**Chapter 1**

**INTRODUCTION**

The network so the existence of the message is unknown. Besides concealing information for confidentially, this approach of data concealing is extended to copyright protection for digital media: audio, video secure data. Secure data. Steganography could be a technique of concealing data in digital media. In distinction to cryptography, the message or encrypted message is embedded in very digital host before passing it through, in good identity cards wherever personal details are embedded within the photograph itself for copyright Management of materials and image. [6]

Steganography is used for big selection of applications like, in defense organizations for safe circulation of secret knowledge, in military and intelligence agencies Due to advances in ICT, most of data is unbroken electronically. Consequently, the protection of data has becomes an elementary issue. Besides cryptography is used. In medical imaging, patients details are embedded at intervals image providing protection of data and reducing coordinated universal time and cost. In on-line legal system therefore on create the web election secure and study against a spread of dishonorable behaviors, for knowledge activity in countries wherever cryptography is prohibited, in rising mobile banking security in tamer proofing therefore on stop or observe unauthorized modification and alternative varied applications. [7]

The basic model of steganography consists of Carrier, Messageand Password. Carrier is also known as cover-object, which the message is embedded and serves to hide the presence of the message. Steganography is a type of hidden communication that literally means “covered writing” (from the Greek words stegano or “covered” and graphos or “to write”). The goal of steganography is to hide an information message inside harmless cover medium in such a way that it is not possible even to detect that there is a secret message. Often times throughout history, encrypted messages have been intercepted but have not been decoded. While this protects the information hidden in the cipher, the interception of the message can be just as damaging because it tells an opponent or enemy that someone is communicating with someone else. Steganography takes the opposite approach and attempts to hide all evidence that communication is taking place. Essentially, the information-hiding process in a Steganographic system starts by identifying a cover medium’s redundant bits (those that can be modified without destroying that medium’s integrity). The embedding process creates a stego medium by replacing these redundant bits with data from the hidden message. Modern steganography’s goal is to keep its mere presence undetectable, but steganographic systems, because of their invasive nature, leave behind detectable traces in the cover medium through modifying its statistical properties, so eavesdroppers can detect the distortions in the resulting stego medium’s statistical properties. The process of finding these distortions is called Statistical Steganalysis.

Internet came into existence in the late 1960s and 1970s out of the need to exchange research data among the researchers across different universities and also to enable communication in the battlefield to convey vital information which could prove advantageous in the war situations. Since the inception of the internet, the security and the confidentiality of the sensitive information have been of utmost importance and top priority.

The reason for this security and confidentiality is because the underlying communication network over which the transfer of sensitive information is carried out is unreliable and unsecured. Anybody with the proper knowledge and right applications can eavesdrop and learn of the communication and intercept the data transfer which could be very dangerous and even life threatening in some situations. Ideally the internet and the communication network and the routing protocols should exhibit the following the properties:

**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.

**Distributed Operation**: The internet should be distributed rather than only residing on some centralized server. In the event of the crash the internet should not lose its functionality and continue performing efficiently.

**Reliability**: Reliable communication is one of the vital properties of the internet. The internet should guarantee the reliable delivery of the information to the intended recipient.

**Fault-Tolerance**: Fault-tolerance means the ability of the system to operate normally even in the events of failure. Internet should exhibit fault-tolerance so that it keeps on functioning even when there is failure in some part of the internet.

**Quality of Service Support**: Quality of Service (QoS) is one of the crucial properties in terms of communication. Inter should provide QoS support to various applications and sensitive data and should prioritize them depending on the nature of the data.

**Robustness**: Internet should be robust in the sense that it should continue functioning normally even in the presence of errors and unexpected situations like invalid input. All the above mentioned properties are ideal and cannot be practically implemented in the structure and functioning of the internet as it comprises of many networks, different infrastructures: wired, wireless, ad hoc and various mobility models. One such property that cannot be guaranteed in the internet is Security. Due to the inability to guarantee security, various vulnerabilities exist in the network that can be exploited and gives rise to several security attacks. Some of the common security attacks are listed below.

**Impersonation or Spoofing:** The main goal of this attack is to assume the identity of the person and convince the sender that it is communicating with the intended recipient.

**Man in the Middle attack:** In this attack, the attacker makes independent connections with the two parties across the network making them believe that they are communicating privately, when in fact the communication is controlled and intercepted by the attacker.

