Chapter 1

Introduction

1.1 Introduction

In last 2 decades the Internet emerged as a dominant media for communication. For examples, simple mail communication, facebook, twitter, e-commerce, etc. are the major applications of the Internet. Providing security to the data in Internet is a very big challenge. We have security methodologies like steganography, watermarking, and cryptography to provide security to the data. The purpose of cryptography is to jumble the data, so that the intruder cannot understand it. While using cryptography for secret communication, the stranger cannot sense the data, but can detect the communication. But in case of steganography, the miscreant cannot feel that communication is happening. Steganography is the mechanism to camouflage data inside another carrier like text, image, video, and audio without compromising the original visual quality of the carrier medium. Watermarking is another mechanism of camouflaging data in a medium and the camouflaged data is known as the watermark. Watermarking is applicable for authentication and integrity check.

This Chapter talks briefly about cryptography, watermarking, and steganography techniques along with the quality attributes. At the end of this Chapter the research objectives are stated.

1.2 Data Security Techniques

As projected in Fig.1.1, data security methodologies have been listed in two categories, (i) Cryptography, and (ii) Data hiding. Cryptography is further divided into 2 types, (i) Symmetric key, and (ii) Asymmetric or public key cryptography. Similarly, the data hiding techniques can be divided into 2 types, (i) Watermarking, and (ii) Steganography.

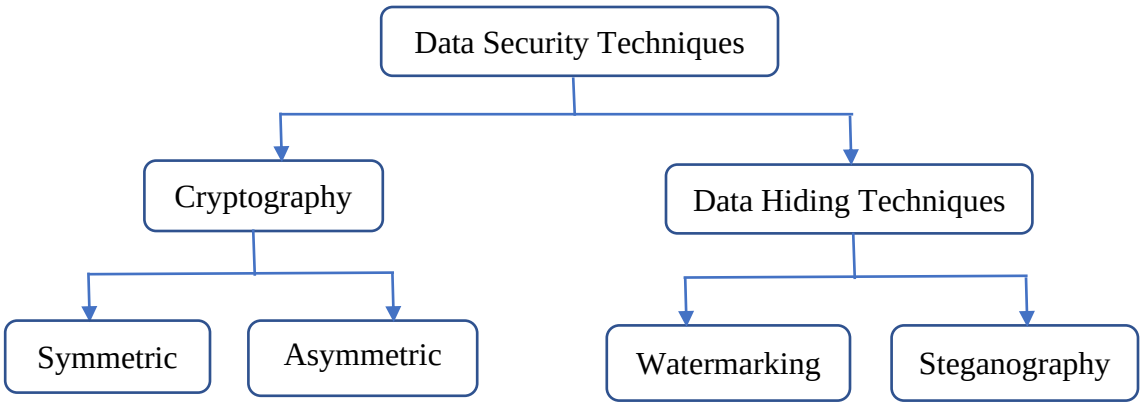


Fig.1.1 Taxonomy of data security techniques

Table 1.1 shows a comparison of the 3 security methodologies, cryptography, watermarking, and steganography. As we can see from this table, the purpose of cryptography is to make encryption at sender and decryption at receiver. Copyright protection has been the principal goal of watermarking, and the principal goal of steganography is un-noticeable communication or covert communication.

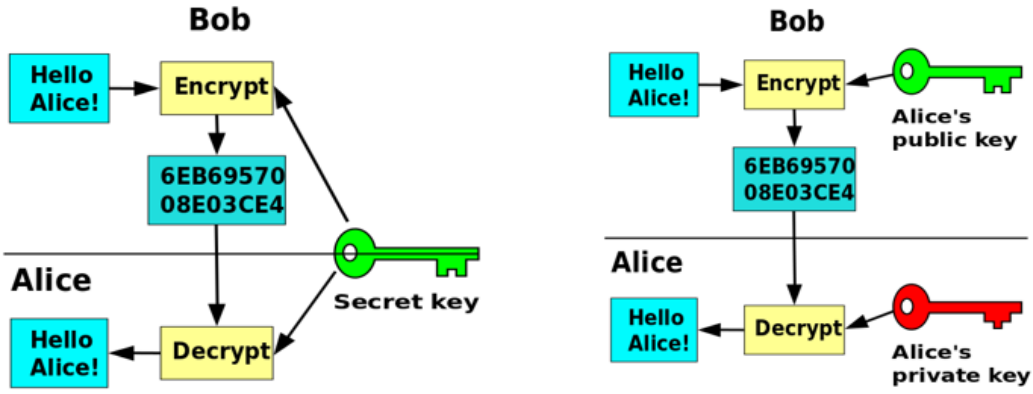
Table 1.1 Comparison of cryptography, watermarking, and steganography

