**EFFICIENT DATA HIDING BY DUAL STEGANOGRAPHY**

**by**

POOJA MAURYA (1901660300037)

Submitted to the Department of Electronics Engineering

in partial fulfillment of the requirements

for the degree of

**BACHELOR OF TECHNOLOGY**

**in**

Electronics Engineering

Logo

Description automatically generated

DR. AMBEDKAR INSTITUTE OF TECHNOLOGY FOR HANDICAPPED, KANPUR

DR A.P.J. ABDUL KALAM TECHNICAL UNIVERSITY

December , 2022

*i*

**ACKNOWLEDGEMENT**

*I would like to place on record my deep sense of gratitude to our project guide* ***Ms****.* ***Prerna Srivastava****, Dept. of Electronics Engineering, Dr. A.I.T.H. Kanpur for her generous guidance, help and useful suggestions.*

*We express our sincere gratitude to* ***Mrs. Shweta Tripathi****, HOD in Department of Electronics Engineering, Dr A.I.T.H. Kanpur, for her stimulating guidance, continuous encouragement and supervision throughout the course of present work.*

*.*

*We are extremely thankful to* ***Prof. Rachna Asthana****, Director, Dr. AITH, Kanpur, for providing me infrastructure facilities to work in, without which this work would not have been possible.*

***ii***

***ABSTRACT***

*In comparison with analog communication, digital communication provides several advantages like better quality, ease of editing, high fidelity, compression, etc. But with rapid growth of World Wide Web and advance computer network, there are some issues related to content security, privacy, and media authentication. In modern age in which data is conveyed through digital medium, the protection of data is top priority concern for any organization. Digital steganography is an advance technique in which secret data can’t be detected easily. Steganography envelopes and information to such degree that it is invisible to a spectator. In this proposed paper the focus is on increasing data security using dual steganography. In dual steganography secret message is first embedded into cover medium and then resulted stegno-object will be again embedded into other cover medium. Mentioned paper also provides a computable evaluation of dual steganography in terms the reduction in the mean square error (MSE) and hence increase in peak signal to noise ratio (PSNR) measure between original host files and generated stenographic files. A preliminary result shows the high imperceptibility of the proposed method as well as the hiding capacity of presented method.*

***Keywords:*** *Dual steganography, Image steganography, LSB, Video steganography, DWT.*

***iii***

**TABLE OF CONTENTS**

|  |  |  |
| --- | --- | --- |
|  | ACKNOWLEDGEMENT…………………….……………………………………..ii  ABSTRACT…………………………………………………………………………...iii LIST OF FIGURES*……………………………………………………………….…iv* |  |
|  | CHAPTER 1: INTRODUCTION…………………………………………………...  1.1 Need of Data Hiding…………………………………………………  1.2 Basic idea of Steganography……………………………………… 1.3 Difference between steganography and cryptography  1.4 Ancient steganography……………………………………………  1.5 Digital Steganography…………………………………………… |  |
|  | CHAPTER 2: DATA HIDING TECHNIQUES…………………………………….  2.1 Image………………………………………………………………………  2.1.1 Pixel…………………………………………………………………  2.1.2 RGB………………………………………………………………..  2.1.3 Gray scale………………………………………………………….  2.2 Digital image data hiding technique………………………………………  2.3 Types of data hiding technique…………………………………………..  2.4 Data hiding………………………………………………………………  2.4.1 Features of applications…………………………………………..  2.4.2 Data Hiding in still images……………………………………….  2.4.3 Security.…………………………………………………………. |  |
|  | CHAPTER 3: STEGANOGRAPHY AND ITS ANALYSIS ………………..…..  3..1 Steganography…………………………………………………………… 3.1.1 Ancient Steganography…………………………………….  3.1.2 Modern Steganography ………………………………  3.1.3 Steganography in practice……………………………………  3.2 Different Techniques…………………………………… |  |
|  | CHAPTER 4: PROPOSED ALGORITHM………………………………………….  4.1 Data insertion stage…………………………………………….   1. 4.2 Data extraction stage……………………………………………. |  |
|  | CHAPTER 5: CONCLUSION ………………………………………22  *References…………………………………………………………………………….* |  |

