CHAPTER 1
INTRODUCTION

1.1 OVERVIEW OF SECURE DATA TRANSMISSION

As of now web and digital media are getting more prominence and the utilization of PCs is incrementing quickly. Digital information can be stored proficiently and with a high caliber, it can be controlled effectively utilizing PCs. Moreover, digital information can be transmitted in a quick and economical route through information correspondence systems without losing quality. Digital media offer a few unmistakable, favorable circumstances under analog media. The nature of digital sound, image and video signals are superior to anything that of their simple partners. Altering is simple in light of the fact that one can get to the precise discrete areas that should be altered. Replicating is effortless without loss of devotion and a duplicate of a digital media is indistinguishable to the original. With Digital media circulation over the World Wide Web, Intellectual Property Right (IPR) is more undermined than any other time in recent memory because of the likelihood of boundless duplication.

Human lives depend on a number of aspects of internet, processors, communication systems (cell phones, e-mails and texting), administration (voter records, social safety, tax records, municipal and metro records), medical (scanning reports, digital BP machines, EEG and ECG), transportation (roadways, railways and airways), finance (e-payments, online banking, loans, checks) and education ( online classes, research, progress reports, attendance messages).

The personal data or information stored on our personal computer or in other’s computer has poor security with a high chance of hacking the data when it is connected to a network. In this scenario, think about the security of information or data residing in the system.

The hackers and malware make the information transmission complex. So the necessity of secure transmission of information likewise expanded. Many algorithms were introduced to transfer information or data in a manner that the occurrence of the message is obscure keeping in mind, the end goal is to discard consideration of the potential hackers (Nagesh et al., 2013). Further concealing data or information for privacy, this methodology of the information stowing away can be stretched out to copyright insurance for digital media.
1.2 STEGANOGRAPHY Vs DIGITAL WATERMARKING

Recently, information or data hiding is rapidly developed algorithm that plays a pivotal role in the discipline of digital security and established a major concentration in both academia and industry. It consists of two faces, such as

1. Digital watermarking
2. Steganography

In the past, Digital Watermarking is used primarily for authentication of products. While steganography is a way of secret communication, the essential reason is to transfer data covertly by obscure the existence of communication (Cox et. al, 2007).

Modern steganography is widely utilized in the platform of digital communications for the detection and encoding of secret information. Steganographic algorithms cover the message by embedding it into another electronic media, thus creates its finding extremely complicated to potential investigations. Steganography implies that the data to be transmitted is invisible to the naked eye (Neeta et al., 2006). The pivotal role of steganography was recently reconsidered by governments with respect to Internet security.

Watermarking is a technique of embedding a message on a host signal. The watermarking is utilized to embed a unique symbol such as the autograph, logo of the trademark or institutes into host signals to identify the owner of the signals. Watermarking is distillate to get high robustness against attacks and it ensures whether the information extracted was successfully completed or not. It has more robustness than the steganography against possible attacks. It can be either visible or invisible. There are many digital watermarking algorithms that are used to embed the copyright data or message into the multimedia data. Information such as serial number, text or pictures can be embedded. The purpose of this information is to provide the copyright security, covert communication, authenticity to differentiate the various data files and so on.

On the other hand, digital watermarking is straightened to verification of digital information and intellectual property right protection. Similar to steganographic algorithms, digital watermarking techniques mask the data in digital media. The variation consists in the determination of the hidden information; it affects the digital medium itself and holds the information about the owner, its consumer, the principle of the content, etc. Digital watermarking has an advantage of inexpensive and quick tracking of information over the free channel. They provide novel ways of ensuring the adequate security of copyright holders in the intellectual property distribution process.
1.3 STEGANOGRAPHY Vs CRYPTOGRAPHY

In general, the principle of both cryptography and steganography methods is to afford cover communication. Cryptography hides or masks the content of secret information, so the secret information cannot be read by malevolent persons. Steganography hides the presence of the message so no one can notice it.

Steganography is different to cryptography; Cryptography transforms the message from plain text to chipper text to formulate it in incomprehensible to malevolent people. In cryptography, once the secret message is read by the malevolent person the system will break. Table 1.1 depicted the comparisons between Steganography and Cryptography.

<table>
<thead>
<tr>
<th>S.No.</th>
<th>Steganography</th>
<th>Cryptography</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Message passing is obscure.</td>
<td>Message passing is renowned.</td>
</tr>
<tr>
<td>2</td>
<td>Modest technology.</td>
<td>Commonly used technology.</td>
</tr>
<tr>
<td>3</td>
<td>Hides the message in another medium so nobody will notice it.</td>
<td>Converts Plain text to chipper text.</td>
</tr>
<tr>
<td>4</td>
<td>The end results in steganography hiding are the stego-media.</td>
<td>The end result is the encryption text.</td>
</tr>
<tr>
<td>5</td>
<td>Can be used in combination with cryptography for encrypting the data before hiding.</td>
<td>Steganography cannot be used.</td>
</tr>
</tbody>
</table>

1.4 SIGNIFICANCE OF THE RESEARCH WORK

The significance of the research work is that the proposed algorithm is highly suitable for multimedia files. Internet extensive ability, Smartphones, Smart devices, Advent of social media like Facebook, YouTube and Twitter made this research work more significant in these areas.

