University of Technology
الجامعة التكنولوجية

Computer Science Department
قسم علوم الحاسوب

Multimedia Security 2
أمنية الوسائط المتعددة ٢

Lecturer Dr. Muna Ghazi
م.د. منى غازي عبد الصاحب

cs.uotechnology.edu.iq

Principles of Steganography

The "classic" model for invisible communication was first proposed by Simmons as the "prisoners' problem." Alice1 and Bob are arrested for some crime and are thrown in two different cells. They want to develop an escape plan, but unfortunately all communications between each other are arbitrated by a warden named Wendy. She will not let them communicate through encryption and if she notices any suspicious communication, she will place them in solitary confinement and thus suppress the exchange of all messages. So both parties must communicate invisibly in order not to arouse Wendy's suspicion; they have to set up a subliminal channel. A practical way to do so is to hide meaningful information in some harmless message: Bob could, for instance, create a picture of a blue cow lying on a green meadow and send this piece of modern art to Alice. Wendy has no idea that the colors of the objects in the picture transmit information. Unfortunately, there are other problems which may hinder the escape of Alice and Bob. Wendy may alter the message Bob has sent to Alice. For example, she could change the color of Bob's cow to red, and so destroy the information; she then acts as an active warden. Even worse, if she acts in a malicious way, she could forge messages and send a message to one of the prisoners through the subliminal channel while pretending to be the other.

The above model is generally applicable to many situations in which invisible communication—steganography— takes place. Alice and Bob represent two communication parties, wanting to exchange secret information invisibly. The warden Wendy represents an eavesdropper who is able to read and probably alter messages sent between the communication partners (see below Figure). Whereas cryptographic techniques try to conceal the contents

of a message, steganography goes yet a bit further: it tries to hide the fact that a communication even exists. Two people can communicate covertly by exchanging unclassified messages containing confidential information. Both parties have to take the presence of a passive, active or even malicious attacker into account.

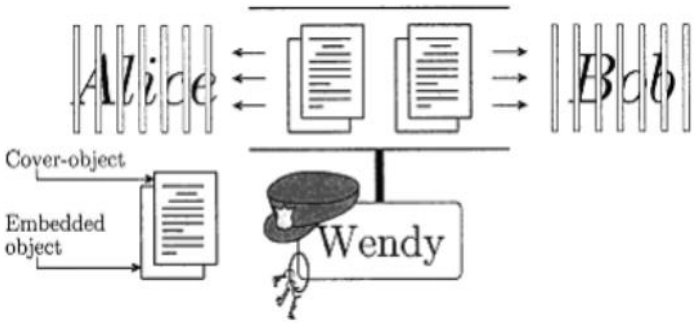


Figure: The prisoners' problem.

Frameworks for Secret Communication

Most applications of steganography follow one general principle, illustrated in Figure. Alice, who wants to share a secret message m with Bob, randomly chooses (using the private random source r) a harmless message **c**, called **cover-object**, which can be transmitted to Bob without raising suspicion, and embeds the secret message into c, probably by using a key **k**, called **stego-key**. Alice therefore changes the cover c to a **stego-object s**. This must be done in a very careful way, so that a third party, knowing only the apparently harmless message s, cannot detect the existence of the secret. In a **"perfect" system, a normal cover should not be distinguishable from a stego-object**, neither by a human nor by a computer looking for statistical pattern. Theoretically, covers could be any computer-readable data such as image files, digital sound, or written text. Alice then transmits s over an insecure channel to Bob and hopes that Wendy will not notice the embedded

message. Bob can reconstruct m since he knows the embedding method used by Alice and has access to the key k used in the embedding process. This extraction process should be possible without the original cover c. A third person watching the communication should not be able to decide whether the sender is active in the sense that he sends covers containing secret messages rather than covers without additional information. More formally, if an observer has access to a set {c1, . . . , cn} of cover-objects transmitted between both communication parties, he should be unable to decide which cover-objects ci contain secret information. Thus, the security of invisible communication lies mainly in the inability to distinguish cover-objects from stego-objects. there are basically three types of steganographic protocols: pure steganography, secret key steganography, and public key steganography.

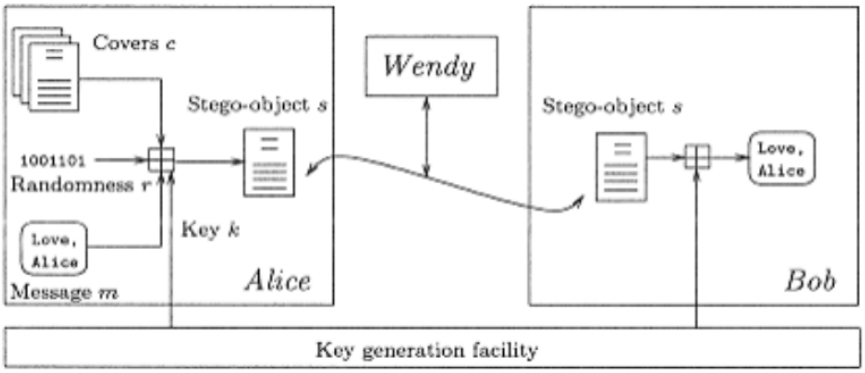


Figure: Schematic description of steganography.

1. Pure Steganography

Pure steganography is steganographic system which does not require the prior exchange of some secret information (like a stego-key). Both sender and receiver must have access to the embedding and extraction algorithm, but the algorithms should not be public.

Definition (Pure steganography) The quadruple = <C, M, D, E>, where C is the set of possible covers, M the set of secret messages with $|C| \geq |M|$, $E : C \times M \rightarrow C$ the embedding function and $D : C \rightarrow M$, the extraction function which extract the secret message out of a cover, with the property that $D(E(c,m)) = m$ for all $m \in M$ and $c \in C$ is called a pure steganographic system.

2. Secret Key Steganography

With pure steganography, no information (apart from the functions E and D) is required to start the communication process; the security of the system thus depends entirely on its secrecy. This is not very secure in practice, so we must assume that Wendy knows the algorithm Alice and Bob use for information transfer. In theory, she is able to extract information out of every cover sent between Alice and Bob. The security of a steganographic system should thus rely on some secret information traded by Alice and Bob, the stego-key. Without knowledge of this key, nobody should be able to extract secret information out of the cover. A secret key steganography system is similar to a symmetric cipher: the sender chooses a cover c and embeds the secret message into c using a secret key k. If the key used in the embedding process is known to the receiver, he can reverse the process and extract the secret message. Anyone who does not know the secret key should not be able to obtain evidence of the encoded information. Again, the cover c and the stego-object can be perceptually similar.

Definition (Secret key steganography) The quintuple = <C, M, K, DK, EK>, where C is the set of possible covers, M the set of secret messages with $|C| \geq |M|$, K the set of secret keys, $EK : C \times M \times K \rightarrow C$ and $DK : C \times K \rightarrow M$ with the property that $DK(EK(c, m, k), k) = m$ for all $m \in M$, $c \in C$ and $k \in K$, is called a secret key steganographic system.

3. Public Key Steganography

As in public key cryptography, public key steganography does not rely on the exchange of a secret key. Public key steganography systems require the use of two keys, one private and one public key; the public key is stored in a public database. Whereas the public key is used in the embedding process, the secret key is used to reconstruct the secret message. One way to build a public key steganography system is the use of a public key cryptosystem. We will assume that Alice and Bob can exchange public keys of some public key cryptography algorithm before imprisonment (this is, however, a more reasonable assumption). Public key steganography utilizes the fact that the decoding function D in a steganography system can be applied to any cover c, whether or not it already contains a secret message (recall that D is a function on the entire set C). In the latter case, a random element of M will be the result, we will call it "natural randomness" of the cover. If one assumes that this natural randomness is statistically indistinguishable from ciphertext produced by some public key cryptosystem, a secure steganography system can be built by embedding ciphertext rather than unencrypted secret messages. In this protocol, Alice first generates a random public/private key pair for use with any public-key cryptosystem. Then she embeds the public key in a channel known to and viewable by Bob (and hence also Wendy). Neither Wendy nor Bob can determine whether the channel contains more than random bits. However, Bob suspects that the stego-object sent by Alice contains Alice's public key and tries to extract it. He uses the received public key to embed a randomly chosen key k along with a short message of acknowledgement, both encrypted with Alice's public key, in a cover and sends it to Alice. Again, Wendy can try to extract the secret information sent by Bob, but will likely notice only random-looking ciphertext. Alice suspects

the arrival of a message from Bob, extracts thesecret information and decrypts it with her private key. Now Alice and Bob share a stego-key k. This protocol is illustrated in the following Figure. However, the protocol is (at the first step) susceptible to a man-in-the-middle attack. If Wendy is active, she can catch the first stego-object sent from Alice to Bob and replace Alice's public key with her own. Bob will encrypt the random secret key k using Wendy's public key instead of Alice's. Now Wendy knows the key k chosen by Bob and can forward it to Alice: she encrypts it with Alice's public key, embeds it in a cover and sends the result to Alice. Although Alice correctly receives k, she is not aware of the fact that Wendy also has access to k.