***v***

**Table of Figures**

|  |  |  |
| --- | --- | --- |
|  | Fig 3.1 Pixel is smallest element of image……………………….......................... |  |
|  | Fig 3.2 a color image is made of 3 matrices……………………........................... |  |
|  | Fig 3.3 A gray scale image……………………………..……….………………… |  |
|  | Fig 3.4 bit black to white gradient……………………….……………………… |  |
|  | Fig 3.5 Block diagram of digital image steganography………..……………….. |  |
|  | Fig 3.6 Data hiding techniques………………………………………………….  Fig 4.1 Steganography ……………………………………………....................... |  |
|  | Fig 4.2 Modern Steganography………………………………………..………… |  |
|  | Fig 4.3 Block Diagram……………………………………………………………. |  |
|  | Fig 4.4 Steganography in practice…………………………………...................... |  |

***vii***

**CHAPTER 1**

**INTRODUCTION**

**1.1 NEED OF DATA HIDING**

Ancient people used various techniques to send secret messages during war times. Sending of massages safely and securely has been top priority for any organization that deals with confidential data. Information hiding techniques are necessary for military, intelligence agencies, internet banking, privacy, etc. so it is on-going research area in present time [1].

Increased use of internet, information become available on-internet, a person who possesses an internet can easily get data from internet for information that they want. As more and more techniques for hiding information are developed and improved, more and more different information detecting techniques are also developed. That has produced a strong need to create new techniques for protecting confidential information from hackers.

**1.2 BASIC IDEA OF STEGANOGRAPHY**

There are numbers of data hiding techniques available for different purpose and applications like steganography, cryptography, and watermarking.

Steganography means covered writing. Cryptography means scrambling of data such that it becomes meaningless to eavesdroppers [3]. Watermarking means embedding of watermark signal into data to generate watermark object [7]. So that it is mostly used in copyright protection and authentication of media. In steganography method confidential data is embedded in such way that the existence of secret data is invisible.

**1.3 DIFFERENCE BETWEEN STEGANOGRAPHY AND CRYPTOGRAPHY**

Steganography is the art of hiding information without the ability for an unauthorized person to detect the presence of information, while in cryptography it is obvious to the public that there is hidden information, but nobody can understand this message apart from the authorized person.

The advantage of steganography over cryptography is that hidden messages do not attract attention in steganography, while encrypted data will arouse suspicion and as a result, someone will always try to break this encrypted message.

## 1.4 ANCIENT STEGANOGRAPHY

The word steganography is of Greek origin, from the two words *stegano* meaning “covered or protected”, and *graphing* meaning “to write”*,* so the word means “concealed writing”.

The first recorded uses of steganography can be traced back to 440 BC when [Herodotus](http://en.wikipedia.org/wiki/Herodotus) mentions two examples of steganography in [The Histories of Herodotus](http://en.wikipedia.org/wiki/The_Histories_of_Herodotus). [Demaratus](http://en.wikipedia.org/wiki/Demaratus) sent a warning about a forthcoming attack to Greece by writing it directly on the wooden backing of a wax tablet before applying its beeswax surface.

## 1.5 DIGITAL STEGANOGRAPHY

In digital steganography, the message is converted into binary message, and is hidden inside a cover object, there are many types of digital steganography; audio signal can be hidden inside an image or inside a video, text files can be hidden inside digital images, text files inside an audio file, and many others.

The hiding process utilities the sensitivity of human systems, for example, each pixel in gray scale images is represented by 8 bits, which means that there are 2^8=256 different color levels, the human visual system normally cannot distinguish between two subsequent colors, this “defect” can be exploited to hide data in the least significant bit of each pixel. Likely, in audio files, part of the less important data can be replaced by data to be hidden without the ability to sense the noise generated by the hiding process.

**2**

**CHAPTER 3**

**BACKGROUND**

**3.1 Image**

An image is essentially a 2-D signal processed by the human visual system. The signals representing images are usually in analog form. However, for image processing, storage and transmission, they are converted from analog to digital form. A digital image is basically a 2-D array of pixels. Images are formed of the significant part of data, particularly in remote sensing, biomedical and video conferencing applications. The use of and dependence on information and computers continue to grow, so does our need for efficient ways of storing and transmitting large amounts of data.

**3.1.1 Pixel**

In digital image, a pixel is a single point in a raster image. It is the smallest unit of picture that can be controlled and is the smallest addressable screen element as shown in Fig. 1. Each pixel has its own address. The address of a pixel corresponds to its coordinates. They are usually arranged in a 2-D grid and are often represented with dots or squares. Each pixel is a sample of an original image. More samples typically provide more accurate representations of the original. The intensity of each pixel is variable. In color image systems, a color is typically represented by three or four component intensities such as red, green, and blue.

