4. Hypothesis

Digital watermarking is a technology that came after two most important methods namely cryptography and steganography.

4.1 Cryptography

Cryptography is a greek word and it simply means secret writing which may be divided into two parts.

4.1.1 Encryption

Encryption is a means of converting a plain text into the cipher text by manipulating the text with the help of a secret key which is known only to the transmitter and the receiver. Example of the encryption is given below.

Let a number 2-two is the secret key and one need to transmit a word named JJTU then the number is added to each letter of the word so as to make that word LLVW and this word is transmitted instead of the original. Third person apart from transmitter and receiver can’t detect the word.

4.1.2 Decryption

Decryption is the reverse process to that of the encryption means getting the plain text back from the cipher text with the help of the same key which was used by the transmitter and with the help of the reverse algorithm to that used at the transmitter.

In our example LLVW is received and we have a number 2-two as our secret key. Receiver knows that addition process is performed at the transmitter end and hence the receiver performs the subtraction process and can get the word JJTU back.

The problem which resides with the cryptography is that the third person can try to decode the message and with the increase in technology now it is very easy task to find the secret key and hence becomes easy to decode the message.

4.2 Steganography

Cryptography protects the content of the message but a new scheme named steganography is used to hide the existence of the message. Steganography is also a greek work and it means covered writing. Example of the system is shown in figure 4.1
4.3 Watermarking

Watermarking also describes the same terminologies as steganography but there are differences between the steganography and watermarking.

1. Steganography only can be used for point to point communication where as watermarking can be used for point to multipoint communication also.

2. Steganography methods are very sensitive to any changes in the cover medium. If the cover medium is change the hidden message completely vanishes. But in case of watermarking, there are methods with the help of which one can protect the message even after some degradation given to the cover medium. Technical name given to this phenomenon of keeping the message even after modification of the cover medium is robustness.

Robustness of the watermarking methods gives more weight age to them compare to steganography.

The process of hiding a watermark is called embedding and process of taking the watermark back is called extracting. The ideas of embedding and extraction are given in figure 4.2 and 4.3 respectively.
4.4 Requirement of Watermarking

There are various requirements that the watermarking scheme should have. They are explained as under.

4.4.1 Robustness

If the watermarking algorithm is able to preserve the message under various modifications like rotation, cropping, scaling, filtering or noise addition, then that method is said to be robust.

4.4.2 Imperceptibility

After watermark is embedded in the cover medium, if the visual quality of the cover medium is such that the changes cannot be noticed with the naked eye, then the method is called imperceptible.
4.2.3 Payload Capacity

It is the size of the message that can be embedded inside a cover medium. It depends on the method used for the watermarking.

Above three requirements carries a trade off triangle as shown in figure 4.4 which states that to achieve two of the three requirements, third one should be traded off. For example to achieve higher robustness and good perceptibility, one need to through away the requirement of higher payload capacity.

![Figure 4.4: Tradeoff between Robustness, Imperceptibility and Payload Capacity](image)

4.5 Types of Watermarking

Figure 4.5 shows various ways in which one can use the concept of watermarking.

![Figure 4.5: Types of Watermarking](image)
4.5.1 Spatial Domain Watermarking

In this method the pixel information of the two-dimensional image is altered so as to embed the hidden data. Three Different techniques are defined in the spatial domain watermarking:

1. Least Significant Bit Technique
2. Correlation Based Technique
3. Spread Spectrum Based Technique

4.5.2 Transform Domain Watermarking

Transform Domain watermarking implies the use of various transforms to be applied on the cover medium so as to find out the frequency coefficients and then changing these coefficients according to the watermark information. Most powerful transforms used for the purpose of copyright protection are:

1. The Discrete Fourier Transform (DFT)
2. The Discrete Cosine Transform (DCT)
3. The Discrete Wavelet Transform (DWT).

4.5.3 Invisible Watermarking

This is the technique of hiding the message in such a way that it can’t visibly be detected by a common man.

4.5.4 Visible Watermarking

In this technique the watermark is superimposed on the cover object in such a way that it can be perceptually visible.

4.5.5 Source Based Watermarking

This technique is used when owner of a document wants to distribute the document to multiple destinations with the same authentication information. The method is used for authentication purpose. With this method one can identify whether the received document is tempered or not.

4.5.6 Destination Based Watermarking

The purpose of this kind of technique is same as source based scheme but here each receiver gets unique watermark information that is embedded behind the document.
Only that receiver can open that document. This method can prevent illegal reselling of the document.