INTRODUCTION

1.1 Concepts

With the advent of high speed communication networks, the Internet acts as a proficient and cost effective information sharing vehicle that makes the globe at large appear like a small digital city. Due to its speed, simplicity and security, digital communication has become an integral part of everyone’s life. In today's ultra-busy society, it is very important to be mindful of the demands on people's time. Ubiquitous Networks and the sudden bloom in cloud computing technologies creates opportunities for individuals and organizations, to share, transmit, and store large amounts of data, images, audios and videos. This information is vulnerable to unauthorized access and interception, while in storage or transmission; thus providing security for this information in all its forms is a challenging issue.

The goal of any communication is to get your message across to the receiver’s clearly, unambiguously and secretly, if desired. This involves effort from both, the sender of the message and the receiver. It’s a process that can be fraught with error, with messages often misinterpreted by the recipient. A miscommunication can result in tremendous confusion, wasted effort and missed opportunity. It is a fact that communication is said to be successful only when both the sender and the receiver understand the same information as a result of the communication. Communication barriers can pop-up at every stage of the communication process (which consists of sender, message, channel, receiver, feedback and context) and have the potential to create misunderstanding and confusion. The communication process diagram has been beautifully explained in “The Mathematical Theory of Communication,” Copyright 1949, by the Board of Trustees of the University of Illinois and is shown below in figure 1.1.
Figure 1.1: The Communication process diagram

Messages are conveyed through channels. Different channels have different strengths and weaknesses. Wikipedia defines a communication channel as a physical transmission medium such as a wire, or a logical connection over a multiplexed medium such as a radio channel. A channel is used to convey an information signal, for example, a digital bit stream from one or several senders (or transmitters) to one or several receivers. A channel has a certain capacity for transmitting information, often measured by its bandwidth in Hz or its data rate in bits per second.

*Covert communication* often refers to the process of communicating data through a channel that is neither designed, nor intended to transfer information (*Lampson, 1973*). It is a channel that can be exploited by a process, to transfer information in a manner that violates the systems security policy. The primary use of covert channels was to allow information transfer by exploiting weaknesses in conventional communication systems like network protocols. *Covert channels* or the so called subliminal channels are studied as part of the science called steganography and the different steganographic methods used in telecommunication networks are referred to as network steganography. An *overt*
channel is a communication channel within a computer network, designed for the authorized transfer of data.

Information hiding (or data hiding) is a general term encompassing a wide range of problems beyond that of embedding messages in content. The term hiding here can refer to either making the information imperceptible (as in watermarking) or keeping the existence of the information secret. Systems for inserting messages in carriers (covers) can thus be divided into watermarking systems; in which the message is related to the cover work, and non-watermarking systems; in which the message is unrelated to the cover work. They can also be independently divided into steganographic systems, in which the very existence of the message is kept secret, and non-steganographic systems, in which the existence of the message need not be secret (Cox et al., 2007).

The tremendous growth in technology has seen more and more of people join the cyberspace revolution. Information sharing and transfer over overt channels has increased exponentially and this makes data security an inevitable task. The secrecy of digital information sent across an open communication channel like the internet is always questionable. In this digital age, it is very important to keep public information public, secret information secret, private information private and protect the copyrights of data. The need for secret communications is as old as the communication itself. To accomplish this task, new methods based on the principle of image processing are being developed and used. To protect important data from being illegally accessed, we can either encrypt it so as to make it available in a gibberish form or we can merely hide its presence. However, the encrypted data exists in a meaningless form and may attract the attention of interceptors (Schneier, 2007). Encryption or the science of cryptography only prevents adversaries from decoding the communication. Sometimes, the mere
existence of communication or even changes in communication patterns, such as an increased message frequency are enough to raise suspicion and reveal the onset of events. Steganography is the art and science of writing secret data in such a way, that no one, except the intended recipient, knows of the existence of the data (Marvel, 1999). It refers to the art of hiding and transmitting data through apparently innocuous carriers, in an effort to conceal the existence of the data. The goal of steganography, is to avoid arousing suspicion to the transmission of a hidden message. Steganography attempts to hide the very existence of communication. Steganography and cryptography are cousins in the spycraft family (Cox et al., 2007). Successful steganography depends upon the carrier medium not attracting attention. When the presence of stego-content is suspected, the main goal of steganography is defeated (Arjun and Negi, 2006). The advantage of steganography over cryptography is that the information cannot be suspected and it protects both, messages and communicating parties. Steganographic data can be embedded in a document file, image file, audio or video file. The content used to embed information is called as carrier or cover object. The cover along with the hidden sensitive information is called as stego-object (Hemalatha et al., 2012).

