1. INTRODUCTION

The development of Information and Communication Technology (ICT) represents an important part of the society; it draws significant attention towards security and integrity of data. But currently the definition of passing secret data in a traditional way is now changed. ICT leads researchers to develop applications which are used to communicate secretly. There are various technologies which are used for Information hiding such as Steganography, Cryptography and Water marking. These are popular techniques available for information security which is a prime concern while communicating on net. Internet is an open resource for all, so this technology is very much useful to transmit data from one end to other very easily and speedily. Therefore information security draws attention of researchers, government agencies; law makers, military, intelligence agencies as well as criminals who require uninterrupted communications. They are interested in understanding these technologies and their weaknesses, so as to detect and monitor hidden messages. Some governments strictly limit internet free speech and the civilian use of cryptography has made people concerned about independence to develop techniques for unwanted communications on the net, including undesirable hackers and Web proxies.

1.2 DIGITAL IMAGES

Digital Images are electronic snapshots taken of a scene or scanned from documents, such as photographs, manuscripts, printed texts, and artwork. The digital image is sampled and mapped as a grid of dots or picture elements (pixels). Each pixel is assigned a tonal value (black, white, shades of gray or color), which is represented in binary code (zeros and ones). The binary digits ("bits") for each pixel are stored in a sequence by a computer and often reduced to a mathematical representation (compressed). The bits are then interpreted and read by the computer to produce an analog version for display or printing [1].
1. INTRODUCTION

1.2.1 RGB CHANNEL OF DIGITAL IMAGE

Color digital images are made of pixels, and pixels are made of combinations of primary colors. A channel in this context is the grayscale image of the same size as a color image, made of just one of these primary colors. For instance, an image from a standard digital camera will have a red, green and blue channel. A grayscale image has just one channel. In the digital area, there can be any number of conventional primary colors making up an image; a channel in this case is extended to be the grayscale image based on any such conventional primary color. By extension, a channel is any grayscale image of the same size with the proper image, and associated with it. Channel is a conventional term used to refer to a certain component of an image. In reality, any image format can use any algorithm internally to store images.

For instance, GIF images actually refer to the color in each pixel by an index number, which refers to a table where three color components are stored. However, regardless of how a specific format stores the images, discrete color channels can always be determined, as long as a final color image can be rendered. The channels can have multiple widths and ranges.

Figure 1 represents Red, Green and Blue channel of image.

![Red Channel](image1.png) ![Green Channel](image2.png) ![Blue Channel](image3.png)

(a) (b)
1. INTRODUCTION

An RGB image consists of three channels: red, green, and blue. RGB channels roughly follow the color receptors in the human eye, and are used in computer displays and image scanners. If the RGB image is 24-bit (the industry standard as of 2005), each channel has 8 bits, for red, green, and blue, in other words, the image is composed of three images (one for each channel), where each image can store discrete pixels with conventional brightness which intensities between 0 and 255, if the RGB image is 48-bit (very high resolution).

1.3 DIGITAL IMAGE PROCESSING

Digital image processing is the use of computer algorithms to perform image processing on digital images. As a subcategory or field of digital signal processing, digital image processing has many advantages over processing. Many of the techniques of digital image processing, or digital picture processing as it often was called, were developed in the 1960s at the Jet Propulsion Laboratory, Massachusetts Institute of Technology, Bell Laboratories, University of Maryland, and a few other
research facilities, with application to satellite imagery, wire-photo standards conversion, medical imaging, videophone, character recognition, and photograph enhancement.[2] The cost of processing was fairly high, however, with the computing equipment of that era. That changed in the 1970s, when digital image processing proliferated as cheaper computers and dedicated hardware became available. Images then could be processed in real time, for some dedicated problems such as television standards conversion.

As general-purpose computers became faster, they started to take over the role of dedicated hardware for all but the most specialized and computer-intensive operations. With the fast computers and signal processors available in the new millennium, digital image processing has become the most common form of image processing and generally, is used because it is not only the most versatile method, but also the cheapest. Digital image processing technology for medical applications was inducted into the Space Foundation Space Technology Hall of Fame in 1994. [3]

Digital image processing focuses on two major tasks like improvement of pictorial information for human interpretation and processing of image data for storage, transmission and representation for autonomous machine perception. In early 1920s, first application of digital image was used in newspaper industry . Digital image processing is useful in various fields like Image enhancement or restoration, medical applications, law enforcement, digital cinema, image transmission and coding , color processing , remote sensing ,robot vision, hybrid techniques, pattern recognition, registration techniques , multidimensional image processing , image processing architectures and workstations , video processing and high-resolution display.
Figure 2(a) represents the digital image processing applications features:

[Fig 2 (a): Digital Image Processing Features]

1.3.1 Image Enhancement

Image enhancement is the process that improves the quality of the image for a specific application. Digital enhancement is the modification of an image to alter impact on the viewer. Generally, enhancement distorts the original digital values; therefore
enhancement is not done until the restoration processes are completed. Basic methods of digital image enhancement are Spatial Domain Methods; these techniques are based on direct manipulation of pixels in an image whereas another technique is frequency domain methods which are based on modifying the Fourier transformation of the image. Image enhancements edit the visual impact of the image by contrast enhancement, Intensity, density slicing, edge enhancement, making digital mosaics, producing synthetic stereo images.

