CHAPTER II
BASIC THEORY

II.1 Security System

In general, security is “the quality or state of being secure to be free from danger”. In other words, protection against adversaries from those who would do harm, intentionally or otherwise is the objective. National security, for example, is a multilayered system that protects the sovereignty of a state, its assets, its resources, and its people. Achieving the appropriate level of security for an organization also requires a multifaceted system.

A successful organization should have the following multiple layers of security in place to protect its operations:

1. Physical security, to protect physical items, objects, or areas from unauthorized access and misuse
2. Personnel security, to protect the individual or group of individuals who are authorized to access the organization and its operations
3. Operations security, to protect the details of a particular operation or series of activities
4. Communications security, to protect communications media, technology, and content
5. Network security, to protect networking components, connections, and contents
6. Information security, to protect the confidentiality, integrity and availability of information assets, whether in storage, processing, or transmission. It is achieved via the application of policy, education, training and awareness, and technology.

The Committee on National Security Systems (CNSS) defines information security as the protection of information and its critical elements, including the systems and hardware that use, store, and transmit that information.

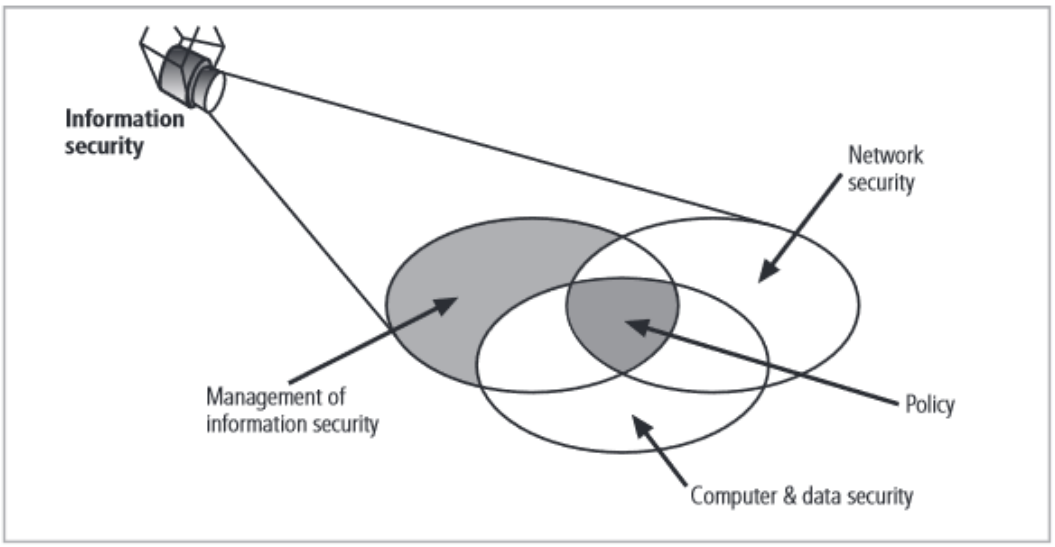

Figure 2.1 Components of Information Security (REF: [1])

Figure 2.1 shows that information security includes the broad areas of information security management, computer and data security, and network security. The CNSS model of information security evolved from a concept developed by the computer security industry called the C.I.A. triangle. The C.I.A. triangle has been the industry standard for computer security since the development of the mainframe. It is based on the three characteristics of information that give it value to organizations: confidentiality, integrity, and availability. The security of these three characteristics of information is as important today as it has always been, but the C.I.A. triangle model no longer adequately addresses the constantly changing environment. The threats to the confidentiality, integrity, and availability of information have evolved into a vast collection of events, including accidental or intentional damage, destruction, theft, unintended or unauthorized modification, or other misuse from human or nonhuman threats. This new environment of many constantly evolving threats has prompted the development of a more robust model that addresses the complexities of the current information security environment.[1]

II. 2 Definition of Encryption

Encryption is one of the principal means to guarantee security of sensitive information. Encryption algorithm performs various substitutions and transformations on the plaintext (original message before encryption) and transforms it into cipher text (scrambled message after encryption). Many

encryption algorithms are widely available and used in information security. Encryption algorithms are classified into two groups: *Symmetric-key* (also called secret-key) and *Asymmetric-key* (also called public-key) encryption [2].

Figure 2.2 Encryption (REF: http://www.tectrade.com/wp-content/uploads/2015/10/encryption.jpeg)

Symmetric key encryption is a form of cryptosystem in which encryption and decryption are performed using the same key. It is also known as conventional encryption.

Asymmetric encryption is a form of cryptosystem in which encryption and decryption are performed using the different keys – one a public key and one a private key. It is also known as public-key encryption [3].