**Traffic Analysis:** In this process the attacker listens to the chatter on the communication network between two parties without interacting between them and tries to learn the information that they are sharing. To mitigate these security vulnerabilities and facilitate seamless and safe transfer of data over the communication channel, techniques like cryptography, hashing, authentication, authorization, steganography are developed. Our paper illustrates various data hiding techniques in steganography to enable the safe transfer of critical data over the unsecure network. Steganography is sometimes erroneously confused with cryptography, but there are some notable and distinctive differences between the two. In some situations steganography is often preferred to cryptography because in cryptography the cipher text is a scrambled output of the plaintext and the attacker can guess that encryption has been performed and hence can employ decryption techniques to acquire the hidden data. Also, cryptography techniques often require high computing power to perform encryption which may pose a serious hindrance for small devices that lack enough computing resources to implement encryption. On the contrary, Steganography is the process of masking the sensitive data in any cover media like still images, audio, video over the internet. This way the attacker does not realize that the data is being transmitted since it is hidden to the naked eye and impossible to distinguish from the original media.

The (*n, n*) - NVSS scheme can share one digital secret image over *n* - 1 arbitrary selected natural images (called natural shares) and one noise-like share. The natural shares can be photos or hand-painted pictures in digital form or in printed form. The noise-like share is generated based on these natural shares and the secret image. The unaltered natural shares are diverse and innocuous, thus greatly reducing the transmission risk problem. We also propose possible ways to hide the noise like share to reduce the transmission risk problem for the share. Experimental results indicate that the proposed approach is an excellent solution for solving the transmission risk problem for the VSS schemes.

The rapid development of Internet technology, people can transmit and share digital content with each other conveniently. In order to guarantee communication efficiency and save network bandwidth, compression techniques can be implemented on digital content to reduce redundancy, and the quality of the decompressed versions should also be preserved. Nowadays, most digital content, especially digital images and videos, are converted into the compressed forms for transmission. Another important issue in an open network environment is how to transmit secret or private data securely. Even though traditional cryptographic

**Secure Information Hiding System (SIHS)**

An information hiding system has been developed for confidentiality. However, in this paper, we study an image file as a carrier to hide message. Therefore, the carrier will be known as cover-image, while the stego-object known as stego-image.

Cover Image (\*.bmp)



Stego Image

Message 

Hi : how are you ?

I am fine.

**Figure 1.1. Producing Stego-Image Process**

Cryptography was fashioned as a way for securing the confidentiality of message. Many Different ways are developed to write in code and rewrite knowledge so as to stay the message surreptitious. Sadly, it's typically not sufficient to remain the contents of a message secret. So, it’s necessary to stay the survival of the message secret. [12]

VISVAL cryptography (VC) is a technique that encrypts a secret image into *n* shares, with each participant holding one or more shares. Anybody who holds fewer than *n* shares cannot reveal any information about the final secret image. Stacking the *n* shares reveals the secret image and it can be recognized directly by the human eyes. [13]

The basics of data rely on three different facts i.e. capacity, security, and robustness. Capacity means the media on which the data is to be hidden should hold the data, so that the complexity of the medium should not be disturbed. Security means the embedding algorithm is said to be secure if the embedded information cannot be removed beyond reliable detection by targeted attacks. Finally, robustness means the amount of manipulation a cover image (original image) can handle without drawing any attention that a change has taken place. Steganography and cryptography have to guarantee any of the requirements. Steganography and Cryptography are parallel data security techniques and the techniques can be implemented side by side, in fact steganographic system can implement cryptographic data security. With cryptography we can protect the message but not hide its existence. Steganography pay attention to the degree of invisibility while cryptography pays attention to the security of the message. Once the presence of hidden information is revealed or even suspected, the purpose of steganography is partly defeated. The strength of steganography can thus be increased by combining it with cryptography.

The main feature of the encryption/decryption program implementation is the generation of the encryption key. Now a day, cryptography has many commercial applications. If we are protecting confidential information then cryptography is provide high level of privacy of individuals and groups. However, the main purpose of the cryptography is used not only to provide confidentiality, but also to provide solutions for other problems like: data integrity, authentication, non-repudiation. Cryptography is the methods that allow information to be sent in a secure from in such a way that the only receiver able to retrieve this information. Presently continuous researches on the new cryptographic algorithms are going on. However, it is a very difficult to find out the specific algorithm, because we have already known that they must consider many factors like: security, the features of algorithm, the time complexity and space complexity. Figure is representing conventional encryption.