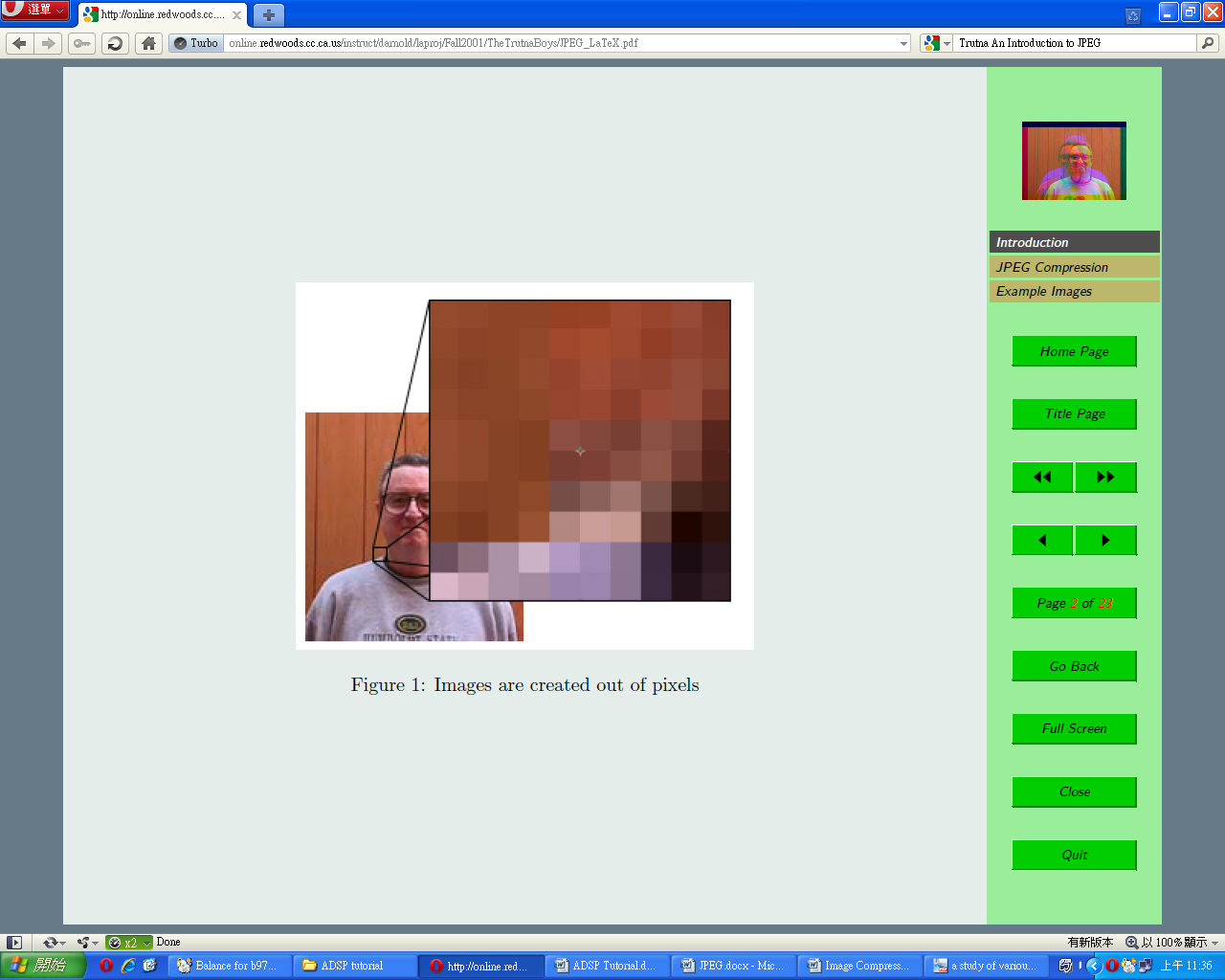


Fig 3.1 Pixel is smallest element of an image

**3**

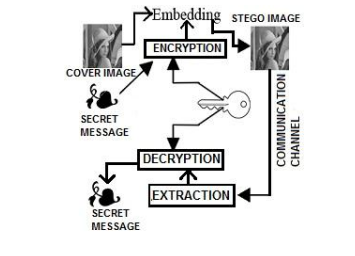
**3.2 DIGITAL IMAGE DATA HIDING TECHNIQUES**

The Stego image visually seems to be indifferent from the original cover but hides the secret message inside it and is transmitted to the desired recipients over the communication channels without creating any suspicion in the minds of the intermediately sniffers or/and receivers. When the authorized recipient receives the image, they follow the extraction procedure to retrieve the secret message. To increase the secrecy or security of the hidden message there may some keys involved in this process of embedding and extraction. At the transmission end, during embedding, the message can suitably be encrypted using one or more encryption techniques. These encryption standards can be key based encryptions or non-key based and in key based techniques, they again can be public or private or a mix.