	Cryptography	**Watermarking**	**Steganography**
Purpose	Un-understandable communication	Copyright protection and authentication	Hidden communication
Authentication	Can be achieved	Can be achieved	Can be achieved
Key	Mandatory	Optional	Optional
Attacks	Cryptanalytic attack, brute force attack	Image processing attacks, cropping, rotation etc.	Steganalysis like RS analysis, PDH analysis
Robustness	irrelevant	Must be higher	Must be higher
Imperceptibility	irrelevant	Must be higher	Must be higher
Merits	Can achieve confidentiality, and authentication	Can achieve confidentiality, and authentication	Can achieve unnoticeable communication
Demerits	The communication is visible	Hiding capacity is low	Cannot provide authentication

1.2.1 Cryptography

It is for un-understandable communication. It has 2 variants [1, 2], namely symmetric key and public key. In symmetric key cryptography, only 1 key is used for embedding/extraction, as projected in Fig.1.2(a). The second one is known as public key cryptography or asymmetric key cryptography, with 2 keys, (i) public, and (ii) private, as shown in Fig.1.2(b). Here, the private key must be secret. But the public key may be given to the partners. User A shares her public key (E_A) to Bob. Her private key (D_A) not shared. User B encrypts her message using key E_A, gets the cipher text, and shares to A. After receiving it, A decrypt it using D_A.

In symmetric key cryptography there is only one shared confidential key amid sender and receiver. This key should be confidential between them. If any third person knows the key, then the confidentiality will be on risk. The size of a key along with the combination of characters, digits, and special characters gives the strength to it. If the key is stronger, it cannot be easily broken. Similarly, in public key cryptography the private key should be stronger. The various applications of cryptography are, (i) confidential communication (ii) message authentication, (iii) user authentication, (iv) digital signature etc.



(a) Symmetric Key (b) Public Key

Fig.1.2 Cryptography

1.2.2 Watermarking

Watermarking is a methodology for overlapping a logo or some text on a file like video or image, and it is very useful for digital work marketing, and copyright defence. In watermarking,

we camouflage some watermark inside the medium and it is calculated from the bits of the medium. If the watermark is visible on the host medium it is known as visible watermark, otherwise it is noted as invisible watermark. Watermarking can be 3 types, such as robust, fragile, and semi-fragile. In fragile watermarking, after a slight modification to the host medium, the watermark is distorted. These are commonly applicable for authentication purposes. In robust watermarking, the watermark is retrievable after some modification in the host medium. These are commonly plied for copyright defence. The semi-fragile watermarking techniques take benefits from both fragile watermarking and robust watermarking. These are plied for both integrity verification and authentication. Furthermore, semi-fragile watermarking methodologies can be able to recognize the tempered zones and correct them.

1.2.3 Steganography

Steganography is known as an art of hidden communication. It is achieved by burying message bits in the carrier file which should look innocuous. In cryptographic approach the communication is secret, but miscreant can see it. In steganography the miscreant cannot see it and also cannot notice it. In cryptography the decryption and encryption algorithms may be openly advertised, but not the keys. In steganography the embedding and extraction procedures are not advertised. Steganography may be done with carriers like (i) text, (ii) audio, (iii) image, and (iv) video [3, 4], see Fig.1.3. When the unnatural message is kept inside a natural image, its inherent statistics must be preserved [5].

Image steganography has 2 main variants, spatial and transform domains. Spatial domain techniques are those, where hiding is done by manipulating the pixel values without any middle operation. Transform domain techniques are those, where we apply any transform on image and then apply data hiding. The image without camouflaged data is termed as the original image (OI). After putting the secret data in it, we call it as stego-image (SI).

“Modulus function (MF), pixel value differencing (PVD), LSB alteration, and exploiting modification direction (EMD), are the well-known techniques in spatial domain” [3]. In transform domain, “discrete wavelet transforms (DWT), fast Fourier transform (FFT), and discrete cosine transforms (DCT)” [6] are popular techniques. From the SI, if we can get back

both OI and secret data, then the steganography technique is known as reversible one [7, 8]. Otherwise, if only secret data can be obtained, then it known as an irreversible technique.