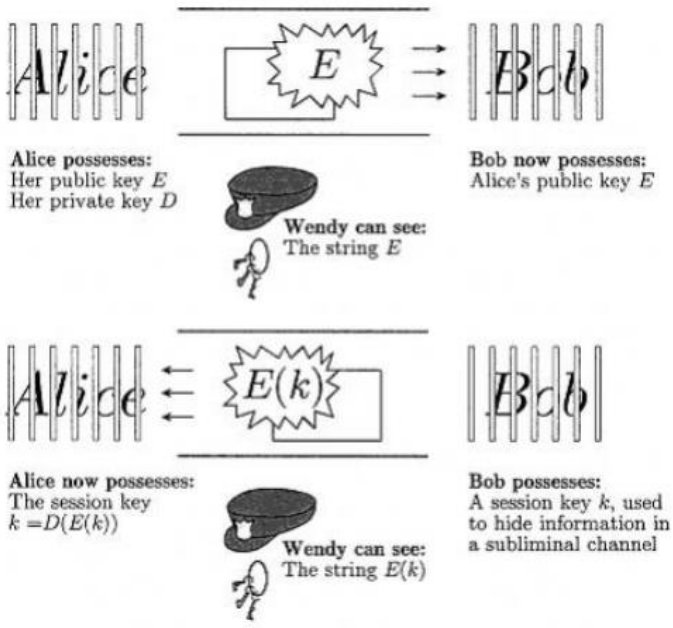


Figure: steganographic key-exchange protocol.

Security of Steganography Systems

Although breaking a steganography system normally consists of three parts: detecting, extracting, and disabling embedded information, a system is already insecure if an attacker is able to prove the existence of a secret message. In developing a formal security model for steganography, we must assume that an attacker has unlimited computation power and is able and willing to perform a variety of attacks. If he cannot confirm his hypothesis that a secret message is embedded in a cover, then a system is theoretically secure.

1. Perfect Security

The main idea the security of steganographic systems is to refer to the selection of a cover as a random variable C with probability distribution. The embedding of a secret message can be seen as a function defined in C; let PS be the probability distribution of EK (c, m, k), that is the set of all stego-objects produced by the steganographic system.

2. Detecting Secret Messages

A passive attacker (Wendy) has to decide whether a cover c sent from Bob to Alice contains secret information or not. This task can be formalized as a statistical hypothesis-testing problem. Therefore, Wendy defines a test function $f : C \rightarrow \{0, 1\}$:

$$f(c) = \begin{cases} 1 & c \text{ contains a secret message} \\ 0 & \text{otherwise} \end{cases}$$

which Wendy uses to classify covers as they are passed on via the insecure channel. In some cases, Wendy will correctly classify the cover, in other cases she will not detect a hidden message, making a type-II error. It is also possible

that Wendy falsely detects a hidden message in a cover which does not contain information; she then makes a type-I error. Practical steganography systems try to maximize the probability β that a passive attacker makes a type-II error.

Active and Malicious Attackers

During the design of a steganographic system special attention has to be paid to the presence of active and malicious attackers. Active attackers are able to change a cover during the communication process; Wendy could capture one stego-object sent from Alice to Bob, modify it and forward the result to Bob. It is a general assumption that an active attacker is not able to change the cover and its semantics entirely, but only make minor changes so that the original and the modified cover-object stay perceptually or semantically similar. An attacker is malicious if he forges messages or starts steganography protocols under the name of one communication partner.

1. Active Attackers: Robust Steganography

Steganographic systems are extremely sensitive to cover modifications, such as image processing techniques (like smoothing, filtering, and image transformations) in the case of digital images and filtering in the case of digital sound. But even a lossy compression can result in total information loss. Lossy compression techniques try to reduce the amount of information by removing imperceptible signal components and so often remove the secret information which has previously been added. An active attacker, who is not able to extract or prove the existence of a secret message, thus can simply add random noise to the transmitted cover and so try to destroy the information. In the case of digital images, an attacker could also apply image processing

techniques or convert the image to another file format. All of these techniques can be harmful to the secret communication. Another practical requirement for a steganography system therefore is robustness. A system is called robust if the embedded information cannot be altered without making drastic changes to the stego-object.

It should be clear that there is a trade-off between security and robustness. The more robust a system will be against modifications of the cover, the less secure it can be, since robustness can only be achieved by redundant information encoding which will degrade the cover heavily and possibly alter the probability distribution PS.

2. Malicious Attackers: Secure Steganography,

In the presence of a malicious attacker, robustness is not enough. If the embedding method is not dependent on some secret information shared by sender and receiver, (i.e., in the case of pure steganography or public key steganography) an attacker can forge messages, since the recipient is not able to verify the correctness of the sender's identity. Thus, to avoid such an attack, the algorithm must be robust and secure. We can define a secure steganographic algorithm in terms of four requirements:

• Messages are hidden using a public algorithm and a secret key; the secret key must identify the sender uniquely;

• Only a holder of the correct key can detect, extract, and prove the existence of the hidden message. Nobody else should be able to find any statistical evidence of a message's existence;

• Even if the enemy knows (or is able to select) the contents of one hidden message, he should have no chance of detecting others;

• It is computationally infeasible to detect hidden messages.

Techniques of Steganography

Steganographic Techniques

Many different steganographic methods have been proposed during the last few years; most of them can be seen as substitution systems. Such methods try to substitute redundant parts of a signal with a secret message; their main disadvantage is the relative weakness against cover modifications. Recently, the development of new robust watermarking techniques led to advances in the construction of robust and secure steganography systems. The Steganography have the following Techniques:

- Substitution systems substitute redundant parts of a cover with a secret message;
- Transform domain techniques embed secret information in a transform space of the signal (e.g., in the frequency domain).
- Spread spectrum techniques adopt ideas from spread spectrum Communication.
- Statistical methods encode information by changing several statistical properties of a cover and use hypothesis testing in the extraction process.
- Distortion techniques store information by signal distortion and measure the deviation from the original cover in the decoding step.
- Cover generation methods encode information in the way a cover for secret communication is created.

A. Substitution Systems

A number of methods exist for hiding information in various media. These methods range from LSB coding also known as bitplane or noise insertion tools manipulation of image. Basic substitution systems try to encode secret information by substituting insignificant parts of the cover by secret message bits; the receiver can extract the information if he has knowledge of the positions where secret information has been embedded. Since only minor modifications are made in the embedding process, the sender assumes that they will not be noticed by a passive attacker.

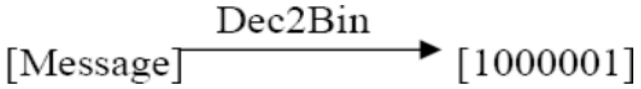
1. Least Significant Bit Substitution

Bitplane tools encompass methods that apply LSB insertion and noise manipulation. These approaches are common in steganography and are relatively easy to apply in image and audio. The image formats typically used in such steganography methods are lossless and the data can be directly manipulated and recovered. Some of these programs apply compression and encryption in addition to steganography services. These services provide better security of the hidden data. The embedding process consists of choosing a subset {j1, . . , jl(m)} of cover-elements and performing the substitution operation cji = mi on them, which exchanges the LSB of cji by mi (mi can either be 1 or 0). One could also imagine a substitution operation which changes more than one bit of the cover, for instance by storing two message bits in the two least significant bits of one cover-element. In the extraction process, the LSB of the selected cover-elements are extracted and lined up to reconstruct the secret message. Applying LSB technique to each byte of a 24-bit image, three bits can be encoded into each pixel. Applying LSB technique

to each byte of an 8-bit image, only one bit can be encoded into each pixel, as each pixel is represented by onebyte.

Example: The following steps illustrate how this method is used to hide the secret data "A" in cover image "Mansoura.bmp".

Step1: Convert the data from decimal to binary. Where the ASCII of A is 65.



Step2: Read Cover Image "Mansoura.bmp" as shown in the following Figure.

144	142	146	152	156	147	151	157
160	155	159	162	133	123	133	145
144	141	141	138	61	55	65	79
120	123	131	144	50	61	74	92
170	167	167	166	61	59	56	59
120	125	131	132	61	59	59	59
124	133	139	131	88	76	77	76
138	153	167	154	139	.....	.....	.....

Figure: The cover image “Mansoura.bmp".

Step3: Convert the Cover Image from decimal to binary.

10010000	10011010	10011100	10010010	10010110	10011101	10101111	10100101
10100000	10011011	10011111	10100010	10000101	01111011	10000101	10010001
10010000	10001101	10001101	10001010	00111101	00110111	01000001	01001111
01111000	01111011	10000011	10010000	00110010	00111101	01001010	01011100
10101010	10100111	10100111	10100110	00111101	00111011	00111000	00111011
01111000	01111101	10000011	10000100	00111101	00111011	00111011	00111011
01111100	10000101	10000111	10000011	01011000	01001100	01001101	01001100
10001010	10011001	10100111	10011010	10001011	.....	.....	.....

Step4: Break the byte to be hidden into bits.