An information-hiding system is characterized be having three different aspects that contend with each other as shown in Figure 1: capacity, security, and robustness. Capacity refers to the amount of information that can be hidden in the cover medium, security to an eavesdropper’s inability to detect hidden information, and robustness to the amount of modification the stego medium can withstand before an adversary can destroy hidden information [6]. Generally speaking, information hiding relates to both watermarking and steganography. A watermarking system’s primary goal is to achieve a

high level of robustness-that is, it should be impossible to remove a watermark without degrading the data object’s quality. Steganography, on the other hand, strives for high security and capacity, which often entails that the hidden information is fragile. Even trivial modifications to the stego medium can destroy it.

The use of cryptography as a way to secure the hidden message mainly addresses the security requirement in the Information-Hiding system. For the purpose of steganography, symmetric encryption is followed. The symmetric encryption is a method of encryption that uses the same key to encrypt and decrypt a message. If one person encrypts and decrypts data, that person must keep the key secret. If the data is transmitted

between parties, each party must agree on a shared secret key and find a secure method to exchange the key. The security of encrypted data depends on the secrecy of the key. If someone gains knowledge of the secret key, he or she can use the key to decrypt all the

data that was encrypted with the key. No encryption method is completely secure. Given

knowledge of the algorithm and enough time, attackers can reconstruct most encrypted data. A strong algorithm (the one that is built on sound mathematical methods, creates no predictable patterns in encrypted data, and has a sufficiently long key) can deter most attacks.

**Color System:-**

**RGB**

The RGB color model is an additive color model in which red, green, and blue light are added together in various ways to reproduce a broad array of colors. The name of the model comes from the initials of the three additive primary colors, red, green, and blue [5]. The main purpose of the RGB color model is for the sensing, representation, and display of images in electronic systems, such as televisions and computers, though it has also been used in conventional photography. Before the electronic age, the RGB color model already had a solid theory behind it, based in human perception of colors [5].

**Color:-**

Color or Color is the visual perceptual property corresponding in humans to the categories called red, yellow, blue, black, etc. The RGB color model is the most common way to encode color in computing, and several different binary digital representations are in use. Color derives from the spectrum of light (distribution of light energy versus wavelength) interacting in the eye with the spectral sensitivities of the light receptors. Color categories and physical specifications of color are also associated with objects, materials, light sources, etc., based on their physical properties such as light absorption, reflection, or emission spectra.

**LSB Encoding:-**

The simplest and the most common steganographic technique is the Least Significant Bit embedding (LSB). The premise here is that changes to the least significant bit will be masked by noise commonly present in digital images. Actually, in the case of color images, there is even more room for hiding messages because each pixel is a triple of red, green, and blue. Again, replacing two or more least significant bits of each pixel increases the capacity of the scheme but at the same time the risk of making statistically detectable changes also increases. Therefore, it is important to study the security of each

specific steganographic technique and argue why it is secure. Even the simple least significant bit encoding may under certain circumstances introduce detectable changes.

**1.1 Motivation:-**

Internet is the fastest growing message medium and essential part of infrastructure, nowadays. To cope with the growth of internet it has become a constant struggle to keep the secrecy of information and when profits are involved, protect the copyright of data. To provide secrecy and copyright of data many of the stenographic techniques has been developed. But each of the technique has their respective pros and cons. Where one technique lacks in payload capacity, the other lacks in robustness. So, the main motivation of proposed work is to overcome these short comings.

**1.2 Aim:-**

An aim to process of hiding one medium of communication (image) methodology is applied to hiding blocks of data indiverse images*.*

**1.3 Objective:-**

The objectives of this project is to create an easy to use environment in which the user can provide a sample image for hiding the secrete data into it using Higher LSB Data Hiding Algorithm & to extract data from an image using Higher LSB Data Extraction Algorithm.

The Main objectives of this proposed method are:-

1. To increase the Payload capacity. It refers to the amount of data that can be inserted into cover media without deteriorating its integrity.
2. To maintain Image Perceptual quality. It is necessary that to avoid suspicion the embedding should occur without significant degradation or loss of perceptual quality of the cover media.