1.3.1.1 Image De-blurring

Image deblurring is meant to the process of processing the image to make it a better representation of the scene, and is fundamental in making pictures sharp and useful.

1.3.1.2 Image De-noising

Noise reduction is the process of removing noise from an image. Digital images are prone to a variety of types of noises. Which occur due to errors in the image acquisition process that result in pixel values that do not reflect the true intensities of the real scene. There are several types of noise like the image is scanned from a photograph made on film; the film grain itself is a source of noise. Moreover noise can also be the result of damage to the film, or may be introduced by the scanner itself or if the image is acquired directly in a digital format, the mechanism for gathering the data can introduce noise or may be electronic transmission of image data can introduce noise. You may remove noise by using linear, median or adaptive filtering technique.

There are two types of noises that can be present in an image: the first one is random noise and the second is non-random noise. When some strips or lines disturb the image, it is a non-random type of noise. Where as some vital information regarding random pixels is missing as may happen during scanning of a picture which is called random noise.
1.3.2 Image Segmentation

In computer vision, image segmentation is the process of partitioning a digital image into meaningful structure. Image segmentation, is often an essential step in image analysis, object representation, visualization, and many other image processing tasks. The goal of segmentation is to simplify and transform the representation of an image into something that is more meaningful and easier to analyze. [4]

Image segmentation is typically used to locate objects and boundaries (lines, curves) in images. More precisely, image segmentation is the process of assigning a label to every pixel in an image such that pixels with the same label share certain visual characteristics. The result of image segmentation is a set of segments that collectively cover the entire image, or a set of contours extracted from the image (see edge detection). Each of the pixels in a region is similar with respect to some characteristic or computed property, such as color, intensity, or texture. Adjacent regions are significantly different with respect to the same characteristics [5].

1.3.2.1 Threshold Based Segmentation

Histogram thresholding and slicing techniques are used to segment the image. They may be applied directly to an image and at the same time can also be combined with pre and post processing techniques.

1.3.2.2 Edge based segmentation

This technique detects edges in an image which are assumed to represent object boundaries, and is used to identify these objects.

1.3.2.3 Region based segmentation

In an edge based technique we may attempt to find the object boundaries and then locate the object itself by filling them in, while a region based technique takes the opposite approach, by (e.g.) starting in the middle of an object and then “growing”
outward until it meets the object boundaries.

1.3.2.4 Clustering techniques

Although clustering is sometimes used as a synonym for segmentation techniques, we use it here to denote techniques that are primarily used in exploratory data analysis of high-dimensional measurement patterns. In this context, clustering methods attempt to group together the patterns that are similar in some sense. This goal is very similar to what we are attempting to do when we segment an image, and indeed some clustering techniques can readily be applied for image segmentation. Figure 3(a) is an example of Image Segmentation.

![Figure 3(a): Image segmentation](image)

1.3.3 Image Acquisition

Digital Image acquisition in image processing can be broadly defined as the action of retrieving an image from some source, usually a hardware-based source, so it can be passed through whatever processes need to occur afterwards. Performing image acquisition in image processing is always the first step in the workflow sequence because, without an image, no processing is possible. The image that is acquired is completely unprocessed and is the result of the kind of hardware that was used to
generate it, which can be very important in some fields to have a consistent baseline from which to work. One of the ultimate goals of this process is to have a source of input that operates within such controlled and measured guidelines that the same image can, if necessary, be nearly perfectly reproduced under the same conditions. So anomalous factors are easier to locate and eliminate.

1.3.4 Image Registration

Image registration is the process of transforming different sets of data into one coordinate system. Data may be multiple photographs or data from different sensors, times, depths, or viewpoints.[6] It is used in computer vision, medical imaging, military automatic target recognition, and compiling and analyzing images and data from satellites. Registration is necessary in order to be able to compare or integrate the data obtained from these different measurements.

1.3.5 Feature Detection

Feature detection refers to methods that aim at computing abstractions of image information and making local decisions at every image point whether there is an image feature of a given type at that point or not. The resulting features will be subsets of the image domain, often in the form of isolated points, continuous curves or connected regions.

1.3.6 Object Recognition

Object recognition is a process for identifying a specific object in a digital image or video. Object recognition algorithms rely on matching, learning, or pattern recognition algorithms using appearance-based or feature-based techniques. Common techniques include edges, gradients, Histogram of Oriented Gradients (HOG), Haar wavelets, and linear binary patterns. Object recognition is useful in applications such
as video stabilization, automated vehicle parking systems, and cell counting in bio-imaging.

1.4 INFORMATION HIDING AND SECURITY

There are various information hiding techniques like Cryptography, Watermarking and Steganography. These are popular data hiding techniques in digital era. Information hiding is the principle of integration of the design to take decisions in a computer program that are most likely to change, thus protecting other parts of the program from extensive modification if the design decision is changed.