Depending upon the encryption method used during the embedding process, the receiver needs to execute certain decryption algorithms to retrieve the correct message. If any of the decryption algorithms or the keys used for the procedure, or the sequence is not known to the receiver then the extraction fails and the receiver cannot retrieve the message. Digital steganography output may be in the form of printed documents. A message, the may be first encrypted by traditional means, producing. Then, an innocuous *cover text* is modified in some way so as to contain the ciphertext, resulting in the *stegotext*. For example, the letter size, spacing,  or other characteristics of a cover text can be manipulated to carry the hidden message. Only a recipient who knows the technique used can recover the message and then decrypt it.  developed  as such a technique.

The ciphertext produced by most digital steganography methods, however, is not printable. Traditional digital methods rely on perturbing noise in the channel file to hide the message, and as such, the channel file must be transmitted to the recipient with no additional noise from the transmission. Printing introduces much noise in the ciphertext, generally rendering the message unrecoverable. There are techniques that address this limitation, one notable example being ASCII Art Steganography.

Although not classic steganography, some types of modern color laser printers integrate the model, serial number, and timestamps on each printout for traceability reasons using a dot-matrix code made of small, yellow dots not recognizable to the naked eye — see [printer steganography](https://en.wikipedia.org/wiki/Printer_steganography) for details.

Fig 3.6Block Diagram of Digital Image Steganography

**3.3 TYPES OF DATA HIDING TECHNIQUES**

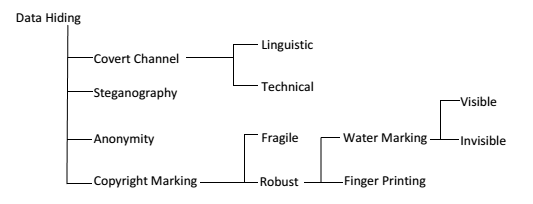
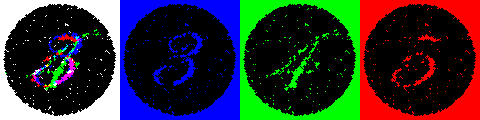


Fig 3.11Data hiding techniques

**3.4 DATA HIDING**

Data hiding, a form of Steganography, embeds data into digital media for the purpose of identification, annotation, and copyright. Several constraints affect this process: the quantity of data to be hidden, the need for invariance of these data under conditions where a “host” signal is subject to distortions, e.g., loss compression, and the degree to which the data must be immune to interception, modification, or removal by a third party.



**3.4.1 Features and applications**

Data-hiding techniques should be capable of embedding data in a host signal with the following restrictions and features:

1. The host signal should be none objectionably degraded and the embedded data should be minimally perceptible. (The goal is for the data to remain hidden. As any magician will tell you, it is possible for something to be hidden while it remains in plain sight; you merely keep the person from looking at it. We will use the words hidden, inaudible, unperceivable, and invisible to mean that an observer does not notice the presence of the data, even if they are perceptible.)

2. The embedded data should be directly encoded into the media, rather than into a header or wrapper, so that the data remain intact across varying data file formats.

4. Asymmetrical coding of the embedded data is desirable, since the purpose of data hiding is to keep the data in the host signal, but not necessarily to make the data difficult to access.

**3.4.2Data hiding in still images**

Data hiding in still images presents a variety of challenges that arise due to the way the human visual system (HVS) works and the typical modifications that images undergo. Additionally, still images provide a relatively small host signal in which to hide data. A fairly typical 8-bit picture of 200\*200 pixels provides approximately 40 kilobytes (kB) of data space in which to work. This is equivalent to only around 5 seconds of telephone-quality audio or less than a single frame of NTSC television. Also, it is reasonable to expect that still images will be subject to operations ranging from simple affine transforms to nonlinear transforms such as cropping, blurring, filtering, and loss compression.