A Key is a numeric or alpha numeric text or may be a special symbol. The Key is used at the time of encryption takes place on the Plain Text and at the time of decryption takes place on the Cipher Text. The selection of key in Cryptography is very important since the security of encryption algorithm depends directly on it. The strength of the encryption algorithm relies on the secrecy of the key, length of the key, the initialization vector, and how they all work together [4].

Asymmetric encryption techniques are about 1000 times slower than Symmetric encryption which makes it impractical when trying to encrypt large amounts of data. Also to get the same security strength as symmetric, asymmetric must use a stronger key than symmetric encryption technique [5].

II.3 Definition of Steganography

Steganography deals with hiding messages in a cover signal so that they can be extracted at the receiving side with the help of a secret key. Applications of steganography include covert communications, watermarking and fingerprinting that seem to hold promise for copyright protection, tracing source of illegal copies, etc.

Figure 2.3 Steganography (REF: http://www.jjtc.com/Steganography/steg05.jpg)

There are several issues to be considered when studying steganographic systems. One among the key performance measures used to compare different message embedding algorithms is *steganography capacity*. In a general sense, it is the maximum message size that can be embedded subject to certain constraints [6].

II.4 Definition of Digital Watermarking

Digital Watermarking is a branch of information hiding which is used to hide proprietary information in digital media like photographs, digital music, or digital video. The ease with which digital content can be exchanged over the Internet has created copyright infringement issues.

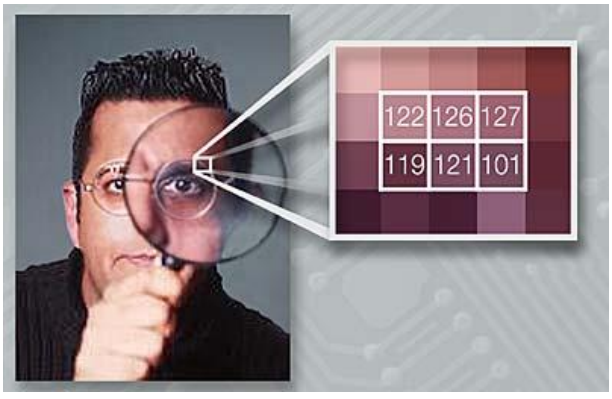

Figure 2.4 Digital Watermarking (REF: http://wiki.cas.mcmaster.ca/images/d/d1/Stegwatermark.png)

Copyrighted material can be easily exchanged over peer-to-peer networks, and this has caused major concerns to those content providers who produce these digital contents. In order to protect the interest of the content providers, these digital contents can be watermarked. In this paper we provide a survey of the latest techniques that are employed to watermark images. Image watermarking techniques can be applied to digital videos as well [7].

II.5 History of Digital Watermarking

Although the art of papermaking was invented in China over one thousand years earlier, paper watermarks did not appear until about 1282, in Italy. The marks were made by adding thin wire patterns to the paper molds. The paper would be slightly thinner where the wire was and hence more transparent. The meaning and purpose of the earliest watermarks are uncertain. They may have been used for practical functions such as identifying the molds on which sheets of papers were made, or as trademarks to identify the paper maker. On the other hand, they may have represented mystical signs, or might simply have served as decoration. By the eighteenth century, watermarks on paper made in Europe and America had become more clearly utilitarian. They were used as trademarks.

The term watermark seems to have been coined near the end of the eighteenth century and may have been derived from the German term *wasser-marke* (though it could also be that the German word is derived from the English. The term is actually a misnomer, in that water is not especially important in the creation of the mark. It was probably given because the marks resemble the effects of water on paper.

About the time the term watermark was coined, counterfeiters began developing methods of forging watermarks used to protect paper money. In 1779 Gentleman's Magazine reported that a man named John Mathison. John Mathison was hanged. Counterfeiting prompted advances in watermarking technology. William Congreve, an Englishman, invented a technique for making color watermarks by inserting dyed material into the middle of the paper during papermaking.

The resulting marks must have been extremely difficult to forge, because the Bank of England itself declined to use them on the grounds that they were too difficult to make. A more practical technology was invented by another English-man, William Henry Smith. This replaced the fine wire patterns used to make earlier marks with a sort of shallow relief sculpture, pressed into the paper mold. The resulting variation on the surface of the mold produced beautiful watermarks with varying shades of gray. This is the basic technique used today for the face of President Jackson on the $20 bill

In 1951, Emil Hembrooke of the Muzak Corporation filed a patent for watermarking musical Works. An identification code was inserted in music by intermittently applying a narrow notch filter centered at 1 kHz. The absence of energy at this frequency indicated that the notch filter had been applied and the duration of the absence used to code either a dot or a dash. The Identification signal used Morse code.