Nowadays so many data are transferred flawlessly on the net so protection of information is a prime requirement to communicate secretly.

Information security means protecting information from unauthorized access. As stated in Department of Economics and social affairs, United Nations [7]. A central challenge is how the new technology can be used not only to increase efficiency for public administration, but also to strengthen confidence in privacy measures by creating mutual transparency between public administration and citizens.

The major aspects of information security are confidentiality, integrity and availability whereof confidentiality refers to preventing the disclosure of information to unauthorized individuals or systems. While, as per Boritz [8], integrity means maintaining and assuring the accuracy and consistency of data over its entire life-cycle and availability is defined as availability of information whenever required. Whereas information hiding systems have three different aspects Capacity, Security, and Robustness [9].Wherein capacity means how much information can be hidden in the cover medium. Security refers to an eavesdropper’s inability to detect hidden information and robustness means the amount of modification the stego medium can withstand before an adversary can destroy hidden information. Information theory enables us to be even more specific on what it means for a system to be perfectly secure.
Figure 4(a) represents various information hiding techniques like cryptography, steganography and watermarking. Whereas Cryptography means converting plaintext to cipher text by using encryption key and decrypt the cipher text to plaintext using decryption key, the key is of two types one is used as secret and other key is public key; Steganography is used to hide image or text within other image to communicate secretly; Watermarking is another information hiding technique its of two types visible and invisible watermarking respectively.

1.4.1 Security Threats

Threats to computers and information systems are highly harmful. Security threats are categorized as follows:

1.4.1.1 Natural Threats
Natural threats are caused by nature like floods, earth quakes, temperature etc. These types of threats are unbearable threats and it is not easy to measure.
1.4.1.2 Intentional Threats

Cyber crimes are the best examples of intentional threats, or when someone purposely damages property or information. These types of threats are a big challenge for e-data as they damage the system very badly.

1.4.1.3 Unintentional Threats

Unintentional threats basically include the unauthorized or accidental modification of software or information. This includes accidentally deleted important file, hardware failure any technical issues or damaging secure information. These threats are a serious matter and continuous logging of system is required.

1.5 VARIOUS METHODS OF INFORMATION HIDING

Steganography, Cryptography and Watermarking are popular information hiding techniques, every technique has its own pros and cons. Researchers are making more and more efforts to find new ways to hide information securely on net.

There are three major information hiding techniques are as follows:

1.5.1 Digital Steganography

The term steganography means to hide the image or text message within another object/Image. Steganography can take data confidentiality to communicate secretly, since it embeds message and pictures within another object by tweaking its properties and it is undetectable by naked eye.

Figure 5, is an example of Digital Steganography where Image 5(a) is an original image, which we call cover or carrier image, image 5(b) is an image to embed within cover image and image 5(c) is an image containing stegogramme. It is been observed
that image containing stegogramme is look alike original image so it is not easy to detect by naked eye that an image is hidden and only intended receiver at the other end can transmit original image or text message.

[Fig.5 (a): Kido Image (Cover/Carrier) (b): Tree Image (Image to Hide) (c): Kido Image (with stegogramme)]

### 1.5.2 Cryptography

Cryptography means the sender converts plaintext to cipher text by using encryption key. On the other side receiver decrypts cipher text to plain text by using decryption Key. The idea is to change the text in to format which is not easy to decrypt without decryption key, changing the alphabets with other alphabets or making a key to arrange the alphabets. Substitution ciphers, Transposition ciphers and RSA are well known techniques of cryptography.

Cryptography is the science of writing in secret code and is an ancient art; the first documented use of cryptography in writing dates falls back to circa 1900 B.C. when an Egyptian scribe used non-standard hieroglyphs in an inscription.

A study of techniques for secure communication in the presence of third parties called adversaries [10] more generally, it is about constructing and analyzing protocols that overcome the influence of adversaries [11] and which are
related to various aspects in information security like data confidentiality, data integrity and authentication [12].

Cryptography prior to the modern age was effectively synonymous with encryption, the conversion of information from a readable state to apparent nonsense. The producer of an encrypted message shared the decoding technique needed to recover the original information only with intended recipients. Since World War I and the advent of the computer, the methods used to carry out cryptology have become more and more complicated and its application more widespread.

Modern cryptography is heavily based on mathematical theory and computer science practice wherein cryptographic algorithms are designed around computational hardness assumptions, making such algorithms hard to break in practice by any adversary. It is theoretically possible to break such a system but it is infeasible to do so by any known practical means. These schemes are therefore termed computationally secure.

Some experts argue that cryptography appeared automatically sometime after writing was invented, with applications ranging from diplomatic missives to war time battle plans. It is no surprise, then, that new forms of cryptography came soon after the widespread development of computer communications.

In data and telecommunications, cryptography is necessary while communicating over any untrusted medium, which includes just about any network, particularly the Internet.

In Figure 6(a), A is a sender who covert plaintext to cipher text by using encryption key at the other end B (Receiver) get the cipher text and by using decryption key convert to actual message(plaintext).
1.5.2.1 Cryptography Types

There are two main types of cryptography:
(i) Secret key cryptography
(ii) Public key cryptography

In cryptographic systems, the key is used to encrypt and decrypt information. The key term refers to a numerical value used by an algorithm to alter information, making that information secure and visible only to those individuals who are having the corresponding key to recover the information.