Practical data-hiding techniques need to be resistant to as many of these transformations as possible. Despite these challenges, still images are likely candidates for data hiding.

**3.4.3 Security**

Security is an important property of the internet. The internet should provide and preserve the confidential and sensitive information that flows through it. The security should be such that only the intended recipient of the information should gain access to it.

**CHAPTER 4**

**STEGANOGRAPHY AND ITS ANALYSIS**

**Message Encoding Techniques**

**4.1 Steganography**

Steganography is the art and science of invisible communication. This is accomplished through hiding information in other information, thus hiding the existence of the communicated information. Thus, image steganography is a better approach than cryptography. Purpose of image processing is to make the quality of an image better so that the required operations can be easily performed on it. Image steganography is performed on the desired formats which are suitable. Steganography includes the concealment of information within computer files. In digital steganography, electronic communications may include steganographic coding inside of a transport layer, such as a document file, image file, program or protocol. Media files are ideal for steganographic transmission because of their large size. As a simple example, a sender might start with an innocuous image file and adjust the color of every 100th [pixel](http://en.wikipedia.org/wiki/Pixel) to correspond to a letter in the alphabet, a change so subtle that someone not specifically looking for it is unlikely to notice it.

The least significant bit (LSB) is one of the most public techniques in steganography. The classical technique is **LSB substitution**. The main idea of this technique is to directly alter some LSB of the cover image with the secret data.

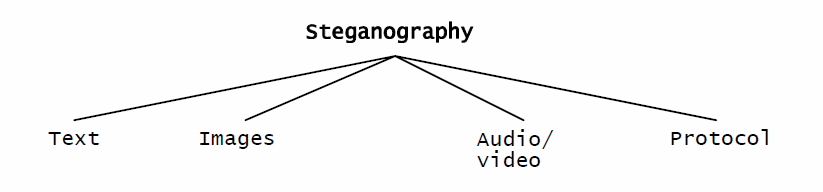
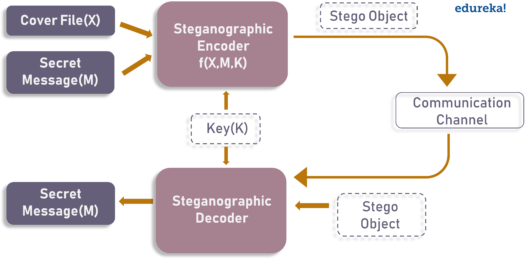


Fig 4.1Steganography



**Patchwork** – The biggest disadvantage of the patchwork approach is the small amount of information that can be hidden in one image. This property can be changed to accommodate more information, but one may have to sacrifice the secrecy of the information. Patchwork’s main advantage, however, is its robustness against malicious or unintentional image manipulation. Should a stego image using patchwork be cropped or rotated, some of the message data may be lost but since the message is repeatedly embedded in the image, most of the information will survive. Patchwork is most suitable for transmitting a small amount of very sensitive information.

**4.1.1 Ancient Steganography**

The first recorded uses of steganography can be traced back to 440 BC when [Herodotus](http://en.wikipedia.org/wiki/Herodotus) mentions two examples of steganography in [*The Histories of Herodotus*](http://en.wikipedia.org/wiki/The_Histories_of_Herodotus). [Demaratus](http://en.wikipedia.org/wiki/Demaratus) sent a warning about a forthcoming attack to Greece by writing it directly on the wooden backing of a wax tablet before applying its beeswax surface. [Wax tablets](http://en.wikipedia.org/wiki/Wax_tablet) were in common use then as reusable writing surfaces, sometimes used for [shorthand](http://en.wikipedia.org/wiki/Stenography). Another ancient example is that of [Histiaeus](http://en.wikipedia.org/wiki/Histiaeus), who shaved the head of his most trusted slave and tattooed a message on it. After his hair had grown the message was hidden. The purpose was to instigate a revolt against the [Persians](http://en.wikipedia.org/wiki/Persian_Empire).

**4.1.2 Modern Steganography**

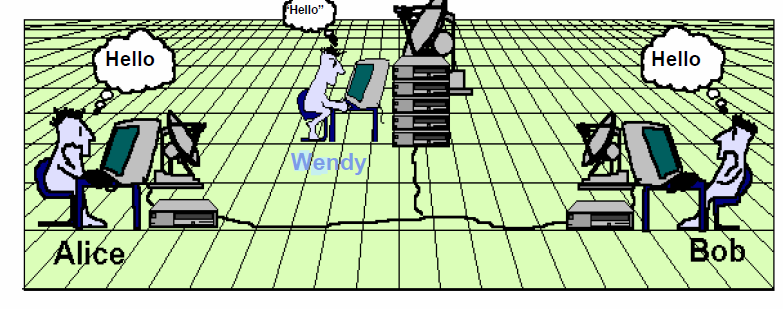


Fig 4.2 1Modern Steganography—THE PRISONER`S PROBLEM

Alice and Bob are communicating with each other using secret message exchanging.