3. To provide security to hidden message from unauthorized accesses.

**1.4 Scope:-**

In this dissertation work, one can find the future scope in the proposed algorithm. So far we are replacing 5 bits of LSB going from LSB to MSB. But it may possible to modify our algorithm so that we manage to replace 6 bits of LSB. If 6 bits of LSB get replaced, it may generate more quantization error. So, one should smart enough to reduce generated quantization error. In the future work we can divot our efforts in improving the Payload capacity but we also need to take the note on the resultant noise which may generated due to increased payload which disturbs the image quality.

**1.5 Problem Definition:-**

Digital media data hiding techniques have developed a strong basis for stegnography area with a growing number of applications like digital privileges management, covert communications, hiding executables for access control, annotation etc. In all application scenarios given above, multimedia stegnography techniques have to satisfy three basic requirements. The best requirement is Perceptual Transparency, i.e. cover object (object not containing any additional data) and stego object (object containing secret message) must be perceptually indiscernible.

The second constraint is high data rate of the embedded data. All the stego applications, besides requiring a high bit rate of the embedded data, have need of algorithms that detect and decode hidden bits without access to the original digital media sequence (Blind detection algorithm).

The third constraint is security that means providing security to the data hidden inside carrier or we can say that inability by unauthorized users to detect/access the communication channel. Information hiding in digital media can be used for such a diverse applications as proof of ownership,authenticaton,integrity, secret communication, broadcast monitoring and event annotation.

All the techniques mentioned earlier were good ways of hiding messages but even with the new twists given to them, they were still nothing compared to the Types of applications developed with the invention of the computer. So, we developed the new algorithm called Higher LSB Data Hiding Algorithm which causes minimal embedding distortion and achieves all three important constraints of data hiding. This provides good perceptual transparency, security & improves payload capacity.

**Chapter 2**

**LITERATURE REVIEW**

|  |
| --- |
|  |

**Background History**

**Tung-Hsiang Liu and Long-Wen Chang et al** **[2004**] a simple data hiding technique for binary images in the proposed method embeds secure data at the edge portion of host binary image. Binary images consist of only two colors therefore changing any pixels in this image could be easily detected by human eyes. Therefore, data is stored in the edge portion of binary image; as the modification of edge pixels is more difficult to be recognized by human eyes. The Distance matrix mechanism is used to find the edge pixels of host binary image. Then the Weight mechanism is used to consider the connectivity of the neighborhood around changeable pixels for choosing the most suitable one. For the security and quality consideration, a random number generator is used to distribute the embedding data into the overall image. This method not only embeds large amounts of data into host binary image but also can maintain image quality. [1]

**H.C. Wu, N.I. Wu, C.S. Tsai and M.S. Hwang** **et al** **[2005]** improve the capacity of the hidden secret data and to provide am imperceptible stego image quality. Has proposed a novel stenographic method based on Least Significant Bit (LSB) Replacement and Pixel Value Differencing (PVD) methods. [2]

**Hsien-Wen Tseng, Feng-Rong Wu, and Chi-Pin Hsieh** **et al** **[2007]** has a novel method for hiding data in binary images. The binary cover image is partitioned into eq ual-sized, non-overlapping blocks and the watermark will be embedded into blocks by flipping pixels. For security consideration, the watermark data is firstly permuted into a meaningless bit sequence by using a secret key. [3]

**Beenish Mehboob and Rashid Aziz Faruqui et al** **[2008]** discussed the art and science of Steganography in general and proposed a novel technique to hide data in a colorful image using least significant bit. Least Significant Bit or its variants are used to hide data in digital image. Digital Images are represented in bits. [4]

**M.B. Ould Medeniand & El Mamoun Souidi et al** **[2010]** a novel stenographic method for gray level images on four pixel differencing and LSB substitution. The proposed approach works by dividing the cover into blocks of equal sizes and split each pixel into two parts .Then it counts number of one’s in most part and embeds the secret message in the least part according to the corresponding number of bits in most part. As shown in following fig. 2.1. [5]



Figure2.1: Split Process



TABLE: 2.1 NUMBER OF 1 AND THE CORRESPONDING NUMBER OF BITS TO EMBED.

Therefore, it embeds the message in the edge of the block depending on the number of ones in left four bits of the pixel. They used K-bit LSB substitution method for hiding the secret data into each pixel where K is decided by the number of one in the most part of pixel. This method gave best values for the PSNR measure which means that there were no big difference between the original and the stegno image.