Given the high degree of redundancy present in a digital representation of multimedia content, there has been an increased interest in using multimedia content for the purpose of Steganography (Radhakrishnan et al., 2005). The goal of every steganographic algorithm is to embed data into a carrier format without altering too much of the original information. By maintaining most of the format’s original information, the resulting steganographic carrier has imperceptible changes for both human and computerized analysis. The strength of a steganographic algorithm is measured as being the degree of resistance against reverse engineering and detection methods (Mare et al., 2011).
There is a visual requirement model which is called *magic triangle* (Duric and Jajodia, 2001) in the field of information hiding, given in Figure 1.2. Imperceptibility, robustness to attacks, and the insertion capacity are in the corners of the magic triangle. This model is convenient for a visual representation of the required trade-offs between the capacity of the embedded data and the robustness to certain attacks, while keeping the perceptual quality of the stego-medium at an acceptable level. It is not possible to attain high robustness to signal modifications and high insertion capacity at the same time (Zhang and Tang, 2007).

![Figure 1.2 Magic triangle representing characteristics of Steganography](image)

The fundamental differences between steganography and watermarking have been well elaborated by Peticolas et al., (1999). The information hidden by a watermarking system is always related to the digital object to be protected or to its owner, while steganographic systems hide any information. They also differ in the robustness criteria...
wherein watermarking concerns potential removal by an adversary while steganography is concerned with the detection of the hidden data. Steganographic communications are usually point to point, while watermarking techniques are usually one towards many.

Steganalysis is the art of detecting the existence of hidden information. Steganology refers to the science of steganography and steganalysis put together. Interest in steganology increased significantly after the terrorist attacks on September 11, 2001, when it became clear that means for concealing the communication itself was likely to be used for criminal activities. Interestingly, USA Today reported on this possibility several months before the September 11, 2001 attack (Cox et al., 2007). However, there has been little evidence to substantiate these claims.

1.2 Classification of Covert Communication Techniques

Covert or Secure communication has become a major challenge in the present digital world. People are continuously striving to develop innovative methods, to aid secure and secret communication. Figure 1.3 describes the various embodiment disciplines of information hiding (Cheddad et al., 2010; Mathew, 2010). The bold face in the figure indicates the focus area in this research work.
1.3 History of Steganography

The word *steganography* was invented by Trithemius; an author of one of the early publications on cryptography. This term is derived from the Greek words *steganos*, which means “covered,” and *graphia*, which means “writing.” Steganography is the art of concealed communication. The very existence of hidden information is secretive. The first instance where steganography was being used to send messages, dates back decades ago, where *(Herodotus, 1992)* reported of a slave sent by his master, Histiaeus, to a city of Miletus with a secret message tattooed on his scalp. After tattooing, the slave was made to re-grow his hair in order to hide the message. He then journeyed to Miletus and, upon arriving, shaved his head to reveal the message to the city’s regent, Aristagoras. The message was to initiate a revolt against the Persian king. Herodotus narrates yet
another story of Demeratus, who scraped the wax off the surface of a wooden writing
tablet and scribbled his warning about the planned invasion of Greece by the Persian
Great King Xerxes into the wood. The tablet was then coated with a fresh layer of wax,
to appear as a blank writing tablet that was safely carried to Sparta without arousing
suspicion.