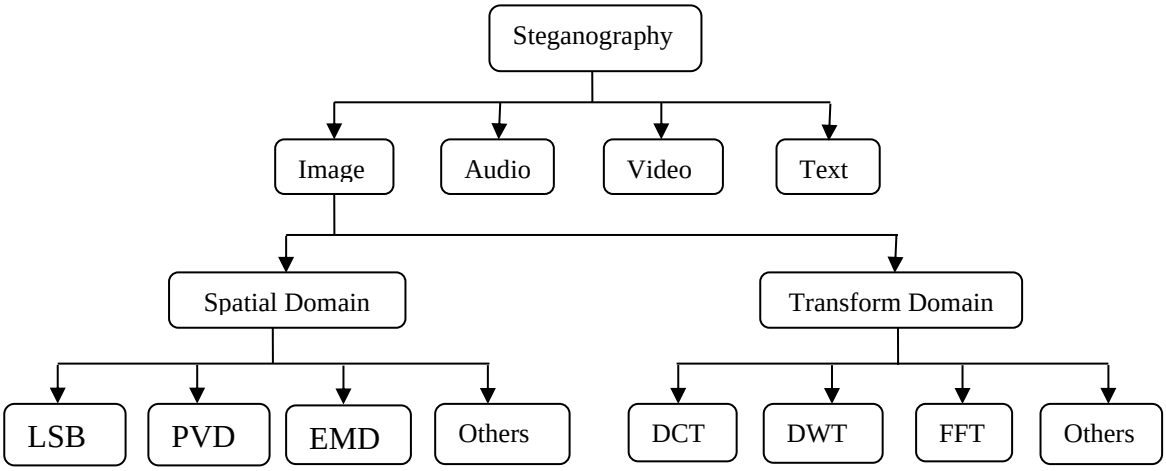


Fig.1.3 A Taxonomy of image steganography techniques

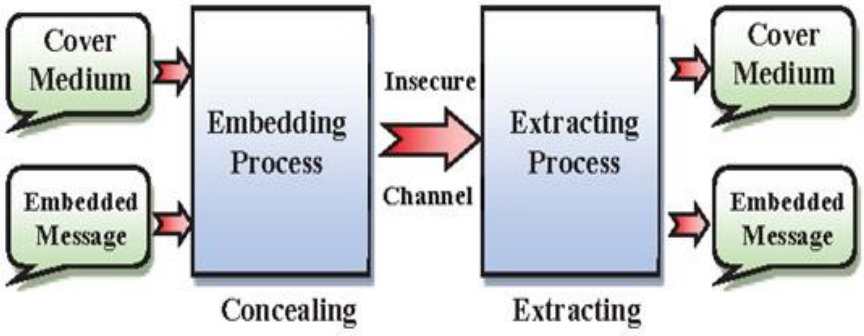


Fig.1.4 A General framework of reversible image steganography technique

Fig.1.4 models a reversible steganography technique. On sender side the secret data is hidden inside the image, and SI is created. It is shared to receiver and receiver extracts the camouflaged bits from it and regenerates the cover medium.

1.3 Quality assessment Parameters in Image Steganography

Refer Fig.1.5, the steganography methods are ranked by 3 parameters or qualifiers, (i) hiding capacity (HC), (ii) distortion assessment, and (iii) security [3]. We can also consider the hiding and extraction times as evaluation factors. The HC may also be presented in 2 ways, first one is total capacity, and second one is “bits per byte (BPB) or bits per pixel (BPP)”. HC is the

maximum count of bits allowed to camouflage in an image. Bits per pixel (BPP) is the mean HC per pixel. A superior steganography method should exhibit higher HC.