**Kousik Dasgupta & J.K. Mandaland Paramartha Dutta** **et al** **[2012]** have proposed a secured has based LSB technique for video stenography. This technique utilizes cover video files in spatial domain to conceal the presence of sensitive data regardless of its format. Video Steganography deals with hiding secret data or information within a video. In this author, a hash based least significant bit (LSB) technique has been proposed. A spatial domain technique where the secret information is embedded in the LSB of the cover frames. Eight bits of the secret information is divided into3, 3, 2 and embedded into the RGB pixel values of the cover frames respectively. As shown in following fig: 2.2



Figure: 2.2 shows secret data embedded in 4 bits of LSB in 3, 3, 2 order in corresponding RGB pixels of carrier frame

A hash function is used to select the position of insertion in LSB bits. The proposed technique takes eight bits of secret data at a time and conceal them in LSB of RGB(Red, Green and Blue) pixel value of the carrier frames in 3, 3, 2 order respectively. Such that out of eight (08) bits of message six (06) bits are inserted in R and G pixel and remaining two (02) bits are inserted in B pixel. After comparing the proposed technique with LSB technique it is found that the performance analysis of proposed technique is quite encouraging. The advantage of this method is that the size of the message does not matter in video stenography as the message can be embedded in multiple frames. [11]

**Tasnuva Mahjabin, Syed Monowar Hossain and Md. Shariful Haque et al** **[2012]** a data hiding method based on PVD and LSB substitution to improve the capacity of the secret data as well as to make stegnalysis a complicated task they made an effort to implement a robust dynamic method of data hiding. [7]

**Ankit Chaudhary and JaJdeep Vasavada et al** **[2012]** an improved stenography approach for hiding text messages in RGB lossless images The security level is increased by randomly distributing the text message over the entire image instead of clustering within specific image portions. [8]

**RigDas and Themrichon Tuithung et al** **[2012]** novel technique for image stenography based on Huffman Encoding. Huffman Encoding is performed over the secret image/message before embedding and each bit of Huffman code of secret Image/message is embedded inside the cover image by altering the least significant bit (LSB) of each of the pixel's intensities of cover image. This paper presents a novel technique for image steganography based on Huffman Encoding. Two 8 bit gray level image of size M X N and P X Q are used as cover image and secret image respectively. Huffman Encoding is performed over the secret image/message before embedding and each bit of Huffman code of secret image/message is embedded inside the cover image by altering the least significant bit (LSB) of each of the pixel's intensities of cover image. The size of the Huffman encoded bit stream and Huffman Table are also embedded inside the cover image, so that the Stego-Image becomes standalone information to the receiver.

**Ming Li, Michel K. Kulhandjian, Dimitris, A. Pados,, Stella N. Batalama, and Michael J. Medley et al** **[2013]** has considered the problem of extracting blindly data embedded over a wide band in a spectrum (transform) domain of a digital medium (image, audio, video).We develop a novel multicarrier/signature iterative generalized least-squares (M-IGLS) core procedure to seek unknown data hidden in hosts via multicarrier spread-spectrum embedding. Neither the original host nor the embedding carriers are assumed available. [11]

**Kai-Hui Lee and Pei-Ling Chiu et al** **[2014]** has developed efficient encryption/decryption algorithms for the (*n, n*) -NVSS scheme. The proposed algorithms are applicable to digital and printed media. The possible ways to hide the generated share are also discussed. The proposed NVSS scheme not only has a high level of user friendliness and manageability, but also reduces transmission risk and enhances the security of participants and shares. [13]