Secret key cryptography is also known as symmetric key cryptography. With this type of cryptography, both the sender and the receiver know the same secret code, called the key. Messages are encrypted by the sender using the key and decrypted by the receiver using the same key. This method works well if your communication zone is limited. But it becomes impracticable to exchange secret keys with a large community. In addition, there is also the issue as to how you communicate the secret key securely.
Public key cryptography, also called asymmetric encryption, uses a pair of keys for encryption and decryption. With public key cryptography, keys work in pairs of matched public and private keys. The public key can be freely distributed without compromising the private key, which must be kept secret by its owner. Since these keys work only as a pair; encryption initiated with the public key can be decrypted only with the corresponding private key.

In 1883, Auguste Kerckhofs [13] enunciated the first principles of cryptographic engineering, in which he recommends that we assume that method used to encipher data is known to the opponent, so security must lie only in the choice of key.

Cryptology related technology has created a number of legal issues. In the United Kingdom, additions to the Regulation of Investigatory Powers Act 2000 required a suspected criminal to hand over his or her decryption key if asked by law enforcement. Otherwise the user will face a criminal charge [14]. The Electronic (EFF) was involved in a case in the United States which questioned whether requiring suspected criminals to provide their decryption keys to law enforcement is unconstitutional. The EFF argued that this is a violation of the right of not being forced to incriminate oneself, as given in the fifth Amendment [15]. Cryptography are used in applications like e-commerce, ATM Cards and Computer Passwords.

1.5.3 Digital Watermarking

The term "digital watermark" was first coined in 1992 by Andrew Tirkel and Charles Osboarne [16].

A digital watermark deals with a pattern of bits inserted into a digital file image, audio or video. Such messages usually carry copyright information of the file. Digital watermarking takes its name from watermarking of paper or money. But the basic difference between those two is that digital watermarks are supposed to be invisible or
at least not changing the perception of original file, different from paper watermarks, which are supposed to be somewhat visible. Digital watermarking came to be in great demand when sharing information on the internet gained momentum while sharing files online, you never know if someone uses them without your consent. To prevent unauthorized commercial use of your files, you can publish them to the web in the worst quality or else don’t publish anything worthwhile at all. It isn’t a good way to solve the problem of unauthorized use, is it? So, one should look for more effective ways of copyright protection, such as digital watermarking.

Figure 7 is an example of visible watermarking.

![Visible watermark image](image)

Digital image watermarking divides in two main groups, visible and invisible watermarks. A visible watermark is a visible partially transparent text or image overlaid on the original image. It allows the original image to be viewed, but it still provides copyright protection by marking the image as its owner’s property. Visible watermarks are more robust against image transformation (especially if you use a
semi-transparent watermark placed over the whole image). Thus they are preferable for strong copyright protection of intellectual property in digital format.

An invisible watermark means an embedded image which cannot be perceived with naked eyes. Only electronic devices can extract the hidden information to identify the copyright owner. Invisible watermarks are used to mark a specialized digital content (text, images or even audio content) to prove its authenticity.

Although the copyright protection is the main field of using digital watermarks, they can also be used for such purposes as advertising (adding company’s name and logo as a watermark for promotion rather than for protection) or even adding memo titles to digital photos. It’s obvious that only visible watermarks can satisfy these requirements.

A digital watermark is an invisible or visible mark embedded in a digital image which may be used for Copyright Protection. A watermark is a visible embedded overlay on a digital photo consisting of text, a logo, or a copyright notice. The purpose of a watermark is to identify the work and discourage its unauthorized use. Though a visible watermark can't prevent unauthorized use, it makes it more difficult for those who may want to claim someone else's photo or art work as their own.

Digimarc Corporation is pioneered in digital watermarking. They offers a service for embedding digital code into photos and other media that is undetectable during normal use, but enables tracking and identification of the media.

One application of digital watermarking is source tracking. A watermark is embedded into a digital signal at each point of distribution. If a copy of the work is found later, the watermark may be retrieved from the copy and the source of the distribution is becomes traced. This technique reportedly has been used to detect the source of illegally copied movies.

Fourier-Mellin transform-based invariants can be used for digital image watermarking. The embedded marks may be designed to be unaffected by any
combination of rotation, scale and translation or transformations. The original image
is not required for extracting the embedded mark [17].

A novel technique for the digital watermarking of still images is based on the concept
of multi resolution wavelet fusion. The algorithm is robust to a variety of signal
distortions. The original unmarked image is not required for watermark extraction.

Analysis to describe the behavior of the method for varying system parameter values,
approach with another transform domain watermarking method. Simulation results
show the superior performance of the technique and demonstrate its potential for the
robust watermarking of photographic imagery [18].

A digital watermark is a kind of marker covertly embedded in a noise
tolerant signal such as audio or image data. It is typically used to identify ownership
of the copyright of such signal. "Watermarking" is the process of hiding digital
information in a carrier signal; the hidden information should [19] but does not need
to contain a relation to the carrier signal. Digital watermarks may be used to verify the
authenticity or integrity of the carrier signal or to show the identity of its owners. It is
prominently used for tracing copyright infringements and for currency note
authentication.