Thus [01000001] -> is divided into 8 bites [0 1 0 0 0 0 0 1].

Step5: Take first 8 byte of original data from the Cover Image.

10010000	10011010	10011100	10010010	10010110	10011101	10101111	10100101

Step6: Replace the least significant bit by one bit of the data to be hidden as follows,

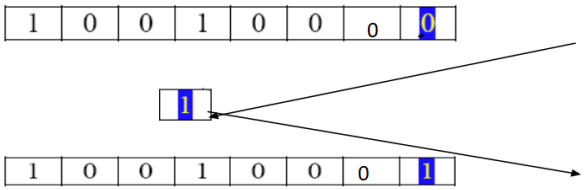
- First byte of original data from the Cover Image.

1	0	0	1	0	0	0	0

- First bit of the data to be hidden.

1

- Replace the least significant bit.



- Repeat the replace for all bytes of Cover Image.
- Finally, the cover image before and after steganography is shown in following figure,

Figure: (a) Cover Image before steganography. (b) Cover Image after steganography.

Choosing to modify values that have a small effect on the cover medium limits the ability to detect the embedding. Embedding strategies may be easily derived and implemented to complicate detection and inhibit the retrieval of the message by a third party, while still allowing easy retrieval by the intended recipient.

2. Image Downgrading and Covert Channels

Image downgrading is a special case of a substitution system in which images act both as secret messages and covers. Given a cover-image and a secret image of equal dimensions, the sender exchanges the four least significant bits of the cover's grayscale (or color) values with the four most significant bits of the secret image. The receiver extracts the four least significant bits out of the stego-image, thereby gaining access to the most significant bits of the secret image. While the degradation of the cover is not visually noticeable in many cases, 4 bits are sufficient to transmit a rough approximation of the secret image.

B. Transform Domain Techniques

We have seen that LSB modification techniques are easy ways to embed information, but they are highly vulnerable to even small cover modifications. An attacker can simply apply signal processing techniques in order to destroy the secret information entirely. In many cases even the small changes resulting out of lossy compression systems yield to total information loss. It has been noted early in the development of steganographic systems that embedding information in the frequency domain of a signal can be much more robust than embedding rules operating in the time domain. Most robust

steganographic systems known today actually operate in some sort of transform domain. Transform domain methods hide messages in significant areas of the cover image which makes them more robust to attacks, such as compression, cropping, and some image processing, than the LSB approach. However, while they are more robust to various kinds of signal processing, they remain imperceptible to the human sensory system. Many transform domain variations exist. A transform maps image data into a different mathematical space via a transformation equation. When mapping image data from the time domain (also called the spatial domain) to the frequency domain (also called the spectral domain), where all the pixels in the input (time domain) contribute to each value in the output (frequency domain). One method is to use the Discrete Cosine Transformation (DCT).

1. The 2-D **Discrete Cosine Transform (DCT)** equation for an N x N image is given by:

$$C(u,v) = \alpha(u)\alpha(v)\sum_{r=0}^{N-1}\sum_{c=0}^{N-1} I(r,c)\cos\left[\frac{(2r+1)u\pi}{2N}\right]\cos\left[\frac{(2c+1)v\pi}{2N}\right]$$

Where:

$$\alpha(u),\alpha(v) = \begin{cases} \sqrt{\frac{1}{N}} & for\ u,v = 0 \\ \sqrt{\frac{2}{N}} & for\ u,v = 1,2,\dots\dots,N-1 \end{cases}$$

While the equation of **inverse discrete cosine transform** is given by:

$$C^{-1}[C(u,v)] = I(r,c) = \sum_{u=0}^{N-1}\sum_{v=0}^{N-1} \alpha(u)\alpha(v)C(u,v)\cos\left[\frac{(2r+1)u\pi}{2N}\right]\cos\left[\frac{(2c+1)v\pi}{2N}\right]$$

2. **Hiding Information in Digital Sound: Phase Coding**

   Embedding secret messages in digital sound is generally more difficult than embedding information in digital images. Moore noted that the human auditory system is extremely sensitive; perturbations in a sound file can be detected as low as one part in 10 million. Although the limit of perceptible noise increases as the noise level of the cover increases, the maximum allowable noise level is generally quite low.

C. Spread Spectrum and Information Hiding

Spread spectrum techniques as "means of transmission in which the signal occupies a bandwidth in excess of the minimum necessary to send the information; the band spread is accomplished by means of a code which is independent of the data, and a synchronized reception with the code at the receiver is used for despreading and subsequent data recovery." This situation is very similar to a steganography system which tries to spread a secret message over a cover in order to make it impossible to perceive. Since spreaded signals tend to be difficult to remove, embedding methods based on SS should provide a considerable level of robustness.

D. Statistical Steganography

Statistical steganography techniques utilize the existence of "1-bit" steganographic schemes, which embed one bit of information in a digital carrier. This is done by modifying the cover in such a way that some statistical characteristics change significantly if a "1" is transmitted. Otherwise, the cover is left unchanged. So, the receiver must be able to distinguish unmodified covers from modified ones. In order to construct a l(m)-bit stego-

system from multiple "1-bit" stegosystems, a cover is divided into l(m) disjoint blocks B1, . . . , Bl(m). The detection of a specific bit is done via a test function which distinguishes modified blocks from unmodified blocks.

E. Distortion Techniques

In contrast to substitution systems, distortion techniques require the knowledge of the original cover in the decoding process. Alice applies a sequence of modifications to a cover in order to get a stego-object; she chooses this sequence of modifications in such a way that it corresponds to a specific secret message she wants to transmit. Bob measures the differences to the original cover in order to reconstruct the sequence of modifications applied by Alice, which corresponds to the secret message.

F. Cover Generation Techniques

In contrast to all embedding methods presented above, where secret information is added to a specific cover by applying an embedding algorithm, some steganographic applications generate a digital object only for the purpose of being a cover for secret communication.

1. Mimic Functions.
2. Automated Generation of English Texts.

Steganalysis

Introduction and Terminology

A goal of steganography is to avoid drawing suspicion to the transmission of a hidden message, so it remains undetected. If suspicion is raised, then this goal is defeated. Steganalysis is the art of discovering and rendering such messages useless. Attacks and analysis on hidden information may take several forms: detecting, extracting, confusing (counterfeiting or overwriting by an attacker, embedding counter information over the existing hidden information), and disabling hidden information. Our objective here is not to advocate the removal or disabling of valid hidden information such as copyrights, but to point out approaches that are vulnerable and may be exploited to investigate illicit hidden information. Any cover can be manipulated with the intent of disabling or destroying some hidden information whether an embedded message exists or not. Detecting the existence of a hidden message will save time in the disabling phase by processing only those covers that contain hidden information. Before going further, we should take a look at new terminology with respect to attacks and breaking steganography schemes. These are similar to cryptographic terminology; however, there are some significant differences. Just as a cryptanalyst applies cryptanalysis in an attempt to decipher encrypted messages, the **steganalyst** is one who applies **steganalysis** in an attempt to detect the existence of hidden information. In cryptanalysis, portions of the plaintext (possibly none) and portions of the ciphertext are analyzed. In steganalysis, comparisons are made between the **cover-object, the stego-object**, and possible portions of the message. The end result in cryptography

is the ciphertext, while the end result in steganography is the **stego -object**. The hidden message in steganography may or may not be encrypted. If it is encrypted, then if the message is extracted, cryptanalysis techniques may be applied to further understand the embedded message.

Somewhat parallel attacks are available to the steganalyst:

• **Stego-only attack.** Only the stego-object is available for analysis.

• **Known cover attack.** The "original" cover-object and stego-object are both available.

• **Known message attack.** At some point, the hidden message may become known to the attacker. Analyzing the stego-object for patterns that correspond to the hidden message may be beneficial for future attacks against that system. Even with the message, this may be very difficult and may even be considered equivalent to the stego-only attack.

• **Chosen stego attack.** The steganography tool (algorithm) and stego-object are known.

• **Chosen message attack.** The steganalyst generates a stego-object from some steganography tool or algorithm from a chosen message.

• **Known stego attack.** The steganography algorithm (tool) is known and both the original and stegoobjects are available.

A Chaotic Encryption Scheme

In our daily lives, one may say "that was complete chaos" to describe a situation of extreme disorder, irregularity, or confusion.

chaos is a phenomenon that has deterministic underlying rules behind irregular appearances.

Chaos theory plays an active role in modern cryptography. As the basis for developing a crypto-system, the advantage of using chaos lies in its random behavior and sensitivity to initial conditions and parameter settings to fulfill the classic Shannon requirements of confusion and diffusion. To meet a great demand for real-time secure image transmission over the Internet, a variety of encryption schemes have been proposed. One of them, chaos-based algorithms have shown some exceptionally good properties in many concerned aspects regarding security, complexity, etc. Chaotic systems are characterized by sensitive dependence on initial conditions, similarity to random behavior. A tiny difference in the starting state and parameter setting of these systems can lead to enormous differences in the final state of the system over a few iterations. Thus, sensitivity to initial conditions manifests itself as an exponential growth of error and the behavior of system appears chaotic. Several schemes have been developed which allow transforming the information signal into a chaotic waveform on the transmitter side and to extract the information signal from the transmitted waveform on the receiver side. The most important among them are: chaotic masking, chaos shift keying, and chaotic modulation.