**2.2. Related Work :-**

Table

|  |  |  |  |
| --- | --- | --- | --- |
| **Sr.No** | **Year** | **Author** | **Advantages** |
| 1 | 2004 | Tung-Hsiang Liu Long-Wen Chang | Large amount of data can be stored in binary images as well as quality of an image is maintained. |
| 2 | 2005 | H.-C. Wu,  N.-I. Wu,  C.-S. Tsai  M.-S. Hwang | Much larger information can be stored in images by using LSB method for storing data in smooth areas of image. |
| 3 | 2005 | M. Carli, M.C.Q. Fariasy,E.Drelie,Gelascaz,R. Tedesco,A. Neri | Quality of a compressed video is estimated by using simple embedding system. |
| 4 | 2007 | Hsien-Wen Tseng,  Feng-Rong Wu,Chi-Pin | This method achieved a good visual quality for watermarked image and has high capacity of embedding. |
| 5 | 2008 | Beenish Mehboob Rashid Aziz Faruqui | LSB method is used for hiding data in colorful images than other techniques which require masking and filtering. |
| 6 | 2010 | M.B.Ould Medeni El Mamoun Souidi | K-bit LSB substitution method used here gave best values for the PSNR measure. |
| 7 | 2012 | Tasnuva Mahjabin,  Syed Monowar Hossain  Md.Shariful Haque | PVD & LSB methods used here which achieved an increased embedding capacity and lower image degradation with improved security. |
| 8 | 2012 | Ankit Chaudhary JaJdeep Vasavada | 1-bit LSB substitution method used which increased the security level and improved the storage capacity |
| 9 | 2012 | Kousik Dasgupta, J.K.Mandal  Paramartha Dutta | It allows embedding the large size of data in multiple frames. Therefore size of the message does not matter. |
| 10 | 2012 | Poonam V Bodhak Baisa L Gunjal | DCT & LSB methods used which provide high security to embedded data. |
| 11 | 2012 | RigDas  ThemrichonTuithung | Huffman Encoding is used for secret message which again improves the security level of hiding data. |
| 12 | 2013 | Ming Li*,*  Michel K. Kulhandjian, Dimitris,  A. Pados*,*  Stella N. Batalama*,* Michael J. Medley | M-IGLS procedure is used for extracting blindly data embedded over a wide band in a spectrum domain of a digital medium. |
| 13 | 2017 | Miss. Sweeti A. Parwatkar, Proff. V.B. Bhagat. | Data Hiding Approaches by Diverse Image Media. |

For hiding secret data in digital media, large varieties of techniques are discussed above which are more complex than others and all of them have their respective pros & cons. Initially Binary Images are used for hiding data and it improved the data hiding capacity greatly by using smooth and edge areas of an image. Later on different variations of LSB method are used for colorful images to hide data. After that, data is hidden in different frames of video by using the concept of hiding the data in an image.

But all of the above methods were somewhere lacked in their performance while for hiding secret data in digital media, large varieties of techniques are discussed above which are more complex than others and all of them have their respective pros & cons. Initially Binary Images are used for hiding data and it improved the data hiding capacity greatly by using smooth and edge areas of an image. Later on different variations of LSB method are used for colorful images to hide data. After that, data is hidden in different frames of video by using the concept of hiding the data in a preserving the quality of an image or in the issues of security. In this section a comparative analysis of different data hiding schemes in steganography is presented. The authors in have all presented techniques to hide data in the still images and generated stego-images as the output. In [6] the authors embed the data in RGB 24 bit color image by using the linked data structures where in, the data hidden in the image is linked with other data. The advantage of this method is that hiding the data randomly than sequential will make it difficult for the attacker to locate it and also without the authentication key the attacker will not be able to access the next piece of data in the image. Instead of using the whole image as the cover image, the authors in have proposed a method that segments the image into blocks of equal sizes. Also, the process involved in this method is reversible hence there is no loss of hidden data. The approach followed in this scheme to conceal data is quite different. In this technique the histograms of the blocks of images is taken and they are shifted to minimum point of the histogram and then the data is hidden between these points. The improvement of this technique is that it provides higher capacity to hide data than the previous method. In optimized bit plane splicing method is implemented. In this method the intensity value of the pixel is divided into different planes and rather than using the traditional method of hiding the data into LSB of the pixel and plane by plane, the data in this approach is hidden based on the intensity of the pixels. The pixels are grouped based on the intensity and then number of pixels used to represent the data is chosen depending on the intensities. Also, rather than hiding the data sequentially in the planes, the data is hidden randomly and during the transmission of the data the planes are transferred randomly to make it difficult to intercept the data The advantage of this technique is that by grouping the pixels according to the intensity more number of bits is available to represent the hidden data than just the LSB of the pixel. In to increase and utilize the higher bit planes to hide the data a different approach from the one discussed earlier is employed. The advantage of this technique is that by grouping the pixels according to the intensity more number of bits is available to represent the hidden data than just the LSB of the pixel. In to increase and utilize the higher bit planes to hide the data a different approach from the one discussed earlier is employed. The advantage of this technique is that by grouping the pixels according to the intensity more number of bits is available to represent the hidden data than just the LSB of the pixel. In to increase and utilize the higher bit planes to hide the data a different approach from the one discussed earlier is employed. This enables to use more number of bits to represent the hidden data. The authors in use audio signals as the cover media to hide the sensitive data. In the authors present two techniques to hide data in the audio signals. In the first method before hiding the data in the LSB of the sample of the audio signal the parity of the sample checked. This method makes the attacker difficult to guess the transmitted data. In the second approach, the LSB‟s are XOR’ed and depending on the result of this operation and the hidden data the LSB of the sample data is decided to be changed or left unchanged. In a separate approach is followed where in the stereo audio signals are used to embed the data. In the proposed algorithm the polarity of reverberations is applied to the high frequency signals which are then replaced by one middle channel to embed the critical data. Jigsaw-based approach is used to transfer data over the communication channel securely. In this scheme the data is fragmented in block of variable sizes and a message authentication code (MAC) is used to authenticate each and every piece of data. Also, every message is prefixed and suffixed with a binary 1 along with XOR-ing the data with the randomly generated one-time pad. By fragmenting the data the attacker is unable to make sense of the data at the same time he cannot access the data unless he possess the authentication code for the data. A diverse approach is followed by the authors in [21]. In this scheme the redundant fields in the IPv4 header is exploited to mask the data. The fragment bit of FLAGS and the 16-bit identification fields are utilized to pass the delicate data over the communication network.