Like traditional watermarks, digital watermarks are only perceptible under certain
conditions, i.e. after using some algorithm, and imperceptible otherwise. If a digital
watermark distorts the carrier signal in a way that it becomes perceivable, it is of no
use [20]. Traditional Watermarks may be applied to visible media (like images or
video), whereas in digital watermarking, the signal may be audio, pictures, video,
texts or 3D models. A signal may carry different types of watermarks at the same
time. Unlike metadata added to the carrier signal, a digital watermark does not change
the size of the carrier signal. The needed properties of a digital watermark depend on
the use case in which it is applied. For marking media files with copyright
information, a digital watermark has to be rather robust against modifications that can
be applied to the carrier signal. Instead, if integrity has to be ensured, a fragile watermark would be applied.

Steganography and digital watermarking employ steganographic techniques to embed data covertly in noisy signals. Whereas steganography aims at imperceptibility to human senses, digital watermarking tries to control the robustness as top priority. Since a digital copy of data is the same as the original, digital watermarking is a passive protection tool. It just marks data, but neither degrades it nor controls access to the data.

1.5.4 Comparison of Various Information Hiding Techniques
The comparison of various data hiding technique is shown in Table 1.

[Table 1: Comparison of various data hiding techniques]

<table>
<thead>
<tr>
<th></th>
<th>DIGITAL STEGANOGRAPHY</th>
<th>CRYPTOGRAPHY</th>
<th>DIGITAL WATER MARKING</th>
</tr>
</thead>
<tbody>
<tr>
<td>Techniques</td>
<td>LSB, Spatial Domain, Jsteg, Outguess</td>
<td>Transposition, Substitution, RSA</td>
<td>compensated prediction, DCT</td>
</tr>
<tr>
<td>Naked eye Identification</td>
<td>No, as message is hide within other carrier (cover image)</td>
<td>Yes, as message is converted in other way, which seeks something is hidden</td>
<td>Yes, as actual message is hidden by some watermark.</td>
</tr>
<tr>
<td>Capacity</td>
<td>Differs as different Technology usually low hiding capacity</td>
<td>Capacity is so high, but as message is long it chances to be decrypted</td>
<td>Capacity depends on the size of hidden data.</td>
</tr>
<tr>
<td>Detection</td>
<td>Not easy to detect because to find steganographic image is hard.</td>
<td>Not easy to detect, depends on technology used to generate</td>
<td>Not easy to detect</td>
</tr>
</tbody>
</table>
1. INTRODUCTION

<table>
<thead>
<tr>
<th>Strength</th>
<th>Hide message without altering the message, it conceals information</th>
<th>Hide message by altering the message by assigning key</th>
<th>extends information and becomes an attribute of the cover image</th>
</tr>
</thead>
<tbody>
<tr>
<td>Imperceptibility</td>
<td>High</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Robust</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

In above, comparison it is observed that steganography is a best to communicate secretly with security as compare to other two techniques like watermarking and cryptography.

1.6 HISTORY OF INFORMATION HIDING AND STEGANOGRAPHY

1.6.1 Information Hiding

The concept of information hiding was first described by David Parnas. Since the early days of communication, diplomats and military commanders understood that it was necessary to provide some mechanism to protect the confidentiality of correspondence and to have some means of detecting tampering.

Julius Caesar is credited with the invention of the Caesar cipher c. 50 B.C.[21], which was created in order to prevent his secret messages from being read, should a message fall into the wrong hands, but for the most part protection was achieved through the application of procedural handling controls. Sensitive information was marked up to indicate that it should be protected and transported by trusted persons, guarded and stored in a secure environment.

Similarly, the development of ICT leads to protect electronic data processing and electronic business conducted through the Internet, along with numerous occurrences of international terrorism.
1.6.2 Steganography

One of the oldest examples of Steganography is situated as back as around 440 BC in Greek History. Herodotus, a Greek historian from the 5th century BC, revealed some examples of its use in his work entitled “The Histories of Herodotus”. One extensive example suggests that Histaeus, ruler of Miletus, tattooed a secret message on the shaven head of one of his most trusted slaves. After the hair had grown back, the slave was sent to Aristagorus where his hair was shaven and the message that commanded a revolt against the Persians was revealed [22]. Astonishingly the method was still used by some German spies at the beginning of the 20th century [23]. Herodotus also tells how Demeratus, a Greek at the Persian court, warned Sparta of an imminent invasion by Xerxes: he removed the wax from a writing table, wrote his message on the wood underneath and then covered the message with wax. The table looked exactly like a blank one and almost deceived the recipient as well as the customs men.

Gaspar schotti [24], in his book of Steganography, entitled schola steganographica, published in 1665, schotti drew immensely upon the work of Johannes Trithemius (1462-1562), a German Monk and early researcher in steganography and cryptography, steganographic research went on developing in the fifteenth and sixteenth centuries as well.