Aeneas too reported many data hiding methods, such as hiding messages in messenger’s
soles or women’s earrings or messages carried by pigeons. He also proposed several
methods for hiding within text by modifying the height of letter strokes or marking
letters in a text using small holes (Tacticius, 1990). In the later years, invisible inks too
have been used in the science of information hiding.

Acrostic or Linguistic steganography was one of the most noted ancient steganographic
methods. Secret messages were encoded as initial letters of words or sentences or
successive tercets in a poem. One of the most renowned works is Amorosa visione by
Giovanni Boccacio wherein the initial of the successive tercets correspond exactly to the
letters of the sonnets. Hypnerotomachia Poliphili, a puzzling and enigmatic book
(Anonymous, 1499), unveiling the guilty love between a monk and a woman was
another popular example of linguistic steganography. In the sixteenth century, a more
advanced version of acrostic originally formulated in China and reinvented by Cardan,
an Italian mathematician was Cardan’s Grille. Here the alphabets of the secret message
were randomly hidden within text and a mask was then used to read the secret message.
The problem was to securely deliver the mask to the receiver. The Germans and the
Allies are said to have used acrostic as a means of communication during the First World
War. The World War also saw the use of microdots by the Germans for communication. However the Allies discovered the use of microdots in 1941.

Gaspar Schott explained how to hide messages in music scores where each note used to correspond to a single letter. John Wilkins demonstrated how two Musicians may dialogue with one another by playing upon their instruments of music as well as by talking with their instruments of speech (Wilkins et al., 1694). He also explained how messages could be secretly hidden into geometric drawings using points, lines, and triangles. Various techniques have been used in electronic publishing projects to conceal serial numbers and copyright messages in the line spacing and other format features of documents (Brassil et al., 1994). It was found that shifting text lines up or down by one-three-hundredth of an inch to encode zeros and ones, was robust against multi-generation photocopying and could not be noticed by most people. Yet other methods included sending a message to a secret agent by marking certain letters in a newspaper using invisible ink, and adding sub-perceptible echo at certain places in an audio recording (Bender et al., 1996; Peticolas et al., 2000; Cox et al., 2007).

1.4 Applications of Steganography

The emanation of commercial espionage and the growing concerns about security due to terrorism, has intensified the nation’s interest in steganography. In the present digital era, where the entire community, banks on the internet and email for data exchange, steganography has created an atmosphere of corporate surveillance that has spawned various interesting applications. The purpose of steganography is to hide secret data in a carrier. It seeks to provide a covert communication channel between two parties. Digital media such as text files, images, audio, and video files have become the most obvious choices for data carriers. This is due to the fact that such digital media usually includes a
random noise component in which the secret message can be easily hidden (Chanu et al., 2012).

Steganography has several useful applications. However, like any other science, it can also be used with unlawful or illegitimate interests. Civilians may use it for protecting privacy while terrorists may use it for spreading terroristic information, which is potential for endangering our national as well as world security (Korhorn, 2002; Das and Tuithung, 2012). Steganography finds its application in defence related departments, police departments, detective investigation departments, medical imaging (Cheddad et al., 2008). Healthcare industry uses steganography in hiding messages in DNA sequences (Taylor et al., 1999). Anonymous communications, including anonymous remailers and Web proxies (Cheddad et al., 2010) are required by legitimate users to vote privately in online elections, make political claims, preserve online free speech, or to use digital cash. But the same techniques can be abused for defamation, blackmail, or unsolicited commercial mailing. Unobtrusive communications are required by military and intelligence agencies, even if the content is encrypted, the detection of a signal on a modern battlefield may lead rapidly to an attack on the signaller. For this reason, military communications use techniques such as spread spectrum modulation or meteor scatter transmission to make signals hard for the enemy to detect or jam (Peticolas et al., 2000).

