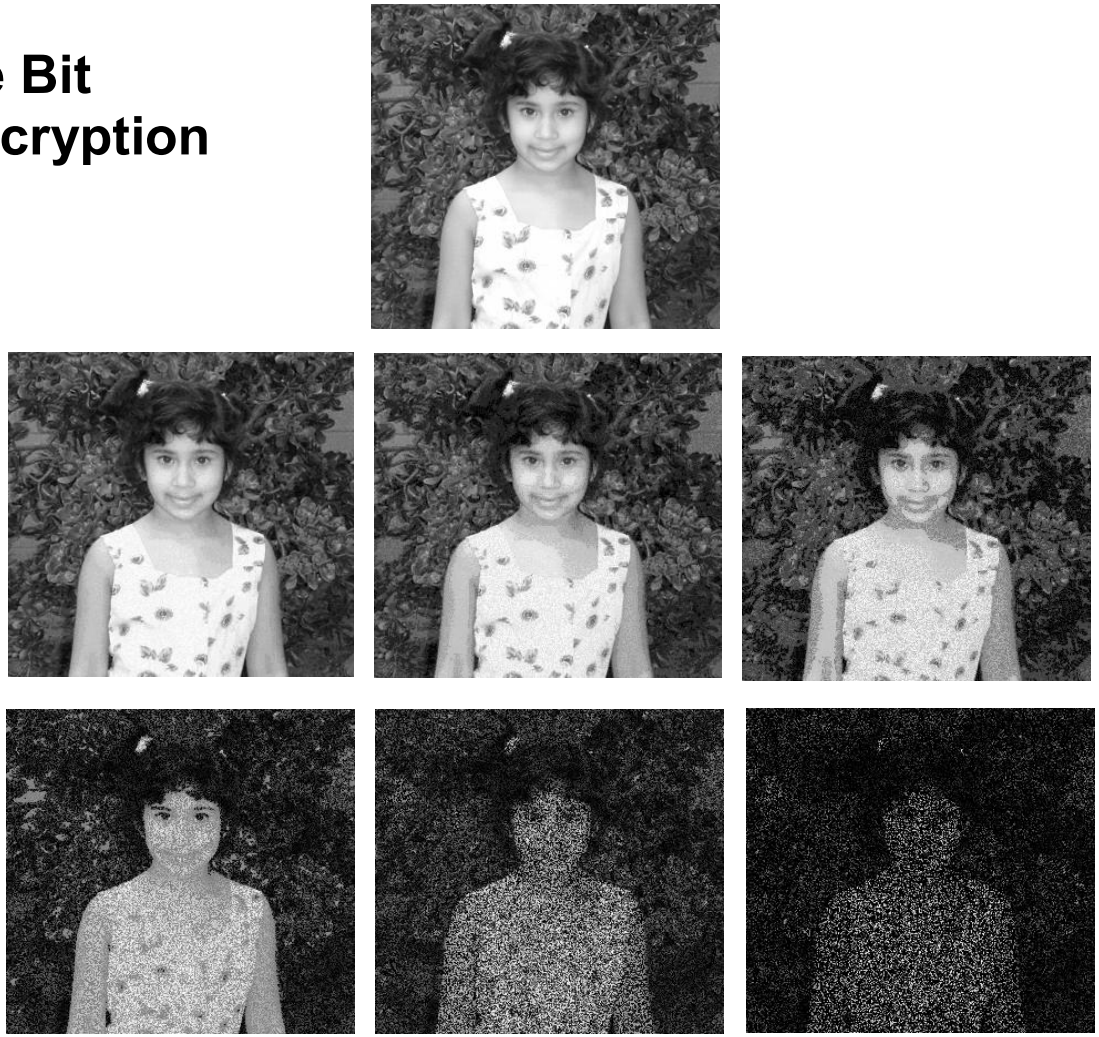
DESIRABLE QUALITIES OF ENCRYPTION

Encrypted Data should have the following qualities

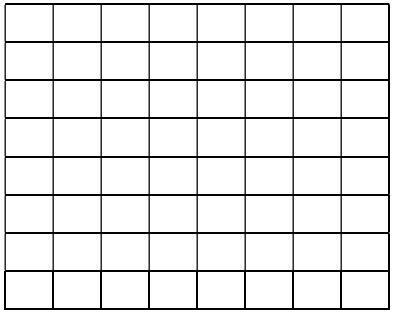
- **Visual acceptance – not necessarily all data should be rendered unintelligible, but should not be completely perceptible.**
- **Selective encryption – not all of the bit stream should be encrypted but able to select areas for encryption, important in media standards!**
- **Time Restrictions – Unlike hard schemes, which are secure and computationally complex, large media streams need to be encrypted in real time**
- **Unchanged bit rate – whether CBR or VBR**
- **Bit stream compliance – encrypted streams still need to received and transmitted using standards based components.**

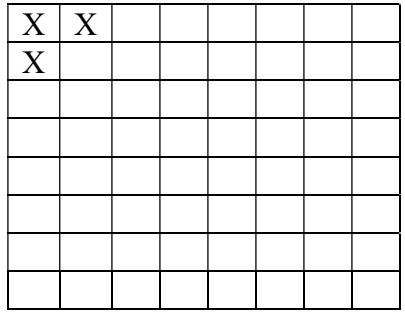
ENCRYPTION IN MEDIA – IMAGES/VIDEO

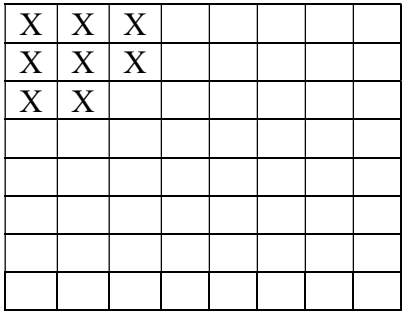
Selective Bit Plane Encryption

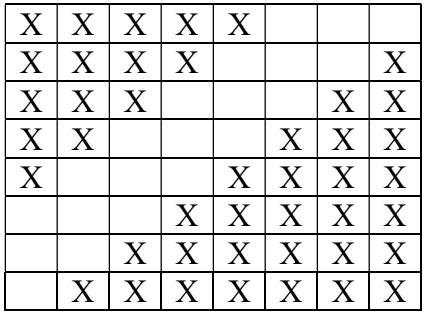


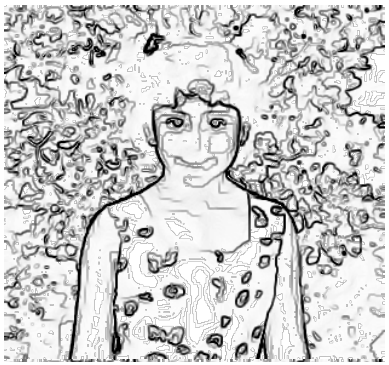
ENCRYPTION IN MEDIA – IMAGES/VIDEO











Encryption in the MPEG domain

DRM SOLUTIONS IN THE INDUSTRY

Music Industry

Motion Picture Industry

Consumer Electronics Industry

Information Technology Industry