Bishop John Wilkins, later the master of Trinity college, Cambridge devised a number of steganographic processes ranging from coding messages in sheet music and string knots to invisible inks [25].

A spy is called successive when he is not identified. Messages have to be sent in a steganographic manner using open codes, microdots, hollow heels, invisible inks etc. Spies had to be very clever to evade the censorship bureau which played a big role in the life of ordinary people during the World Wars because all mails were scrutinized.

In 1941 Bermuda had become suspicious of the Joe K letters and had managed to develop secret inks used to write letters used by Ludwig using [26].
Nazi spies [27] employed many measures to frustrate the secret writing tests of the censorship bureau; one was to split a piece of paper, write a secret-ink message on the inner surface, then rejoins the halves. With the ink on the inside no reagent applied to the outside could develop it. The technique was traced when one spy used too much ink and the excess soaked through.

In Jargon code, an apparently innocuous word stands for the real in a text that has been made to look as innocent as possible. Jargon code was used extensively during the World Wars. In 1917 Captain William Hall was head of the cryptanalytic group of the British navy. Their job was to analyze any German cryptographic information captured by the British.

Trebitsch Lincoln was an embittered former member of parliament. He sent a lot of military information to the Germans in jargon code. In one of his jargon systems, family names meant ships or ports; in another, various petroleum products stood for them [28].

During 1980’s British Prime Minister Margaret Thatcher became so irritated at press leaks of cabinet documents that she had the word processors programmed to encode their identity in the word spacing of documents, so that disloyal ministers could be traced [29].

1.7 STEGANALYSIS

Steganalysis means detecting text or images concealed with other image using steganography. The purpose of steganalysis is to identify suspected images and determine whether or not they are concealed with stegogramme and try to recover the original message. Steganalytical schemes are associated with targeted steganalysis, including visual, structural, and statistical attacks.
1.7.1 Attacks

Different types of attacks are described as follows.

1.7.1.1 Visual Attacks

These attacks are widely regarded as the simplest form of steganalysis. As the name suggests, a visual attack largely involves examining the subject file with the naked eye to identify any obvious inconsistencies. Of course, the first rule of steganography is that any modifications made to a file should not face any consequences in quality degradation, so a good steganographic implementation will create stegograms that do not look any more susceptible than the cover work at least not at face value. However, when we remove the parts of the image that were not altered as a result of embedding a message, and instead concentrate on the possible areas of embedding in isolation, it is usually possible to observe signs of manipulation.

1.7.1.2 Structural Attacks

Structural attacks are designed to take advantage of the high-level properties that are known to exist for a particular steganographic algorithm. Structural attacks rarely analyze each image on its own merits. Instead, the images are scanned to see if they contain any of the known side-effects for various steganographic algorithms. Images that contain these properties are often subjected to further investigation. There are sometimes cases where the image may possess symptoms of steganography when it is actually perfectly innocent.

For example, computer generated images are likely to have a different color composition from those of natural life because they are not influenced by the same elements such as light, shadowing, and sampling. Computer generated images may therefore appear structurally similar to what is expected for a stegogramme, but they
do not necessarily contain hidden messages; this is why a more thorough investigation usually follows a structural attack.

1.7.1.3 Statistical Attacks

In mathematics, the study of statistics makes it possible to determine whether some phenomenon occurs at random within a data set [30]. Usually, a theory would be constructed that seemingly explains why the phenomenon occurs, and statistical methods can be used to prove this theory to be either true or false. If we think of the data structure for a stegogramme; we can begin to see how statistics can be useful for steganalysis to proving whether the image contains a hidden message or not. A stegogramme can be broken down into two data sets: image data, and message data. The image data relates to the information regarding the physical image that we can see, and will typically relate to pixel values that point towards the colours used in that region of the image. The message data on the other hand, relates to information regarding the secret message, and if encrypted it is typically more randomly composed than image data. It can safely be derived that the message data is more random than image data, and this is where statistical attacks usually operate. Even as there is usually far less message data than image data, the small percentage of randomness created by the message data is enough to invoke an attack.

There are several methods that are known to prove the existence of a hidden message via statistical approaches; each aimed at identifying signs of embedding for specific stego systems.

1.7.2 BLIND STEG ANALYSIS

There are several methods available for attacking a stegogramme via a targeted approach. In order for these attacks to work effectively however, the steganalyst ideally needs to know how the stegogramme was created such that they can apply the correct attack. Either this or they will need to have access to the original cover image
in order to calculate the expected properties for a clean image, and make a comparison with what is seen for the stegogramme.

As time goes on, more and more stego systems are created, and we cannot be sure how all of them operate. Subsequently, an approach is needed that is capable of identifying the probability of embedding, even when we are not sure how the information might have been embedded. This is known as blind steganalysis.

Blind steganalysis therefore works differently to targeted steganalysis because it assumes that nothing is known about either the algorithm or the cover image that was used to produce a suspect image. The attacks attempt to evaluate the probability of embedding which is based solely on the data of the suspect image. Such approaches are more general in real-world steganalysis because a steganalyst will rarely know much more about an image than what they can extract from the image itself.