However, there are some limitations of block ciphers proposed using chaotic maps. Firstly, the distribution of the ciphertext is *not flat* enough to ensure high security since the occurrence probability of cipher blocks decays

exponentially as the number of iterations increases. Secondly, the *encryption speed of these cryptographic schemes is very slow* since at least 250 iterations of the chaotic map are required for encrypting an 8-bit symbol. The number may vary upto 65532. Thirdly, *the length of ciphertext is at least twice that of plaintext*, a byte of message may result in several tens of thousands of iterations that need two bytes to carry.

Several chaotic stream ciphers have been known to be insecure and known plaintext attacks have been proposed. Besides, cryptographic security some of the factors influencing the design of a good chaotic stream cipher for real time applications are encryption speed and hardware implementation. Some digital chaotic ciphers are too slow to be feasible for real-time encryption. While the chaotic systems are running in finite precision, the fixed-point arithmetic is preferable over floating point mathematics which require more hardware resources and computation time.

Typical features of chaos:

commonly-accepted features of chaos include:

1. **Deterministic**. It has deterministic rather than probabilistic underlying rules which every future state of the system must follow.
2. **Nonlinear**. The underlying rules are nonlinear; if they are linear, it cannot be chaos.
3. **Irregular**. The behavior of the system shows sustained irregularity.
4. **Sensitive to initial conditions**. Small changes in the initial state of chaotic systems can lead to radically different behavior in the final state.
5. **Long term prediction** is practically impossible in most cases due to sustained irregularity and sensitivity to initial conditions, which can only be known to a finite precision.

Secure Wavelet Transform

The recent emergence of embedded multimedia applications, such as mobile-TV, surveillance, video messaging, and telemedicine have increased the scope of multimedia in our personal lives. These applications increase the concerns regarding privacy and security of the targeted subjects. Another growing concern is the protection and enforcement of intellectual property rights for images and videos. These and other issues such as image authentication, rights validation, identification of illegal copies of a (possibly forged) image are grouped and studied under the label of digital rights management (DRM). The computer security protocols (e.g., SSL, TLS) and cryptographic ciphers, e.g., AES, DES, drive much of the world's electronic communications, commerce, and storage. These techniques have been used for conventional multimedia encryption and authentication. This naive approach is usually suitable for text, and sometimes for small bit rate audio, image, and video files that are being sent over a fast dedicated channel. The naive approach enables the same level of security as that of the used conventional cryptographic cipher. Depending on the scheme used, the encryption operation is performed either at some intermediate level during compression or after the final compression. However, these cryptographic ciphers require a large amount of computational resources. To reduce the computational requirements of full encryption schemes. A scheme presents for encryption of Discrete Cosine Transform (DCT) coefficients' signs and watermarking of DCT coefficients.

One method of multimedia encryption scheme based on parameterized construction of the DWT and sub band reorientation for the wavelet decomposition, called the secure wavelet transform (SWT). A single stage of

image decomposition can be implemented by successive horizontal row and vertical column wavelet transforms. Thus, one level of DWT operation is represented by filtering with high and low pass filters across row and column, respectively. After each filtering stage, down sampling is done by a factor of two to remove the redundant information. Applying a 2D DWT to an image of resolution M X N results in four images of dimensions M\2 X N\2 Subsequent levels of DWT-based decomposition yield a multi-resolution structure suitable for image compression. The simplest form of wavelets, the Haar wavelet function.

There are four filters that comprise the two-channel bi-orthogonal wavelet system. The analysis and synthesis low-pass filters are denoted by H1 and H2, respectively. The analysis and synthesis high pass filters are denoted by G1 and G2, respectively. depicts a two stage discrete wavelet transform, where x is first passed through low-pass and high-pass filters, and then the resulting signals are down-sampled by a factor of two. a one stage discrete wavelet transform decomposes (analysis) a signal into low frequency (approximation) and high frequency (detail) bands. The reconstruction operation inverse wavelet transform (synthesis) it is evaluated by up-sampling (interpolating) the approximate coefficients.

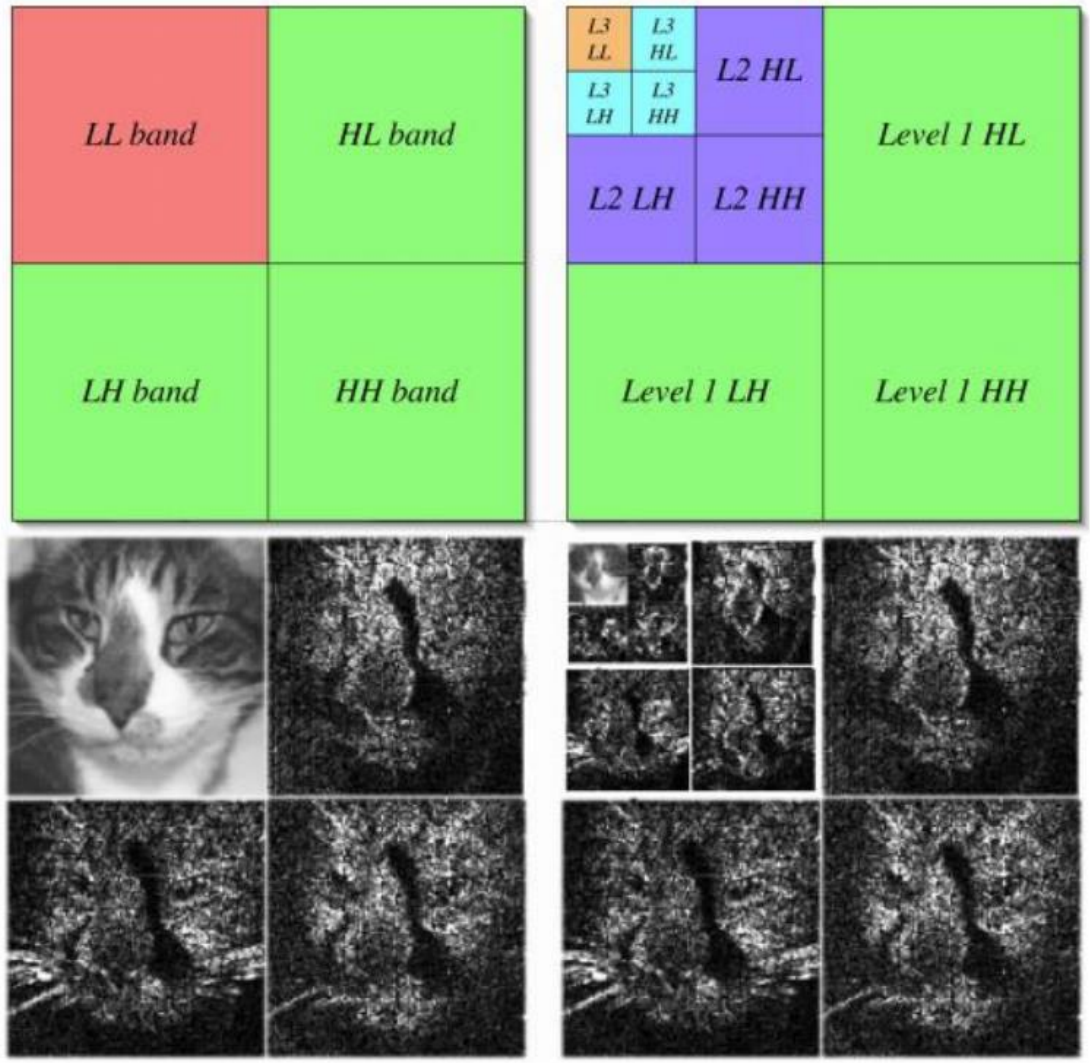


Figure: Two-dimensional wavelet transform: (left) one-level 2D DWT of sample image, and (right) three level 2D DWT of the same image. Note that the LH bands tend to isolate horizontal features, while the HL band tend to isolate vertical features in the image.