The Significance of information hiding is:

- **Personal and private information**

To convey individual information and private information through a medium it ought to be sheltered and outsider more current envision it. Further, the approved clients can access the information.
• **Confidential data and trade secrets**
  In the military, the data which has to be transmitted should be confidential and whereas the company trade secrets should be hidden otherwise it will lead to a great loss.

• **Sensitive information**
  Sensitive information incorporates a wide variety of information and can include your ethnic or racial birthplace, participation, religious or other comparative convictions, political feeling, physical or psychological wellness points of interest, individual life, or illegal offenses. These data are ensured by our civil authorities.

• **To avoid misuse of data**
  Hiding information also provides the authentication, if anyone misuses the data, we can claim against them.

• **Unintentional damage to data, human error and accidental deletion of data**
  Securing data means keeping data safe from accidental damage or malicious damage.

• **Consequences of accidental and malicious damage to information systems.**
  Associations can endure misfortunes of cash, merchandise or data through cyber crime and negligence. Utilizing an organization's IT framework, installments could be occupied deceitfully into false records; merchandise could be conveyed to an unapproved destination; documents or databases could be abused or duplicated and sold, and vandalism could crush or degenerate information.

• **Monetary and extortion purposes.**
• **To shroud hints of wrongdoing.**
• **Lastly, for fun.**

### 1.5 BACKGROUND OF PROBLEM
Steganography became more crucial as more people entered into cyberspace revolution. It is an art of concealing data. The main aim of steganography is to avert doubtful about the existence of covert information. This data hiding technique has become significant in several applications. Digital images, audio, and digital video are increasingly furnished with distinguishing but unnoticeable marks, which may contain a
hidden or masked copyright notice to avoid illegal copying. Military communication system makes utilization more of the traffic security process. These algorithms are used in cell phones and patterns proposed for digital elections.

It is not possible to maximize imperceptibility, capacity and robustness, simultaneously in any data hiding scheme. Therefore, the bearable balance of parameters is struck based on the particular application. Figure 1.1 depicts the relationship between the characteristics of steganography. It shows that if we want to embed high payload/capacity then, either imperceptibility may be lost or the stego-system may not remain robust to common statistical attacks or the message may become detectable by the eavesdropper. Information hiding techniques can be classified based upon the choice of the cover media used and the domain in which the information is hidden. Here, three types of media are used to hide information namely Video, Image, and Audio. The secret messages are Image, Audio or Text/Microsoft word documents.

![Figure 1.1: Tradeoff among security, robustness and undetectability, payload and imperceptibility.](image)

1.6 MOTIVATION

Nowadays there is a large scope to develop more data hiding techniques for information embedding and retrieval with high privacy and security. The security is a pivotal issue to avoid extraction of concealed data by an unknown person. Steganography is a technique of embedding information for secret communication. The steganography plays a significant role in image processing, signal processing, video processing, and covert systems. Existing algorithms of steganography concentrate on the policy of
embedding and more notice to encryption, which depends on familiar encryption algorithms. These methods aren’t appropriate to steganography applications where flexibility robustness and safety are essentially required. The critical explanation behind choosing steganography was because of the freshness of the phrase that twigged an eagerness for the topic.

Nowadays, the usage of internet and social media is increasing rapidly. Transmitting and sharing the data becoming easier through free channels. Secure data transmission is more essential. The way of providing security to message in transmission motivates me to do the research.

Another motivation factor to select it is because of its wide range of applications. Applications of the data-hiding process include image tamper proofing, verification, in-band captioning, embedded control, secret communication, verification, and revision tracking etc. A gadgets organization in America was arranging the user arrival of its new mobile phone. Meanwhile, an opponent organization in Taiwan built up the mobile and propelled the definite form much before the American organization. Later it worked out that a representative of the American organization transferred a music record — Michael Jackson's "Thriller" — to an online document sharing website. Inside the music, the record has shrouded the schematics of the new mobile. The Taiwanese partner downloaded it within minutes of it being transferred.

Another inspiration for examining the subject was in the wake of perusing an online article in the USA Today titled "Tertionror groups hide behind Web encrypt" that claims terrorists and, specifically, Osama Bin Laden and the al-Qaida system, maybe using steganography to speak with other in arranging terrorist attacks. It is believed that images with masked messages are put on notice sheets or dead drops for distinct terrorists to get and recover concealed messages. So far, this idea has yet to be demonstrated.

1.6.1 why is it interesting for the third party

There are several uses in Steganography, and there are some programmes to make it easier to use. Some of the ways in which companies could benefit from the exact use of this Steganography concept are discussed below.

Email has turned into indispensable to the corporate world, and as a result of that truth, numerous organizations now check all approaching an active email for infections and other things, however, imagine a scenario where you don’t need the email manager to know precisely what is in the email being sent. Passing mystery messages to a customer or colleague in apparently harmless messages is utilization for this craftsmanship.
Numerous organizations have a need to send data to a customer that may sometimes be very sensitive, for example, a sales representative affirming another value or discount that ought not to get to be known by the overall population. Another such utilize would be a CFO sending so far unreleased data to the CEO before a board or stockholder meeting.