This science is also widely used to hide data on the network in case of a breach, in peer-to-peer private communications, in posting sensitive confidential data on the Web to avoid transmission, in embedding corrective audio or image data in case corrosion occurs from a poor connection or transmission, to hide the copyrights information into the image to intact its legality to owner, to hide the descriptive elements of an image such as
name of people in the image, location in a map, or content of the image (Hussain et al., 2010). Individual’s details are also embedded in their photographs in smart IDs and identity cards (Chanu et al., 2012). The use of Steganography also has an important role in strengthening national security. It can also be regarded as secret sharing since messages can be shared secretly without being hacked or corrupted (Korhorn, 2002). Various corporations have also identified the potential of the science of steganography, in communicating trade secrets or new release information. Avoiding communication through well-known channels greatly reduces the risk of information being leaked in transit (Hemalatha et al., 2012). Hiding information in a photograph of the company anniversary celebration is less suspicious than communicating an encrypted file. This gives steganography a positive edge in secret communication.

1.5 Significance of Steganography

Electronic communication is increasingly susceptible to eavesdropping and malicious interventions. Encrypted messages are obvious, and when intercepted, it is clear that the sender and the recipient are communicating secretly. Encryption provides the means to assure the privacy of communications between various parties. If a sufficiently large encryption key is used, then the likelihood of decryption by technical means is negligible, irrespective of the resources available to a hacker. Unfortunately, the very fact that two people are exchanging encrypted messages, indicates that they have something to conceal. Any adversary may therefore decide to obtain the decryption key through forceful or even unlawful means.

Instead of encrypting messages, we can hide them in other innocuous looking objects, so that their very presence is not revealed. Steganography may therefore be a safer form of
communication. Law enforcement and counter intelligence agencies are interested in understanding the science of steganography, so that they are able to detect and trace hidden messages (Anderson and Peticolas, 1998). It is an enormous task for the law enforcement and intelligence agencies to monitor the million phone lines and million broadband connections, deciding which communication to intercept and which one to leave, so as to stop or eliminate the secret communications (Mathew, 2010).

Provos and Honeyman (2001), at the University of Michigan, scrutinized three million images from popular websites looking for any trace of steganography. They did not find any proof of infringement (Cheddad et al., 2010).

1.6 Issues of Concern in Steganography

A steganographer has the privilege to choose a cover medium of his choice. Embedding sensitive information into images freely available on the World Wide Web is not advisable, as a steganalyst might take note and opportunistically have recourse to decoding the stego image. In order to evade any Human Visual Perceptual attack, the generated stego image must not have visual artefacts. Smooth homogeneous areas such as a cloudless grey sky must be avoided; however images with natural redundant noise background and salient rigid edges should be targeted (Cheddad et al., 2008).

In image steganography, improving the capacity of hidden data into cover image, without causing any statistically significant modification is of major concern. There is always a trade-off between amount of secret data that can be hidden, and its perceptibility to attacks. The important issue is how to select the embedding regions or positions in the cover image that result in low distortion of the stego image. The
challenge is to find a way, to camouflage a secret message in an image without perceptible degrading the image quality and to provide better resistance against steganalysis process.

1.7 Research questions

Steganography is being used in order to enable secret communication. Following, are some of the research questions pertaining to the steganography domain:

- How to transfer sensitive data without arousing suspicion of a hacker?
- Is there a manner other than passwords and data encryption to safeguard confidential data?
- Which are the techniques available to transfer confidential data in a manner that it remains confidential?
- Images are often exchanged between people. Can they be used to communicate confidential data?
- What are the benefits and limitations the science of steganography brings to society?
- Can an algorithm be developed that is strong enough to withstand the many unique forms of steganalysis?
- Are the existing algorithms being used for steganography independent of file formats?
- Are terrorists the only ones with steganography tools?
1.8 Objectives of Research

➢ To investigate and analyse the existing methods used for steganography.

➢ Propose a technique for covert (secret) transmission of data with good embedding capacity and high imperceptibility, after noting the research gap analysis.

➢ Test the security/robustness of the proposed technique.