Example: *Given the following 3x3 sub image, Find it's Haar wavelet coefficients for two passes:*

7	8	6	7
6	5	8	5
4	3	7	8
8	4	6	4

Solution:

$$L_i = \frac{X_{2i} + X_{2i+1}}{2}, \qquad H_i = \frac{X_{2i} - X_{2i+1}}{2}$$

Pass1:

a. **Row process:**

$\frac{7+8}{2}$	$\frac{6+7}{2}$	$\frac{7-8}{2}$	$\frac{6-7}{2}$
$\frac{6+5}{2}$	$\frac{8+5}{2}$	$\frac{6-5}{2}$	$\frac{8-5}{2}$
$\frac{4+3}{2}$	$\frac{7+8}{2}$	$\frac{4-3}{2}$	$\frac{7-8}{2}$
$\frac{8+4}{2}$	$\frac{6+4}{2}$	$\frac{8-4}{2}$	$\frac{6-4}{2}$

=

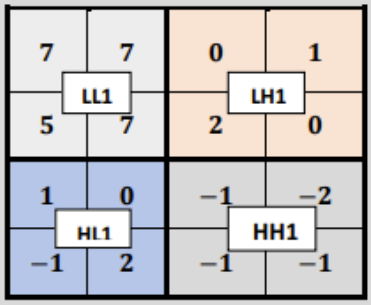
8	7	−1	−1
6	7	1	2
4	8	1	−1
6	5	2	1

L1 H1

b. Column process:

$\frac{8+6}{2}$	$\frac{7+7}{2}$	$\frac{-1+1}{2}$	$\frac{-1+2}{2}$
$\frac{4+6}{2}$	$\frac{8+5}{2}$	$\frac{1+2}{2}$	$\frac{-1+1}{2}$
$\frac{8-6}{2}$	$\frac{7-7}{2}$	$\frac{-1-1}{2}$	$\frac{-1-2}{2}$
$\frac{4-6}{2}$	$\frac{8-5}{2}$	$\frac{1-2}{2}$	$\frac{-1-1}{2}$

=

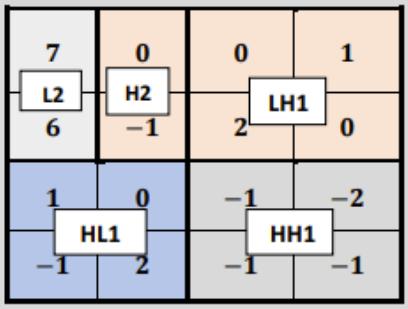


Pass2:

a. Row process:

$\frac{7+7}{2}$	$\frac{7-7}{2}$	0	1
$\frac{5+7}{2}$	$\frac{5-7}{2}$	2	0
1	0	−1	−2
−1	2	−1	−1

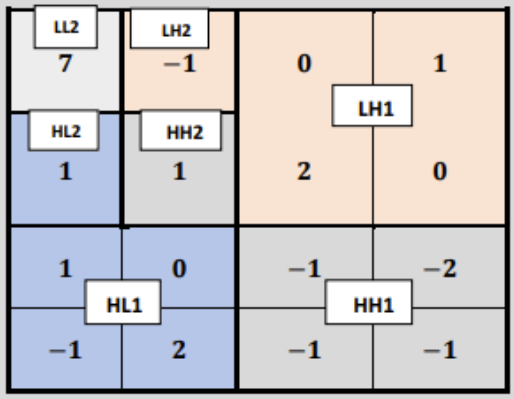
=



b. Column process:

$\frac{7+6}{2}$	$\frac{0-1}{2}$	0	1
$\frac{7-6}{2}$	$\frac{0+1}{2}$	2	0
1	0	−1	−2
−1	2	−1	−1

=



Watermarking

Watermarking, as opposed to steganography, Digital watermarking is the method of embedding data into digital multimedia content (the watermark) into an image or video (visible or invisible). This is used to verify the content or to recognize the identity of the digital content's owner. Visible watermarks, as the name says, are visual patterns like logos which are inserted into or overlaid on images (or video), very similar to visible paper watermarks. Even if the existence of the hidden information is known it should be hard for an attacker to destroy the embedded watermark without knowledge of a key. Watermarks have been proposed for Copyright Protection of digital images, audio and video and, extensively, multimedia products. Watermarks are digital signals that are embedded into other digital signals. A watermark should represent exclusively the copyright owner of the product and can be detected only by him/her. Watermarks must be robust to any product modification that does not degrade its quality.

Basic Watermarking Principles

All watermarking methods share the same generic building blocks: a watermark embedding system and a watermark recovery system. The below Figure shows the generic watermark embedding process.

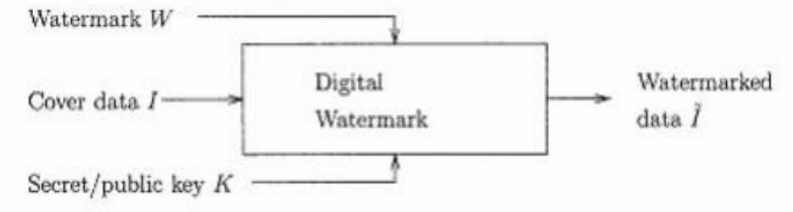


Figure: Generic digital watermarking scheme.

The input to the scheme is the watermark, the cover-data and an optional public or secret key. The watermark can be of any nature such as a number, text, or an image. The key may be used to enforce security, that is the prevention of unauthorized parties from recovering and manipulating the watermark. All practical systems employ at least one key, or even a combination of several keys. In combination with a secret or a public key the watermarking techniques are usually referred to as secret and public watermarking techniques, respectively. The output of the watermarking scheme is the watermarked data. For real-world robust watermarking systems, a few very general properties, shared by all proposed systems, can be identified. They are:

• **Imperceptibility.** The modifications caused by watermark embedding should be below the perceptible threshold, which means that some sort of perceptibility criterion should be used not only to design the watermark, but also quantify the distortion. As a consequence of the required imperceptibility, the individual samples (or pixels, features, etc.) that are used for watermark embedding are only modified by a small amount.

• **Redundancy.** To ensure robustness despite the small allowed changes, the watermark information is usually redundantly distributed over many samples (or pixels, features, etc.) of the cover data, thus providing a global robustness which means that the watermark can usually be recovered from a small fraction of the watermarked data. Obviously watermark recovery is more robust if more of the watermarked data is available in the recovery process.

• **Keys.** In general, watermarking systems use one or more cryptographically secure keys to ensure security against manipulation and erasure of the watermark. As soon as a watermark can be read by someone, the same person may easily destroy it because not only the embedding strategy, but also the

locations of the watermark are known in this case. These principles apply to watermarking schemes for all kinds of data that can be watermarked, like audio, images, video, formatted text, 3D models, model animation parameters, and others.

Types of Digital Watermark

Digital watermarking may be classified in several categories.

A. Division based on human perception: Digital watermarking can be classified as **visible** and **invisible**.

1. Visible watermarks: The visible watermarks are viewable to the normal eye such as company logos and television channel logos etc. This type of watermarks is easily viewable without any mathematical calculation but these embedded watermarks can be destroyed easily.

2. Invisible watermarks: The locations in which the watermark is embedded are secret, only the authorized persons extract the watermark. Some mathematical calculations are required to retrieve the watermark. This kind of watermarks is not viewable by an ordinary eye. Invisible watermarks are more secure and robust than visible watermarks.

B. Division based on applications: Based on application watermarks are divided into **fragile**, **semi-fragile** and **robust watermarks**.

1. Fragile watermarks: These watermarks are very sensitive. They can be destroyed easily with slight modifications in the watermarked signal.

2. Robust watermarks: These watermarks cannot be broken easily. Robust watermark should remain intact permanently in the embedded signal such that attempts to remove or destroy the robust watermark will degrade or even may destroy the quality of the image. This method can be used to ensure copyright protection of the signal.

C. Division Based on User's Authorization to Detect the Watermark: This is divided into **private**, **Semiprivate** and **Public watermarks**.

1. Private watermarking (also called non blind watermarking) systems require at least the original media object and the watermark for the extraction. That means that only the distributor will be able to extract the embedded watermark.

2. Semiprivate watermarking (or semi blind watermarking) is similar to private watermarking but for this case the original media object is not needed, only the watermark. This can be used by systems that automatically check the watermark.

3. Public watermarking (also referred to as blind or oblivious watermarking) neither the original nor the watermark is needed to be able to extract the watermark.

Watermarking Applications

Although watermarking methods have to be robust in general, different levels of required robustness can be identified depending on the specific application-driven requirements.

1.Watermarking for Copyright Protection

Copyright protection is probably the most common application of watermarking today. The objective is to embed information about the source, and thus typically the copyright owner, of the data in order to prevent other parties from claiming the copyright on the data. Thus, the watermarks are used to resolve rightful ownership, and this application requires a very high level of robustness. The driving force for this application is the Web which contains millions of freely available images that the rightful owners want to protect.

2. Fingerprinting for Traitor Tracking

There are other applications where the objective is to convey information about the legal recipient rather than the source of digital data, mainly in order to identify single distributed copies of the data. This is useful to monitor or trace back illegally produced copies of the data that may circulate. This type of application is usually called "fingerprinting". Watermarks for fingerprinting applications also require a high robustness.

3. Watermarking for Copy Protection

A desirable feature in multimedia distribution systems is the existence of a copy protection mechanism that disallows unauthorized copying of the media. An example is the DVD system where the data contains copy information embedded as a watermark. A compliant DVD player is not allowed to playback or copy data that carry a "copy never" watermark.

4. Watermarking for Image Authentication

In authentication applications, the objective is to detect modifications of the data. This can be achieved with so -called "fragile watermarks" that have a low robustness to certain modifications. Nevertheless, among all possible watermarking applications, authentication watermarks require the lowest level of robustness by definition.

Evaluation and Benchmarking of Watermarking Systems

Besides designing digital watermarking methods, an important issue addresses proper evaluation and benchmarking. This not only requires evaluation of the robustness, but also includes subjective or quantitative evaluation of the distortion introduced through the watermarking process. In general, there is a trade -off between watermark robustness and watermark perceptibility. Hence, for fair benchmarking and performance evaluation one has to ensure that the methods under investigation are tested under comparable conditions.