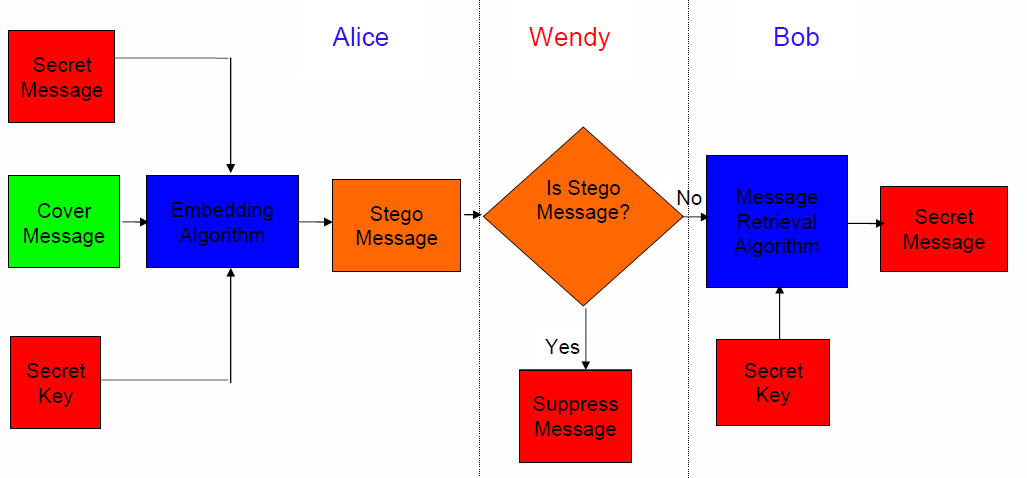


Fig 4.3 Block Diagram

**4.1.3 Steganography in practice**

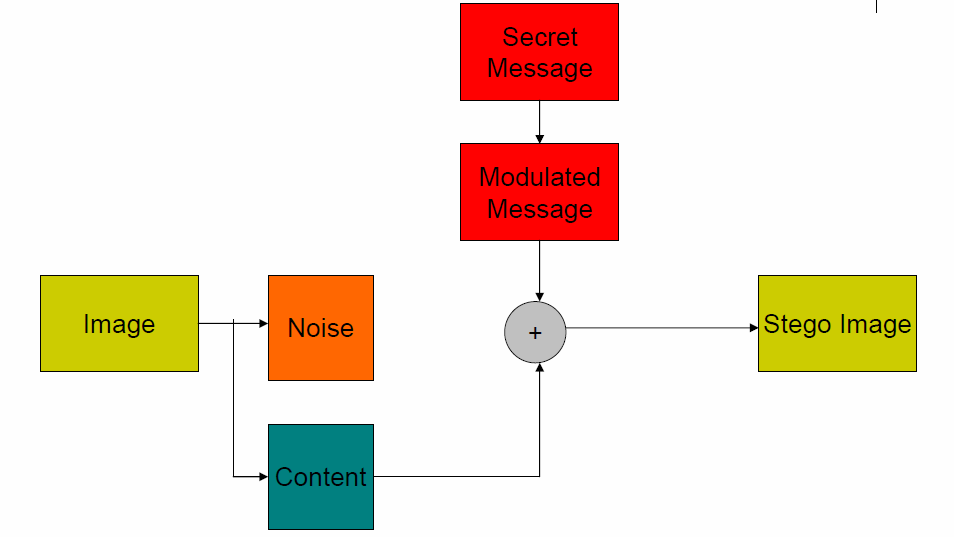


Fig 4.4 Steganography in practice

Steganography is a special case of data hiding. But data hiding cannot always be steganography. In steganography main goal is to escape from Wendy when Alice and Bob are communicating with each other.