**Chapter 3**

**PROPOSED WORK**

* 1. **Basic Idea :-**

The basics of data rely on three different facts i.e. capacity, security, and robustness. Capacity means the media on which the data is to be hidden should hold the data, so that the complexity of the medium should not be disturbed. Security means the embedding algorithm is said to be secure if the embedded information cannot be removed beyond reliable detection by targeted attacks. Finally, robustness means the amount of manipulation a cover image (original image) can handle without drawing any attention that a change has taken place. Steganography and cryptography have to guarantee any of the requirements.

**3.2 Methodology:-**

Proposed Methodology has been divided in 2 Phases:-

1) Data Hiding

2) Data Extraction

**1) Data Hiding:-**

In this phase, we split the image in different parts. Then intensity of the image gets check to find whether it is closer to darkness or brightness. If it is closer then that image sample will be selected for hiding the data. For hiding the secrete data, firstly data is encrypted with shifting method and then segmented into equal parts. After that each data segment is hiding behind the specific sample of image. At last all the samples are concatenated which will give the stego image.

Encrypted Segments

Input Image

Higher LSB Data Hiding

Stego Image

Figure 3.1: Architecture for Data hiding.

**Algorithm for Data hiding:-**

1. *Select an Image*
2. *Image Preparation & Extract features.*
3. *Encrypt features.*
4. *Select carrier image.*

*Hide Secrete images into carrier image at 1 to 6 LSB position based.*

1. *Stop.*

**3.2. Data Flow Diagram:-**

Start

Select an Image

Image Preparation & Extract features

Encrypt features

Select Carrier Image

Higher LSB Data Hiding Method 1 to 6 bit

Stego Image

Stop

Figure 3.2: Flow diagram for Data hiding in an Image.

**2) Data Extraction:-**

In this phase, whatever the data is hidden in first phase that is being extracted. Following steps will be performed:-

1. First Split the image.
2. Extract the data segment from image samples.
3. Decrypt the data segments.
4. Assemble the data obtain from data segment.

At last plain text will be obtain from the assembled data that is required secrete data.

Stego Image

Higher LSB Data Extraction

Payload

Figure 3.3: Architecture for Data Extraction

**Algorithm for Data Extraction:-**

1. *Select a Stego Image.*
2. *Split stego Image.*
3. *Apply Higher LSB 1 to 6 bit Extraction algorithm.*
4. *Select length Key.*
5. *Extract data bits from 1 to 6 LSB color pixels bits.*
6. *Generate Data.*
7. *Decrypt Data.*
8. *Stop*

Start

Select Stego Image

Split Stego Image

XOR Keys

Higher LSB 1 to 6 bit Extraction Algorithm

Extracted data

POSITION Keys

Shift Encryption Algorithm

Decrypted Data

Stop

Figure.3.4: Flow diagram for Data Extraction form Image.

**Algorithm for Decryption:-**

1. *Select Stego Image.*
2. *Extract encrypted image.*
3. *Decrypt Image.*
4. *Generate Original Image.*
5. *Stop.*

Select Stego Image

Extract Encrypted Image

Decrypt Image

Generate Original Image

Stop

Figure.3.5: Flow diagram for Decryption.