Performance Evaluation and Representation

Independent of the application purpose type of data, the *robustness of watermarks depends on the following aspects*:

• **Amount of embedded information.** This is an important parameter since it directly influences the watermark robustness. The more information one wants to embed, the lower the watermark robustness.

• **Watermark embedding strength**. There is a trade-off between the watermark embedding strength (hence the watermark robustness) and

watermark perceptibility. Increased robustness requires a stronger embedding, which in turn increases perceptibility of the watermark.

• **Size and nature of data.** The size of the data has usually a direct impact on the robustness of the embedded watermark. For example, relatively small images used for image watermarking do not have significant commercial value; nevertheless, a marking software program needs to be able to recover a watermark.

Distortion Metrics used for Evaluation:

1- Mean Squared Error (MSE)

The most common measures applied to image quality are Mean Squared Error (MSE) and Peak Signal-to-Noise Ratio (PSNR). The MSE measure is used to compare two images (or signals) by describing the degree of similarity between them. It is assumed that one of the images is original and the other is distorted. The formula for MSE is:

$$\text{MSE}= \frac{1}{MN} \sum_{j=1}^{M} \sum_{k=1}^{N} \left(x_{jk} - x_{jk}^{'}\right)^2$$

2- Peak-Signal-to-Noise-Ratio (PSNR)

PSNR is the most widely used objective image quality metric, and the average PSNR over all frames can be considered a video quality metric. PSNR is used as a measure of the quality of modified image, the signal in this case is the original image (cover image) and the noise is the error introduced (stego image). PSNR is defined via the MSE, the high value of PSNR indicates the high quality of the image, where PSNR is measured in decibels (dB). The formula for PSNR is:

$$\text{PSNR} = 10 \log_{10} \left(\frac{\text{L}^2}{MSE}\right)$$

Where L is the maximum gray level.
MSE is the mean square error between the original and the modified image (or signal).

3- Average Difference (AD)

Average Difference (AD) is the average difference between two images (or signals). A lower value of the Average Difference (AD) gives high image quality. The formula for AD is:

$$\text{AD}= \frac{1}{MN} \sum_{j=1}^{M} \sum_{k=1}^{N} \left(x_{jk} - x_{jk}^{'}\right)$$

4- Maximum Difference (MD)

Maximum Difference (MD) is one of the measures that take the maximum difference between the original image and modified image, large value of MD means that the image is of poor quality. The formula of MD is:

$$\text{MD} = \max\left(\left|x_{jk} - x'_{jk}\right|\right)$$

Where in the formulas above, the variables represent the following:

M represents the number of pixels in the row direction,

N represents the number of pixels in the column direction

x Represents the pixel of original image

$x^{'}$ Represents the pixel of modified image

And also, there are several other methods, such as the Structured Similarity Index (SSIM), Laplacian Mean Square Error (LMSE), Signal-to-Noise-Ratio (SNR) and etc.

Example: Find the image quality using the following quality measurements MSE, PSNR, AD and MD.

original image $=\begin{bmatrix}3 & 2 & 1\\ 1 & 2 & 1\\ 3 & 2 & 2\end{bmatrix}$ modified image $=\begin{bmatrix}3 & 2 & 2\\ 1 & 1 & 2\\ 1 & 1 & 1\end{bmatrix}$

Sol:

1- MSE$=\frac{1}{MN}\sum_{j=1}^{M}\sum_{k=1}^{N}\left(x_{jk}-x'_{jk}\right)^2$

MSE$=\frac{1}{9}[(3-3)^2+(2-2)^2+(1-2)^2+(1-1)^2+(2-1)^2+(1-2)^2+(3-1)^2+(2-1)^2+(2-1)^2]$

$=\frac{1}{9}[0+0+1+0+1+1+4+1+1]=1$

2- PSNR $=10\log_{10}\left(\frac{L^2}{MSE}\right)=10\log_{10}\left(\frac{255^2}{1}\right)=48.13$ dB

3- AD$=\frac{1}{MN}\sum_{j=1}^{M}\sum_{k=1}^{N}\left(x_{jk}-x'_{jk}\right)$

AD$=\frac{1}{9}([(3-3)+(2-2)+(1-2)+(1-1)+(2-1)+(1-2)+(3-1)+(2-1)+(2-1)])=\frac{1}{9}[0+0-1+0+1-1+2+1+1]$

$=\frac{3}{9}=0.33$

4- MD $=\max\left(\left|x_{jk}-x'_{jk}\right|\right)$

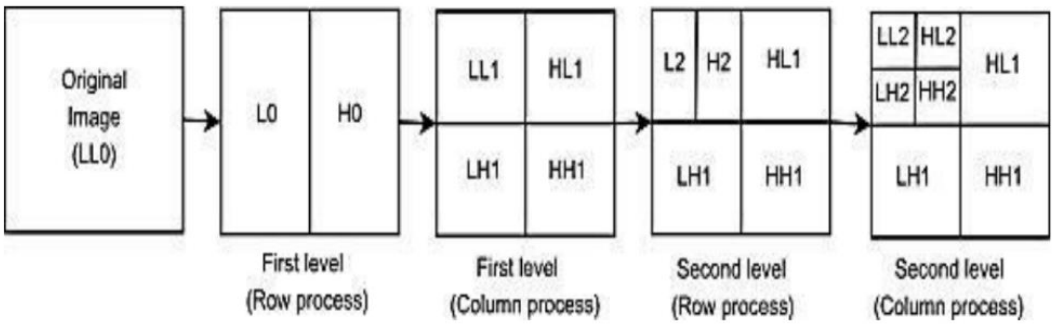
$=\max(|3-3|,|2-2|,|1-2|,|1-1|,|2-1|,|1-2|,|3-1|,|2-1|,|2-1|)$

$=\max(|0|,|0|,|-1|,|0|,|1|,|-1|,|2|,|1|,|1|)=2$

Watermarking Techniques

Wavelet Domain

Wavelets are becoming a key technique in the ongoing source compression standard JPEG-2000. In several recent publications, this technique has been applied to image watermarking. The positive arguments closely resemble those for advocating DCT for JPEG. The multi resolution aspect of wavelets is helpful in managing a good distribution (i.e., location) of the message in the cover in terms of robustness versus visibility. The wavelet transform consists in a multiscale spatial-frequency decomposition of an image. By applying wavelet, the image is actually decomposed into four sub bands. These four sub bands arise from separable applications of vertical and horizontal filters. The sub-bands labeled Low-High (LH), High-Low (HL) and High-High (HH) represent the finest scale wavelet coefficients (i.e., detail images) while the sub-band Low-Low (LL) corresponds to coarse level coefficients (i.e., approximation image). To obtain the next coarse level of wavelet coefficients, the sub band LL alone is further decomposed and critically sampled in iterative manner. Figure below shows the Lena's decomposition with three scale factors. The lowest frequency band at the lowest scale factor is found in the top-left corner (LL3).



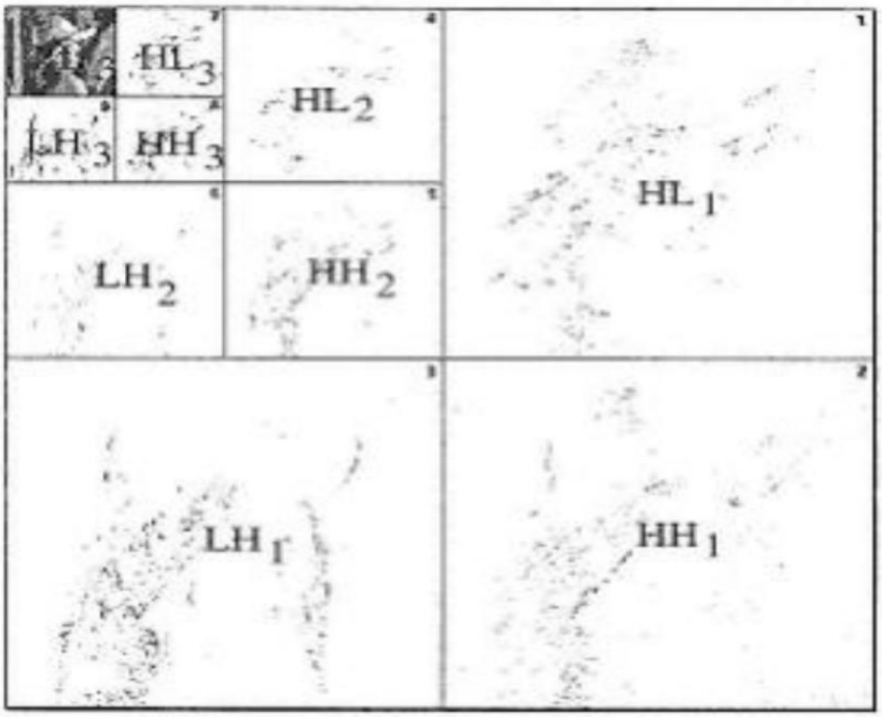


Figure: Multiscale decomposition.