In SI, the distortion can be computed by "Mean of Square Error (MSE), Eq.1.1, Root of MSE (RMSE), Eq.1.2, Peak Signal-to-Noise Ratio (PSNR), Eq.1.3, Quality Index (QI), and weighted PSNR (WPSNR), Eq.1.4" [9, 10]. Here, p_{ij} and q_{ij} are the original and stego pixels, m and n represent the size of the image. If the MSE value is small, then SI is less distorted. The RMSE as computed is also a measure of distortion.

$$\text{MSE} = \frac{1}{m \times n} \sum_{i=1}^{m} \sum_{j=1}^{n} (p_{ij} - q_{ij})^2 \qquad (1.1)$$

$$\text{RMSE} = \sqrt{\frac{1}{m \times n} \sum_{i=1}^{m} \sum_{j=1}^{n} (p_{ij} - q_{ij})^2} \qquad (1.2)$$

If PSNR ≥ 40 decibels (dB) it is good. If PSNR falls amid 30 and 40 dB, we can still accept the SI. But if it falls below 30 dB, then the SI shall not be acceptable because of greater distortion.

$$\text{PSNR} = 10 \times \log_{10} \frac{255 \times 255}{\text{MSE}} \qquad (1.3)$$

WPSNR, demonstrated in Eq.1.4 is also plied to measure the distortion [11], where Noise Visibility Function (NVF) can be in between 0 and 1. The NVF is defined in Eq.1.5.

$$\text{WPSNR} = 10 \times \log_{10} \left(\frac{255}{\sqrt{\text{MSE}} \times \text{NVF}} \right)^2 \qquad (1.4)$$

$$\text{NVF}(i, j) = \frac{1}{1 + \sigma^2_{l(i,j)}} \qquad (1.5)$$

In NVF $\sigma^2_{l(i,j)}$ is the local variance from the central pixel at position (i, j).

Correlation, r is an assessment for equivalence amid SI and OI, as shown in Eq.1.6 [12], where $\bar{q}$ and $\bar{p}$ are the average values of pixels in SI and OI respectively. Equation 1.7 represents the QI to assess the alikeness amid the SI and OI.

$$r = \frac{\sum_{i=1}^{m} \sum_{j=1}^{n} (p_{ij} - \bar{p}) \times (q_{ij} - \bar{q})}{\sqrt{\left(\sum_{i=1}^{m} \sum_{j=1}^{n} (p_{ij} - \bar{p})^2 \right) \times \left(\sum_{i=1}^{m} \sum_{j=1}^{n} (q_{ij} - \bar{q})^2 \right)}} \qquad (1.6)$$

$$\text{QI} = \frac{4 \sigma_{xy} \bar{p} \bar{q}}{(\sigma_x^2 + \sigma_y^2)[(\bar{p})^2 + (\bar{q})^2]} \qquad (1.7)$$

Where $\bar{p}$, $\bar{q}$, σ_x^2, σ_y^2, and σ_{xy} are defined in Eqs. (1.8), (1.9), (1.10), (1.11), and (1.12) one by one.

$$\bar{p} = \frac{1}{m \times n} \sum_{i=1}^{m} \sum_{j=1}^{n} p_{ij} \quad (1.8)$$

$$\bar{q} = \frac{1}{m \times n} \sum_{i=1}^{m} \sum_{j=1}^{n} q_{ij} \quad (1.9)$$

$$\sigma_x^2 = \frac{1}{m \times n-1} \sum_{i=1}^{m} \sum_{j=1}^{n} (p_{ij} - \bar{p})^2 \quad (1.10)$$

$$\sigma_y^2 = \frac{1}{m \times n-1} \sum_{i=1}^{m} \sum_{j=1}^{n} (q_{ij} - \bar{q})^2 \quad (1.11)$$

$$\sigma_{xy} = \frac{1}{m \times n-1} \sum_{i=1}^{m} \sum_{j=1}^{n} (p_{ij} - \bar{p})(q_{ij} - \bar{q}) \quad (1.12)$$

Like QI, Structural Similarity (SSIM) can also be plied to compute the alikeness [13] as shown in Eq. 1.13, where the constants c_1 and c_2 are used to ensure the terms $(\bar{p}^2 + \bar{q}^2 + c_1)$ and $(\sigma_x^2 + \sigma_y^2 + c_2)$ are non-zero. The $c_1 = (K_1 L)^2$, wherein for a gray image, the L value is 255 and $K_1 \ll 1$. Similarly, $c_2 = (K_2 L)^2$, where $K_2 \ll 1$. It can be noticed that if $c_1 = 0$ and $c_2 = 0$, then SSIM is as QI.

$$\text{SSIM} = \frac{(2\bar{p}\,\bar{q} + c_1)(2\sigma_{xy} + c_2)}{(\bar{p}^2 + \bar{q}^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)} \quad (1.13)$$

By Eq.1.13, SSIM can be computed for an 8×8 block of pixels. Then we can compute the mean SSIM (MSSIM) using Eq.1.14, where n is the entire blocks.