It was probably 1990s the term digital watermarking really came into vogue. About 1995, interest in digital watermarking began to mushroom. In the late 1990s several companies were established to market watermarking products. Most recently, a number of companies have used watermarking technologies for variety applications.[8]

II.6 Types of Digital Watermarking

There are 5 types of digital watermarking according Chawla, Saini, Yadav & Kamaldeep:

1. Division Based on Human Perception

   This is sub-divided into visible watermarks and invisible watermarks.

   a. Visible Watermarks

      These watermarks can be seen clearly by the viewer and can also identify the logo or the owner. Visible watermarking technique changes the original signal. The watermarked signal is different from the original signal.

Visible watermark embedding algorithms are less computationally complex. The watermarked image cannot with stand the signal processing attacks, like the watermark can be cropped from the watermarked image.

Figure 2.5 Visible Watermarked Image (REF: [9])

Spreading the watermark throughout the image is a best option, but the quality of the image is degraded which prevents the image from being used in medical applications.

b. Invisible Watermarks

These watermarks cannot be seen by the viewer. The output signal does not change much when compared to the original signal.

Figure 2.6 Invisible Watermarked Image (REF: [8])

The watermarked signal is almost similar to the original signal. As the watermark is invisible, the imposter cannot crop the watermark as in visible watermarking. Invisible watermarking is more robust to signal processing attacks when compared to visible watermarking. As

the quality of the image does not suffer much, it can be used in almost all the applications.

2. Division Based on Application

Based on application watermarks are sub-divided into fragile, semi-fragile and robust watermarks.

a. Fragile Watermarks

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

Figure 2.7 Fragile Watermarked Images (REF: [9])

b. Semi Fragile Watermarks

These watermarks are broken if the modifications to the watermarked signal exceed a pre-defined user threshold. If the threshold is set to zero, then it operates as a fragile watermark. This method can be used to ensure data integrity and also data authentication.

c. Robust Watermarks

These watermarks cannot be broken easily as they withstand many signal processing attacks. 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

3. Division Based On Level Of Information Required To Detect The Embedded Data

Based on the level of required information all watermarks are sub-divided into blind watermarks, semi-blind watermarks and non-blind watermarks

a. Blind Watermarks

These watermarks detect the embedded information without the use of original signal. They are less robust to any attacks on the signal.

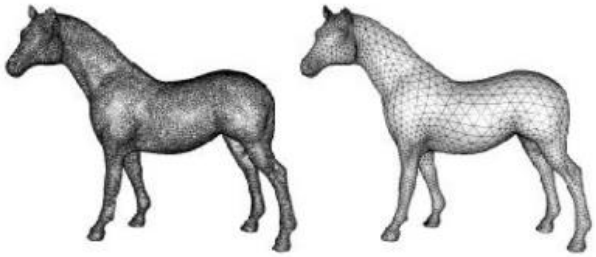

Figure 2.8 Blind Watermarks (REF: https://image.slidesharecdn.com/applicability-of-tracability-technologies-for-3d-printing-robust-blind-watermarking-ucl-150217034026-conversion-gate02/95/applicability-oftracabilitytechnologiesfor3-dprintingrobustblindwatermarkingucl-12-638.jpg?cb=1424145020)

b. Semi Blind Watermarks

These watermarks require some special information to detect the embedded data in the watermarked signal.

c. Non Blind Watermarks

These watermarks require the original signal to detect the embedded information in the watermarked signal. They are more robust to any attacks on the signal when compared to blind watermarks.

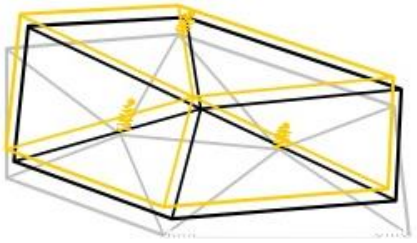

Figure 2.9 Non Blind Watermarks (REF: https://image.slidesharecdn.com/applicability-of-tracability-technologies-for-3d-printing-robust-blind-watermarking-ucl-150217034026-conversion-gate02/95/applicability-oftracabilitytechnologiesfor3-dprintingrobustblindwatermarkinguc l-12-638.jpg?cb=1424145020)

4. Division Based On User's Authorization To Detect The Watermark

   This is sub-divided into public watermarks and private watermarks

   a. Public Watermarks

      In this watermarking, the user is authorized to detect the watermark embedded in the original signal.

   b. Private Watermarks

      In this watermarking, the user is not authorized to detect the watermark embedded in the original signal.

5. Division Based on Knowledge of The User on The Presence of The Watermark

   This is sub-divided into steganographic watermarking and non-steganographic watermarking.

   a. Steganographic Watermarking

      The user is not aware of the presence of the watermark.

   b. Non-Steganographic Watermarking

The user is aware of the presence of the watermark