One of the earliest blind steganalysis techniques was developed by Nasir Memon [31] who used image quality measures to check the system such that it could classify images according to the probability that they contain message data. The approach projected the score for a large amount of research in neural network steganalysis. Hany Farid [32] also suggested a method based on features extracted from the wavelet (transform) decomposition of the suspect image. His conclusion stated that there are strong high-order statistical regularities within these regions for natural images, and that these regularities are altered as a message is embedded.

1.8 FRACTALS

A fractal is a mathematical set whose patterns are self similar. This means it is "the same from near as from far"[33]. Fractals may be exactly the same at every scale.

Fractals are different from regular geometric figures by their fractal dimensional scaling. Doubling the edge lengths of a square scales its area by four, which are two to the power of two, because a square is two dimensional. Likewise, if the radius of a sphere is doubled, its volume scales by eight, which are two to the
power of three, because a sphere is three-dimensional. A fractal has a fractal dimension that usually exceeds its topological dimension [34] and may fall between the integers [35].

Fractals have attracted widespread interest. Virtually every area of science has been examined from a fractal viewpoint, with fractal geometry becoming a major area of mathematics, both as a subject of interest in its own right and as a tool for a wide range of applications. Fractals have also achieved a popular trend, with attractive, highly coloured, fractal pictures appearing in magazines, books, and art exhibitions, and even used for scenery in science fiction films. Further public interest has been generated with the widespread use of computers at home and at school, enabling anyone with a basic knowledge of programming to generate complicated fractal pictures by repeatedly applying a simple operation.

1.8.1 Techniques for Generating Fractals

Three common techniques for generating fractals are as follows:

1.8.1.1 Iterated Function Systems
These have a fixed geometric replacement rule. Cantor set, Sierpinski carpet, Sierpinski gasket, Hilbert curve, Koch snowflake, Harter-Heighway dragon curve, T-Square, Menger sponge, are some examples of such fractals.

1.8.1.2 Escape Time Fractals
These fractals are defined by a recurrence relation at each point in a space (such as the complex plane).
Examples of this type are the Mandelbrot set, the Burning Ship fractal and the Lyapunov fractal.

1.8.1.3 Random Fractals
Random fractals are generated by stochastic rather than deterministic processes, for Example of this type of fractals are landscapes, Levy flight and the Brownian tree.
1.8.2 Fractals and self-similarity

Fractals can also be categorized according to their self-similarity. There are three types of self-similarity found in fractals.

1.8.2.1 Exact self-similarity

This is the strongest type of self-similarity; the fractal appears identical at different scales. Fractals defined by iterated function systems often display exact self-similarity.

1.8.2.2 Quasi-self-similarity

This is a loose form of self-similarity; the fractal appears approximately (but not exactly) identical at different scales. Quasi-self-similar fractals contain small copies of the entire fractal in distorted and degenerated forms. Fractals defined by recurrence relations are usually quasi-self-similar but not exactly self-similar.

1.8.2.3 Statistical self-similarity

This is the weakest type of self-similarity; the fractal has numerical or statistical measures which are preserved across scales. Most reasonable definitions of "fractal" trivially imply some form of statistical self-similarity. (Fractal dimension itself is a numerical measure which is preserved across scales.) Random fractals are examples of fractals which are statistically self-similar, but neither exactly nor quasi-self-similar.

1.8.3 FRACTAL GEOMETRY

A fractal is a geometric figure or natural object. Its parts have the same form or structure as the whole, except that they are at a different scale and may be slightly
deformed. Its form is extremely irregular or fragmented, and remains so, whatever the scale of examination. It contains "distinct elements" whose scales are very varied and cover a large range. A fractal is a quantity or object which exhibits self similarity on all scales. Fractals are self-similar, meaning thereby that a fractal is exactly or approximately similar to a part of itself. Self-similarity means that each smaller portion can reproduce exactly a larger portion when magnified.

There are many phenomena which, although governed by the basic laws of science, historically regarded as too irregular or complex to be described or analysed using traditional mathematics. Classical geometry concentrated on smooth or regular objects such as circles, ellipses, cubes, or cones.

The calculus, introduced by Newton and Leibniz in the second half of the 17th century, was an ideal tool for analysing smooth objects and rapidly became so central both in mathematics and science that any attempt to consider irregular objects was sidelined. Indeed, many natural phenomena were looked over, perhaps deliberately, because their irregularity and complexity made them difficult to describe in a form that was mathematically manageable.

Figure (8:(a),(b),(c),(d),(e),(f),(g),(h),(i) and (j)) represent different types of fractals like Koch snowflake, Sierpinski, Cantor, Dragon, Landscape, Brownan tree, Lyapunov, Menger Sponge, T-square and Burning Ship respectively.
1. INTRODUCTION

1.9 MANDELBROT FRACTAL

Mandelbrot Fractals were first described by mathematician Benoit Mandelbrot. He was a French and American mathematician, noted for developing a "theory of roughness" in nature and the field of fractal geometry to help prove it, which included coining the word "fractal". He later discovered the Mandelbrot set of intricate, never-ending fractal shapes, named in his honour. [36] He found geometry to be incomplete. It could not describe the enormous and irregular shape of a mountain. It had no formal representation of the appearance of a cloud. The new geometry that he developed could do all this. It was a description of the beautiful yet irregular and fragmented patterns around us. The term ‘Fractal’ was coined by Mandelbrot from the Latin Fractus, an adjective for the irregular and the fragmented. Essentially, they replicate themselves by fragmentation.