$$\text{MSSIM} = \frac{1}{n} \sum_{i=1}^{n} \text{SSIM}_i \quad (1.14)$$

Kullback–Leibler divergence **(**KLD) is a statistical measure to compute the difference between the SI and the OI. "If h_1 is for histogram of OI and h_2 is for histogram of SI, then one can declare d_1, K-L divergence (KLD) from h_1 to h_2 plying Eq.1.15" [14]. Similarly, we can declare d_2, the KLD from h_2 to h_1 plying Eq.1.16. Then the mean KLD, $D_{KL} = \frac{(d_1 + d_2)}{2}$. The d_1 and d_2 values are 0 if the SI and OI are entirely alike.

$$d_1 = \sum_{i=0}^{255} h_1(i) \times \log \frac{h1(i)}{h2(i)} \quad (1.15)$$

$$d_2 = \sum_{i=0}^{255} h_2(i) \times \log \frac{h2(i)}{h1(i)} \quad (1.16)$$

Manhattan distance, D_m and Euclidian distance, E_m [15] between h_1 and h_2 can be estimated using Eq.1.17 and Eq.1.18 respectively.

$$D_m(h_1, h_2) = \sum_{i=0}^{255} |h_1(i) - h_2(i)| \qquad (1.17)$$

$$E_m(h_1, h_2) = \sqrt{\sum_{i=0}^{255} (h_1(i) - h_2(i))^2} \qquad (1.18)$$

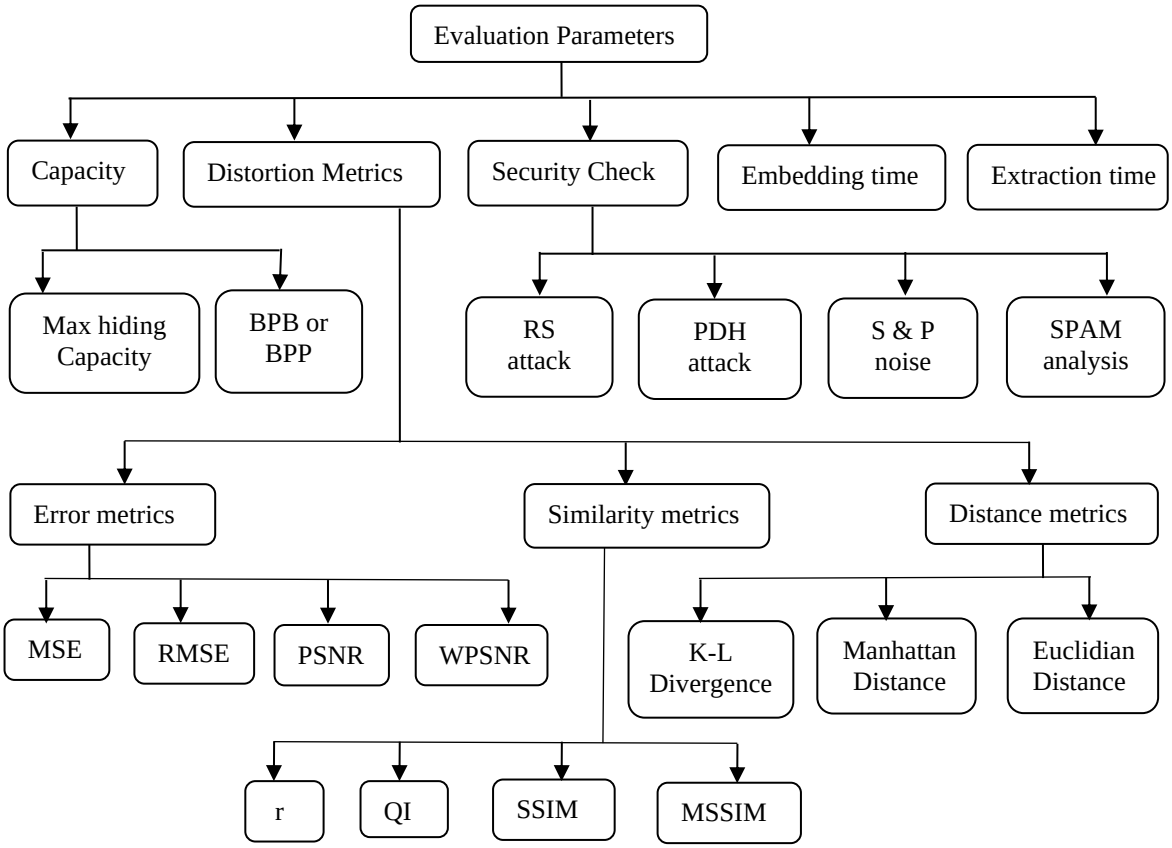


Fig.1.5 Evaluation parameters

There are a good number of steganalysis techniques to detect the SIs. Regular-Singular (RS) analysis is the one, which can detect the SI, if LSB substitution is applied in it. Pixel difference histogram (PDH) is the one to detect the SI, if PVD is applied on it. If we design a technique using both LSB and PVD, the it should be protected from both RS and PDH tests.

There are numerous applications of image steganography described in literature [16, 17, 18, 19, 114].

1.4 The Research Issues and Objectives

This research focusses on 3 problems, (i) fall off boundary problem (FOBP) in recent PVD based techniques, (ii) HC of adaptive PVD (APVD) techniques are low due to unused block problem (UBP), and (iii) PDH analysis does not detect multi-directional PVD techniques. To address these three problems, we propose three new works as stated below.

Objective 1: To propose an improved steganography technique combining quotient value differencing (QVD), and pixel value correlation (PVC), as a result FOBP can be avoided.

Objective 2: To devise a steganography scheme introducing on remainder replacement (RR), adaptive QVD (AQVD), and quotient value correlation (QVC), so a trade-off between HC and PSNR can be done.

Objective 3: To develop a multi-directional PDH (MDPDH) mechanism for detecting multi-directional PVD (MDPVD) techniques.