Multimedia Fingerprinting

Fingerprinting refers to the process of adding fingerprints to an object or of identifying fingerprints that are already intrinsic to an object.

Examples of Fingerprinting

Human fingerprints: It is known that each fingerprint has a different pattern that distinguishes it from others. For investigation purpose, human fingerprints are collected from prisoners and criminals. Human fingerprints are also used for access control as shown in several spy movies.

Fired bullet: Each weapon has its own type of fired bullet depending on both the manufacturer and the type of weapon. Typewriters are similar; each typewriter has its own typesets.

PGP public keys: PGP (Pretty Good Privacy) is one of the most widely used public key packages and fingerprints for PGP public keys are used as one of the most important methods of identification. This fingerprint is almost unique, and can be used as an identifier in directories of keys such as the Global Internet Trust Register.

Digital audio/video: It has been suggested to use fingerprints to check out piracy of video data. In a pay-TV broadcast system, fingerprinting is applied to trace illegal subscribers.

Documents: As copyright protection means, fingerprinting is used in documents to discourage copying.

Terminology of Fingerprinting

A mark is a portion of an object and has a set of several possible states; a fingerprint is a collection of marks; a *distributor* is an authorized provider of fingerprinted objects to users; an *authorized user* is an individual who is authorized to gain access to a fingerprinted object; an *attacker* is an individual who gains unauthorized access to fingerprinted objects; and a *traitor* is an authorized user who distributes fingerprinted objects illegally.

Classification

Fingerprinting can be classified by the objects to be fingerprinted, detection sensitivity, fingerprinting methods, and generated fingerprints. These four categories are not exclusive.

1. Object-Based Classification

There are two categories in object-based classification: *digital fingerprinting and physical fingerprinting*. If an object to be fingerprinted is in digital format so that computers can process fingerprints, we call it **digital fingerprinting**. If an object has its own physical characteristics that can be used to differentiate it from others, we speak of **physical fingerprinting**. Human fingerprints, iris patterns, voice patterns, and coded particles of some explosives are of this type.

2. Detection-Sensitivity-Based Classification

Based on the detection sensitivity against violation, we classify fingerprinting into three categories: *perfect fingerprinting, statistical fingerprinting, and threshold fingerprinting*. If any alteration to the objects that makes the fingerprint unrecognizable must also make the object unusable, we speak of **perfect fingerprinting**. Thus the fingerprint generators can always identify

the attacker by one misused object. **Statistical fingerprinting** is less strict. Given many sufficiently misused objects to examine, the fingerprint generators can gain any desired degree of confidence that they have correctly identified the compromised user. The identifier is, however, never certain. **Threshold fingerprinting** is a hybrid type of the above two. It allows a certain level of illegal uses, say threshold, but it identifies the illegal copy when the threshold is reached. Thus it is allowed to make copies of an object less than the threshold, and the copies are not detected at all. When the number of copies exceeds the threshold, the copier is traced.

3. Fingerprinting Method-Based Classification

Primitive methods for fingerprinting such as *recognition, deletion, addition, and modification* have also been used as another classification criterion. If the fingerprinting scheme consists of recognizing and recording fingerprints that are already part of the object, it is of **recognition type**; examples are human fingerprints and iris patterns. In **deletion-type fingerprinting**, some legitimate portion of the original object is deleted. If some new portion is added to the object, it is of **addition type**. The additional part can be either sensible or meaningless. When a change to some portion of the object is made, it is of **modification type**; examples are maps with variations.

4. Generated Fingerprint-Based Classification

We may identify two types of fingerprints: *discrete fingerprinting and continuous fingerprinting*. If the generated fingerprint has a finite value of discontinuous numbers, the fingerprint is called **discrete**. Examples include hash values of digital files. If the generated fingerprint has a continuous value and essentially there is no limit to the number of possible values, the fingerprint is called **continuous**. Most physical fingerprints are of this type.

Fingerprinting Schemes

In this section, we list important achievements in fingerprinting, which are statistical fingerprinting, traitor tracing, collusion-secure fingerprinting, asymmetric fingerprinting, and anonymous fingerprinting. and summarize traitor tracing.

Traitor Tracing

When the set of people that have access to the secret is large, however, a more complex situation arises. If all of them share exactly the same data, the problem of determining guilt or innocent is unsolvable. One possibility to find a traitor from the secret sharers is to give a slightly different secret to the sharers. For this application, it is necessary to identify whether piracy is going on and to prevent information transfer to pirate users while harming no legitimate users. Furthermore, the legal evidence of the pirate identity should be provided. An application of their scheme to trace pirates who abuse a broadcast encryption scheme under the above requirements is presented. The distributor generates a base set R of r random keys and assigns m keys out of R to every user, which form the user's personal key. Note that different personal keys may have a nonempty intersection. A traitortracing message consists of multiple pairs (enablingblock, cipherblock), see Figure below.

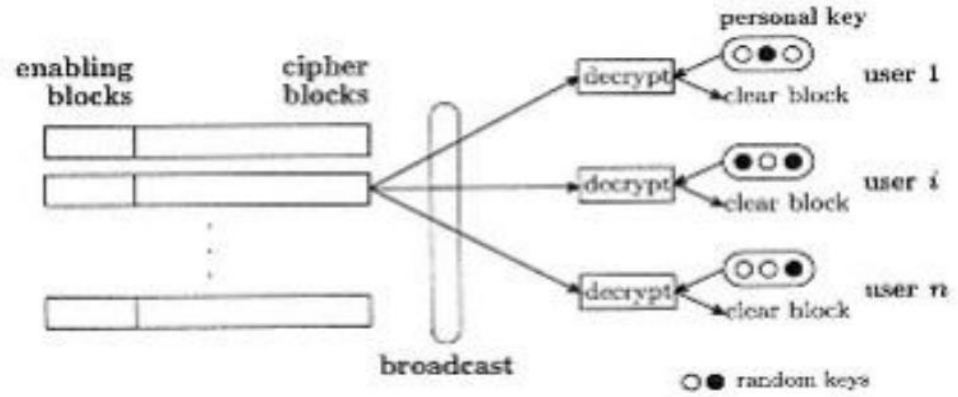


Figure: Traitor Tracing.

Biometric

Introduction

- The Term Biometric Comes from The Greek Words Bios (Life) And Metrikos (Measure).

- For our use, biometrics refers to technologies for measuring and analyzing a person's physiological or behavioral characteristics. These characteristics are *unique* to individuals, hence can be used to verify or identify a person.

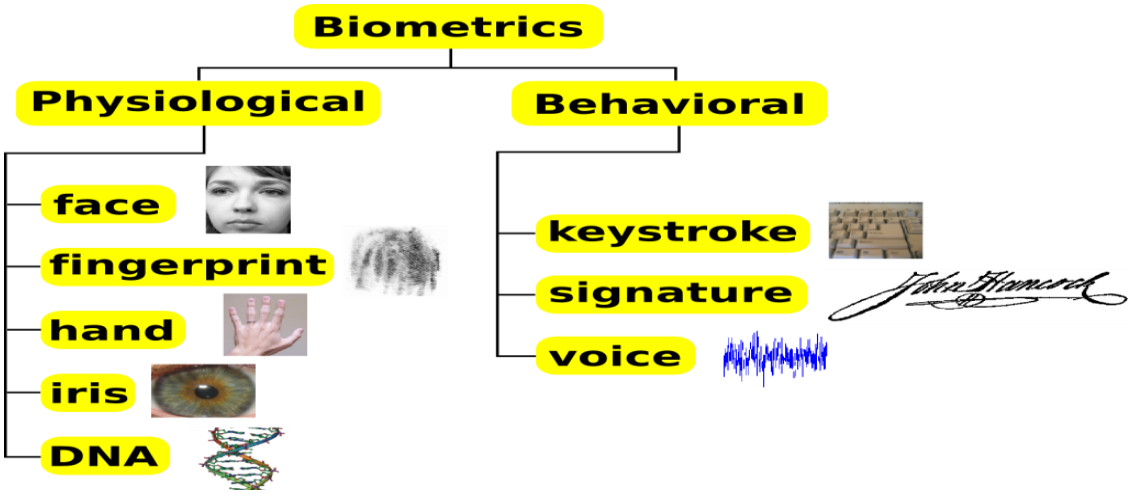
- Because a biometric property is an intrinsic property of an individual, it is difficult to duplicate and nearly impossible to share.

Why Biometric?

- Passwords are not reliable.
  - Can be stolen
  - Forgotten
  - Shared
  - Many passwords easy to guess
  - PIN Can be duplicated
  - PIN can be Lost or stolen
- Protect Sensitive Information
  - Banking
  - Commercial
  - Government

What is Biometric?

Biometrics can be physiological and/or behavioral characteristics. These characteristics are unique to individuals, hence can be used to verify or identify a person. Figure below shows some examples of different biometrics.