**4.2 Different techniques**

**4.2.1 Physical steganography**

* Hidden messages within [wax tablets](http://en.wikipedia.org/wiki/Wax_tablet) — in ancient [Greece](http://en.wikipedia.org/wiki/Greece), people wrote messages on the wood, and then covered it with [wax](http://en.wikipedia.org/wiki/Wax) upon which an innocent covering message was written.
* Hidden messages on messenger's body — also used in ancient Greece. [Herodotus](http://en.wikipedia.org/wiki/Herodotus) tells the story of a message [tattooed](http://en.wikipedia.org/wiki/Tattoo) on a [slave](http://en.wikipedia.org/wiki/Slave)'s [shaved](http://en.wikipedia.org/wiki/Shaving) head, hidden by the growth of his hair, and exposed by shaving his head again. The message allegedly carried a warning to Greece about [Persian](http://en.wikipedia.org/wiki/Persian_Empire) [invasion](http://en.wikipedia.org/wiki/Invasion) [plans](http://en.wikipedia.org/wiki/Plan). This method has obvious drawbacks, such as delayed transmission while waiting for the slave's hair to grow, and the restrictions on the number and size of messages that can be encoded on one person's scalp.

.

**4.2.2 Digital Steganography**

Modern steganography entered the world in 1985 with the advent of the personal computer being applied to classical steganography problems. Development following that was slow, but has since taken off, going by the number of "stego" programs available. Digital steganography techniques include:

* Concealing messages within the lowest bits of [noisy](http://en.wikipedia.org/wiki/Image_noise) images or sound files.
* Concealing data within encrypted data or within random data. The data to be concealed is first encrypted before being used to overwrite part of a much larger block of encrypted data or a block of random data (an unbreakable cipher like the [one-time pad](http://en.wikipedia.org/wiki/One-time_pad) generates cipher texts that look perfectly random if you don't have the private key).

**4.2.3 Network Steganography**

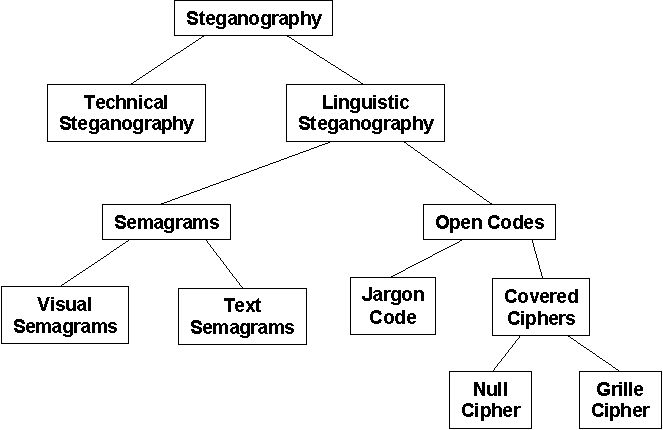
All information hiding techniques that may be used to exchange steganographs in telecommunication networks can be classified under the general term of network steganography. This nomenclature was originally introduced by Krzysztof Szczypiorski in 2003. Contrary to the typical steganographic methods which utilize digital media (images, audio and video files) as a cover for hidden data, network steganography utilizes communication protocols' control elements and their basic intrinsic functionality. As a result, such methods are harder to detect and eliminate.

**4.2.4 Printed Steganography**

Digital steganography output may be in the form of printed documents. A message, the [*plaintext*](http://en.wikipedia.org/wiki/Plaintext), may be first encrypted by traditional means, producing a [*cipher text*](http://en.wikipedia.org/wiki/Ciphertext). Then, an innocuous *cover text* is modified in some way so as to contain the cipher text, resulting in the *stego text*. For example, the letter size, spacing, [typeface](http://en.wikipedia.org/wiki/Typeface), or other characteristics of a cover text can be manipulated to carry the hidden message. Only a recipient who knows the technique used can recover the message and then decrypt it. [Francis Bacon](http://en.wikipedia.org/wiki/Francis_Bacon) developed [Bacon's cipher](http://en.wikipedia.org/wiki/Bacon%27s_cipher) as such a technique.

**4.2.5 Text Steganography**

Steganography can be applied to different types of media including text, audio, image and video etc. However, text steganography is considered to be the most difficult kind of steganography due to lack of redundancy in text as compared to image or audio but still has smaller memory occupation and simpler communication. The method that could be used for text steganography is data compression. Data compression encodes information in one representation into another representation.



**CHAPTER 5**

**PROPOSED ALGORITHM**

In this paper dual steganography of text for secure communication has been proposed. Here in dual steganography, image steganography is used within video steganography.