This first objective brings a new steganography scheme using two principles, (i) QVD, and (ii) PVC. It does not suffer from FOBP unlike many steganography techniques that use the principle of PVD. It performs 2 stages of camouflaging in 3×3 blocks. During the 1st stage of camouflaging procedure QVD and RR is performed on 5 pixels (central pixel, upper, right, lower, and left positions). Basing on these altered 5-pixel values, PVC camouflaging is plied on the other (4 corner) pixels. Hence performance is improved. The data camouflaging capacity is very high with acceptable level of distortion. Security check has been performed using RS and PDH analyses. It has been justified from the results that PDH plots of the SIs could not show any irregular shape. In other words, PDH test did not detect the SI. Furthermore, it is also justified in the RS curves that the regular-singular conditions like "$R_m \approx R_{-m} > S_m \approx S_{-m}$" is met, it means that RS test could not break this steganography technique.

The second objective brings a new steganography technique based on RR, AQVD, and QVC. It performs embedding and extraction operation on 3×3 blocks. It possesses two advantages, (i) avoids UBP and (ii) makes a tradeoff between HC and PSNR. From the 3×3 block 2 additional blocks are spawned, remainder block (RB), and quotient block (QB). Every remainder value in RB is equivalent of decimal value of 2 binary bits, and it is to be replaced by 2 secret bits' decimal equivalent. Each quotient in QB is analogous to 6 bits. The AQVD logic is applied to camouflage bits in 4 corner quotients of the QB. The quotients in bottom and top middle are used as focal values of AQVD logic. QVC logic is plied in center, middle (left and right) quotients to hide the data with relation to their bottom and top neighbors. The results justify that there is a fair balance between PSNR and HC. Obtained improved PSNR and HC values. Also, RS and PDH tests are not successful to detect the SI.

The third objective brings a MDPDH technique which can detect MDPVD steganography. This MDPDH scheme exploits 1-direction, 2-direction, 3-direction, 5-direction, and 8-directions in blocks of size 2, 3, 4, 6, and 8 accordingly. This MDPDH scheme comprises 5 algorithms altogether. The results justify that the MDPDH scheme is able to detect MDPVD steganography.

1.5 Thesis Organization

There are 6 Chapters of this Thesis. The Chapter 1 is an introductory one. The Chapter 2 is a Literature study. Chapters 3 to 5 are the proposed works. Chapter 6 is the conclusion.

- Chapter 3 discusses about the proposed QVD+PVC technique which avoids FOBP.
- Chapter 4 discusses the proposed hybrid technique using RR, AQVD, and QVC to avoid UBP and to establish a trade-off between HC and PSNR.
- Chapter 5 discusses about the proposed MDPDH steganalysis scheme which detects the MDPVD techniques.