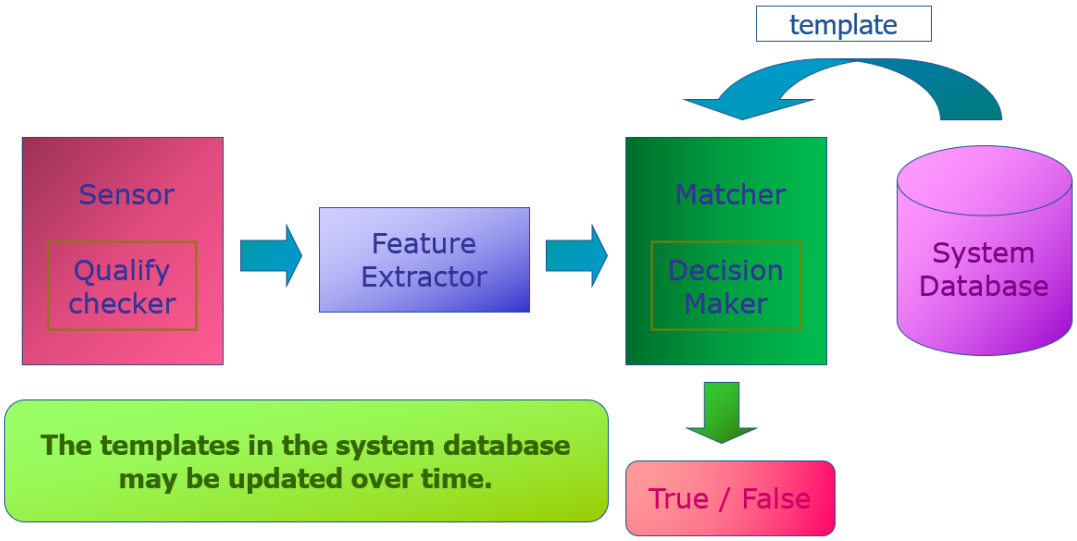
Biometric System

- A biometric system may operate either in verification mode or identification mode.
  - A. Verification mode:
    - "Does this biometric data belong to Bob?"
    - It determines whether the person is indeed who he claims to be.
  - B. Identification mode:
    - "Whose biometric data is this?"
    - It determines the identity of the person.

- "Recognition" is the generic term of verification and identification.

- A Biometric System is designed using the following four main modules:
  1) Sensor Module (Quality Checking Module).
  2) Feature Module.
  3) Matcher Module (Decision Making Module).
  4) System Database Module.

A sample flow chart:



Biometrics Techniques

- Retina scanning
- Iris scanning
- Fingerprint scanning
- Hand scanning
- Face recognition
- Voice recognition
- Signature recognition
- Keystroke recognition
- DNA
- Body color

Fingerprint Scanning:

- "Fingerprint authentication" describes the process of obtaining a digital representation of a fingerprint and comparing it to a stored digital version of a fingerprint.
- Measures unique characteristics in a fingerprint (minutiae) , which are:

– Crossover
– Core
– Bifurcations
– Ridge ending
– Island
– Delta
– Pore

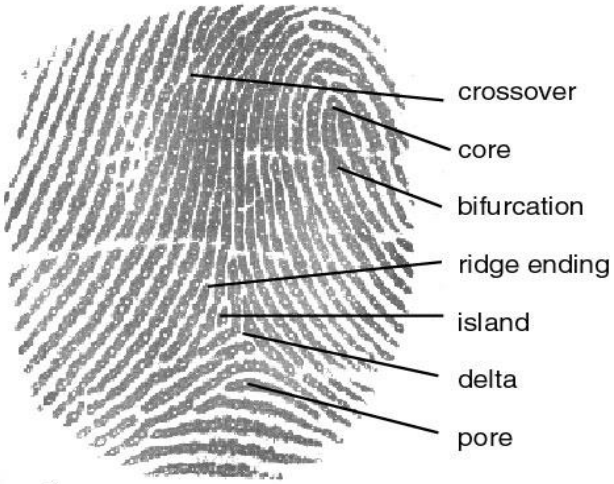
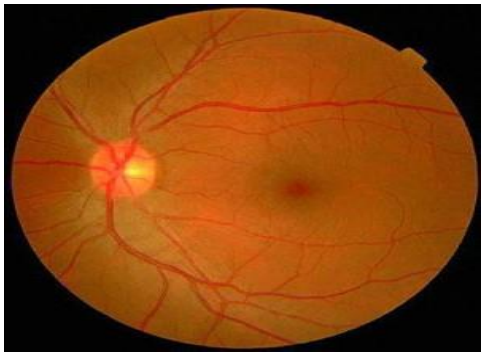


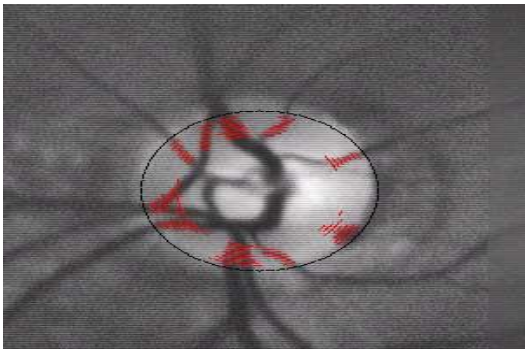
Figure 1

Retina Scanning:

Measures unique characteristics of the retina, which are:

- Blood vessel patterns.
- Vein patterns.



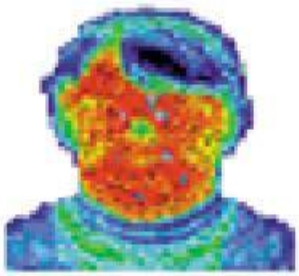


Facial Scanning:

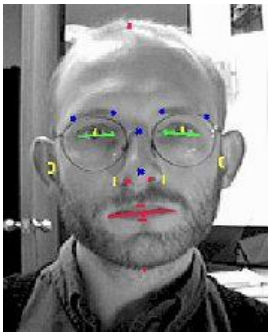
Uses off-the-shelf camera to measure the following facial features:

- Distance between the eyes.
- Distance between the eyes and nose ridge.
- Angle of a cheek.
- Slope of the nose.
- Facial Temperatures.

face



facial thermogram



Voice Pattern:

- Identification of the person who is speaking by characteristics of their voices (*voice biometrics*), also called **Voice Patterns**.
- There is a difference between ***speaker recognition*** (recognizing **who** is speaking) and ***speech recognition*** (recognizing **what** is being said).
- Measure the following features:

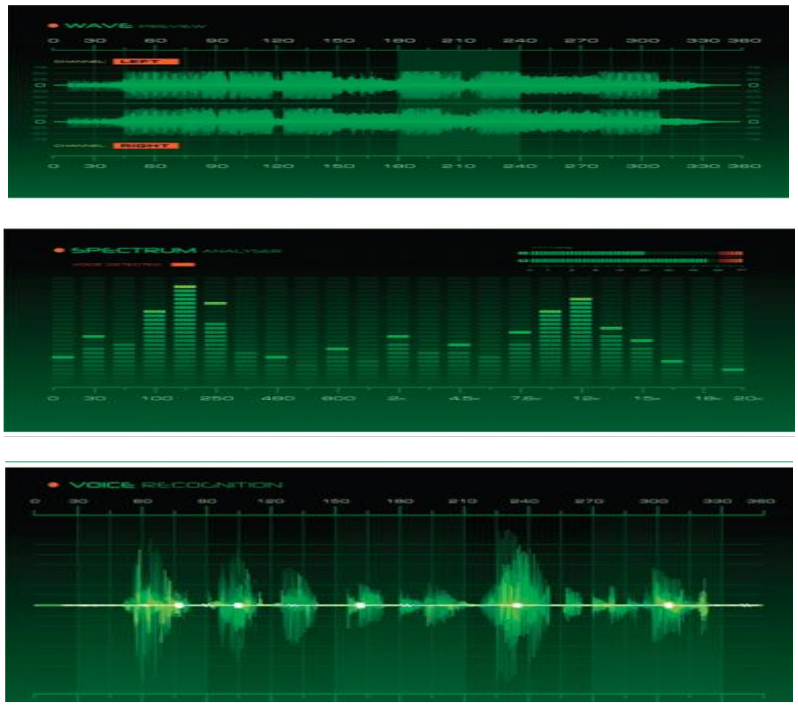
– Pitch

– Quality

– Strength

– Frequency

– Tone



Biometric System Errors

A biometric verification system makes two types of errors:

1) Mistaking biometric measurements from two different persons to be from the same person (called *False Match*).
2) Mistaking two biometric measurements from the same person to be from two different persons (called *False Non-match*).

Application of Biometric Systems

The application of biometric can be divided into five main groups: forensic, government, commercial, health-care and travelling and immigration.

1) **Commercial**

   ATM, credit card, cellular phone, distance learning, etc.
2) **Government**

   ID card, driver's license, social security, etc.
3) **Forensic**

   terrorist identification, missing children, etc.
4) **Health-Care**

   Access to medical details, Patient Info, etc.
5) **Travelling and Immigration**

   Air Travel, Boarder Crossing, Passport, etc.

Example - Face Recognition in Airport