1. Data insertion stage

The process of embedding data in host file is shown in figure (1). The secret data has been embedded inside cover image with the help of 4-bit LSB (least significant bit) algorithm along with the stego-key. The key used is maximum of 10 bit length. Key is embedded in the cover image during the LSB embedding process. This should be known at the iver side during the apprehend process for retrieving the secret file.

The algorithm works as follows:

**Image steganography:**

• Cover image is separated into RGB planes.

• Secret data taken is then converted into binary form.

• Those values are separated into upper and lower nibbles which are embedded in two separate planes of the cover image.

• Upper nibbles are embedded in green plane and lower nibbles in red plane using 4bit LSB method.

• Stego key is embedded inside the blue plane.

• After which, all the three planes are combined to generate stego-image.

**Video steganography:**

• Input the cover video stream.

• Convert the video sequence into a number of frames.

• Split each frame into the YUV color space.

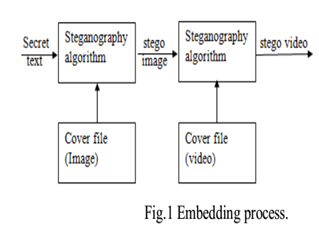
• Apply the two-dimensional DWT twice separately to each Y frame component.

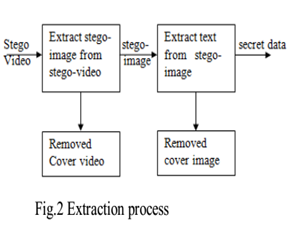
• Embed the message (stego-image) into the middle frequency coefficients (LH, HL) of each of the Y components.

• Apply the inverse two-dimensional DWT on the frame components.

• Rebuild the stego frames from the YUV stego components.

• Output the stego videos, which are reconstructed from all embedded frames.





**B. Data extraction stage**

The process of extraction is shown in figure (2). In section the process of retrieving the embedded message (stegno image) from stego-videos first and the retrieving secret massage (text) from stego-image is introduced.

**The algorithm works as follows:**

• Input the cover video stream

• Convert the video sequence into a number of frames.

• Split each frame into the YUV color space.

• Apply the two-dimensional DWT twice separately to each Y frame component.

• Extract the message (stego-image) from the middle frequency coefficients (LH, HL) of each of the Y components.

• Perform inverse DWT method.

• The extract secret massage from stego-image

**CHAPTER 6**

**CONCLUSION**

This paper presents a state-of-the-art combination work of two popular information security approaches, namely cryptography and steganography. However, both of techniques provide security for secrete information but separately one can’t guarantee for absolute security of data. Therefore, to provide more security to the information at the time of communication over unsecured channel a novel advance technique for data security is needed.

In all experiments, the average PSNR is greater than 84dB for image steganography and 64 for video steganography. Therefore, experimental results show that the proposed model is effective. It maintains the quality of the video and no variation between the cover data and stegano-data that can be detected by the human vision system. Future work can be done in way to combining the concepts of hybrid cryptography and audio steganography, to provide more security to the secrete message.

**REFERENCES**

[1] Sumeet Kaur, Savina Bansal, and R. K. Bansal., “Steganography and Classification of Image Steganography Techniques”. International Conference on Computing for Sustainable Global Development.978-93 -80544-12-0/14 2014 IEEE 2014.

[2] Mennatallah M. Sadek & Amal S. Khalifa & Mostafa G. M. Mostafa. “Video steganography: a comprehensive review” DOI 10.1007/s11042- 014-1952-z Springer Science New York 2014.

[3] Wang Tianfu, K. Ramesh Babu., “Design of a Hybrid Cryptographic Algorithm”. International Journal of Computer Science & Communication Networks,Vol 2(2), 277-283.

[7] Priyanka Singh, Sunita Agarwal, and Akanksha Pandey “A Hybrid DWT-SVD Based Robust Watermarking Scheme for Color Images and its Comparative Performance in YIQ and YUV Color Spaces” 2013 3rd IEEE International Advance Computing Conference (IACC) 978-1- 4673-4529-3 IEEE 2012.

[8] Smita P. Bansod Vanita M. Mane Leena R. Raghav., “Modified BPCS steganography using Hybrid Cryptography for Improving Data embedding Capacity”. 978-1-4577-2078-9 IEEE 2011.

[9] N. Provos and P. Honey man, “Hide and Seek: An introduction to steganography”, IEEE Security and Privacy Journal, 2003.