Indeed, even the organization site page can be utilized to pass mystery data in a basic way. This may be an arranged thing utilized by your organization or could be an unplanned thing utilized against your organization. This data can be contained in images, audios, videos, or even website page content. Another utilization of steganography is hiding documents and directories on a system network or even on an individual hard drive. Utilization of this expertise can permit an IT individual to make numerous protections on the system or individual drives to encourage recuperation or reconstruct after a debacle.

Copyright security is one of the numerous uses of steganography if your organization distributes a lot of composed material, images, or even music files digitally the chances are that you are as of now intrigued by computerized watermarking, or as it is likewise at times called, digital fingerprinting. At present this type of steganography is genuinely well known for being utilized by numerous extensive enterprises, sadly that likewise makes it helpless against those, who wish to render it futile.

1.7 OBJECTIVES

The ultimate goal of this research work is to develop a multimedia steganography technique that will be efficient in data security and protection applications.

The objectives of the proposed research work can be summarized as follows:

- To design secured and improved steganographic technique that is able to embed a secret message into the multimedia files and also able to extract it.
- To develop a Hybrid algorithm for secure data transmission through multimedia files by combining steganography and cryptography techniques.
- To evaluate measures like PSNR, MSE, SC, embedding capacity, and HER., etc and to compare the performances with the existing techniques.

1.8 SCOPE

The need for hiding or maintaining secrecy arose as the man started communicating. This thesis proposes methods to increase capacity for hiding personal information.
The methods proposed here can be used for hiding personal information in a LAN environment or on computers which are shared among several users. For hiding personal information like Automated Teller Machine (ATM) PIN, Passport details, Income tax details, Income tax returns, Passwords, personal data/letters/photographs, Salary details, confidential data etc, these methods can be easily used. The choice of cover images should be such that they may not raise suspicions like God, Goddess, or personal photographs, pets, flowers, etc.

1.9 METHODOLOGY

The methodology of research work is

i) Literature Survey

Different techniques related to steganography such as audio, image, and video steganography are reviewed in spatial and transform domain.

ii) Implementation of existing algorithms

Most of the people have done research on image steganography because images are most widely used medium and are made up of pixels. The existing algorithms related to image steganography are implemented and applied on image datasets collected from the public domain on the internet to calculate the performance of the existing techniques.

iii) Design of Steganography algorithm using Polynomial equations and HLSB Method

Design a steganography algorithm for data transmission using polynomial equations and Hash-based Least Significant Bit. Here polynomial equations are used as Stego key to embedding the secret information throughout the host medium. Hash-based Least Significant Bit increases the payload of secret information. The results are compared with existing methods.

iv) Development of a stegno-crypto model

To increase the security of the secret information; steganography is combined with cryptography techniques. Here, before embedding the secret information into the host medium it is encrypted with transpose method and linear block codes.

v) Evaluation of the Steganographic methods

The evaluation measures to examine the performance of the proposed algorithms is done by using several dependent variables such as PSNR-Peak Signal to Noise Ratio, Mean Square Error, Structural Content, time computation, payload size etc. A comparative study of the proposed algorithms is performed.
1.10 RESEARCH CONTRIBUTIONS

Keeping in mind the requirements of high imperceptibility of stego-image, high embedding capacity and undetectability of steganography scheme, we embark upon the task of combining cryptography and steganography. The emphasis of current research has been focused more on developing Hybrid hiding method.

The contribution of the research is

- For increasing capacity and security, the existing LSB based steganography is enhanced by performing double encryption of the secret message before embedding.
- A hybrid method is developed that can override statistical and structural measures of detection by spreading message bits randomly. One of the main characteristics of this steganographic technique is that the data are embedded randomly in the cover object using polynomial as a secret key.

1.11 THESIS OUTLINE

This dissertation contains six chapters.

Chapter 1 provides an introduction to the thesis. It contains an overview of secure data transmission and its comparison, the significance of research work, and background of the problem, motivation, scope, objective of the work, methodology and research contribution.

Chapter 2 explores the literature survey. It contains an overview of various techniques in steganography such as image steganography, audio steganography, and video steganography.

Chapter 3 uncovers the general steganography system, characteristics of the data hiding method such as capacity, imperceptibility, security, etc. In this chapter classification and different carriers, performance measurement tools of steganography are discussed.

In chapter 4 the proposed methods of secure data transmission such as DPE, DPHLSB, and DDPHLSB explained for embedding and extraction phase to different cover objects such as image, audio and video files using polynomial equations, hash method, LSB and double encryption.

Chapter 5 presents the simulation results of the proposed method to the different cover object. Text, image, and audio were chosen as secret data. The performance
analysis of a proposed method for different secret data is evaluated to different cover object and compared with existing methods.

Chapter 6 conveys the conclusion that the proposed method has a larger embedding capacity with high imperceptibility and more security than existing methods.