Mandelbrot was one of the first to use computer graphics to create and display fractal geometric images, leading to his discovering the Mandelbrot set in 1979. In so doing, he was able to show how visual complexity can be created from simple rules. He said that things typically considered to be "rough", a "mess" or "chaotic", like clouds or shorelines, actually had a "degree of order".[37] His research career included contributions to fields including geology, medicine, cosmology, engineering and the social sciences. Science writer Arthur C. Clarke credits the Mandelbrot set as being "one of the most astonishing discoveries in the entire history of mathematics". [38]

Towards the end of his career, he was excellent Professor of Mathematical Sciences at Yale University, where he was the oldest professor in Yale's history to receive tenure. [39] Mandelbrot also held positions at the Pacific Northwest National Laboratory, University Lille Nord de France, and Institute for Advanced Study and Centre National de la Recherche Scientifique. During his career, he received over 15 honorary doctorates and served on many science journals, along with winning numerous awards. His autobiography, The Fractalist, was published in 2012.
1. INTRODUCTION

Figure 9((a), (b)) is an example of Mandelbrot fractal. If we look at a fractal pattern and we see a form; we look closely at a particular region of the pattern and we will see the same form all over again only much smaller this time. And so on it goes, from the largest scales to the smallest. So, the fractals are the repetition of the same structured form.

![Mandelbrot Fractal](image)

The Mandelbrot set has its place in complex dynamics; a field first investigated by the French mathematicians Pierre Fatou and Gaston Julia at the beginning of the 20th century. The first pictures of this fractal were drawn in 1978 by Robert W. Brooks and Peter Matelski as part of a study of Kleinian groups. [40] On 1 March 1980, at IBM’s Thomas J. Watson Research Center in Yorktown, Heights, New York, Benoit Mandelbrot first saw a visualization of the set. [41]

1.10 HILBERT CURVE

A Hilbert curve (also known as a Hilbert space-filling curve) shown in figure 10(a) is a continuous fractal space-filling curve first described by the German mathematician David Hilbert in 1891, [42] as a variant of the space-filling curves discovered by Giuseppe Peano in 1890. [43] He is recognized as one of the most influential and
universal mathematicians of the 19th and early 20th centuries. Hilbert discovered and developed a broad range of fundamental ideas in many areas, including invariant theory of geometry. He also formulated the theory of Hilbert spaces, [44] one of the foundations of functional analysis.

![Hilbert Curves with ever increasing density](image)

(a)

[Fig 10 (a): Hilbert Curves with ever increasing density [14]]

The mathematical concept of a Hilbert space generalizes the notion of Euclidean space. It extends the methods of vector algebra and calculus from the two-dimensional Euclidean plane and three-dimensional space to spaces with any finite or infinite number of dimensions. A Hilbert space is an abstract vector space possessing the structure of an inner product that allows length and angle to be measured.

Furthermore, Hilbert spaces are complete: there are enough limits in the space to allow the techniques of calculus to be used.

Hilbert spaces arise naturally and frequently in mathematics and physics, typically as infinite-dimensional function spaces. The earliest Hilbert spaces were studied from this point of view in the first decade of the 20th century by David Hilbert, Erhard Schmidt, and Frigyes Riesz. They are indispensable tools in the theories of partial
differential equations, quantum mechanics, Fourier analysis (which includes applications to signal processing and heat transfer theory, which forms the mathematical underpinning of thermodynamics.

John von Neumann coined the term Hilbert space for the abstract concept that underlies many of these diverse applications. The success of Hilbert space methods resulted in a very rich era for functional analysis. Apart from the classical Euclidean spaces, examples of Hilbert spaces include spaces of square-integrable functions, spaces of sequences, Sobolev spaces consisting of generalized functions, and Hardy spaces of holomorphic functions.
1.11 SUMMARY

Steganography is a very useful information hiding technique. The major advantage of using this technique is that the message which was hidden is not easy to detect by naked eye detection. Our research has addressed major aspects of steganography.

In this chapter we have presented an overview of Digital Image Processing as well as different information hiding techniques like Steganography, Cryptography and Digital watermarking. Furthermore, fractals overview is presented as Fractals are used for Digital Image Steganography.
REFERENCES


1969.

Technologies/1994". Space Foundation, each channel is made of 16-bit  


Computing Surveys (CSUR) archive, Volume 24 , Issue 4, Pages: 325 – 376,  

[7] "e-Goverment for the People," Department of Economic and Social Affairs,  


[9] B. Chen and G. Wornel, "Quantization Index Modulation : A Class of  
Provably Good Methods for Digital Watermarking and Information
1. INTRODUCTION


1. INTRODUCTION


1. INTRODUCTION


1. INTRODUCTION


