# A REAL TIME IMPLEMENTATION OF DATA HIDING IN AUDIO FOR MILITARY APPLICATIONS

**CH. NAGA CHAITANYA** [1], **A. NITHIN** [2], **B. HARITH KUMAR REDDY** [3], **CH. HEMANTH KUMAR REDDY** [4]

Department of Electronics and Communication Engineering

RISE Krishna Sai Prakasam Group of Institutions; JNTU KAKINADA

(chandavoluchaitanya@gmail.com [1], andranithin703@gmail.com [2] , harithkumarbhumireddy@gmail.com [3], hemanthreddychalla04@gmail.com [4])

**ABSTRACT-** In this paper we propose Secret communication through Audio with Textual Information using Steganography method. Steganography is an art of sending hidden data or secret messages over a public channel so that a third party cannot detect the presence of the secret messages. The goal of steganography is different from classical encryption, which seeks to conceal the content of secret messages; steganography is about hiding the very existence of the secret messages. Modern steganography is generally understood to deal with electronic media rather than physical objects. There have been numerous proposals for protocols to hide data in channels containing pictures, video, audio and even typeset text. This makes sense for a number of reasons.

## INTRODUCTION-

As the development of Internet technologies increases, the transmission of digital media is now-a-days convenient over the networks. But secret message transmissions over the Internet system suffer from serious security overhead. So, protecting of secret messages during transmission becomes an important issue. Though cryptography changes the message so that it cannot be understood but this can generates curiosity level of a hacker. It would be rather more sensible if the secret message is cleverly embedded in another media so that no one can guess if anything is hidden there or not. This idea results in steganography, which is a branch of information hiding by camouflaging secret information within other information.The word steganography in Greek means "covered writing" ( Greek words "stegos" meaning "cover" and "grafia" meaning "writing") [1]. The main objective of steganography is to hide a secret messageinside harmless cover media in such a way that the secret message is not visible to the observer. Thus the stego_image should not diverge much from original cover image. In this generation, steganography is mostly used on computers with digital data being the carriers and networks being the high speed delivery channels.

The advantage of steganography, over cryptography alone, is that messages do not attract attention to themselves. Plainly visible encrypted messages—no matter how unbreakable—will arouse suspicion, and may in themselves be incriminating in countries where encryption is illegal. Therefore, whereas cryptography protects the contents of a message, steganography can be said to protect both messages and communicating parties.

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 to correspond to a letter in the alphabet, a change so subtle that someone not specifically looking for it is unlikely to notice it.

Among all digital file formats available nowadays image files are the most popular cover objects because they are easy to find and have higher degree of distortion tolerance over other types of files with high hiding capacity due to the redundancy of digital information representation of an image data.

## 1.2 Applications digital stegonography

Stegonography is not restricted to just hide information of the author in the work, there are various other purposes for which watermarking may be incorporated into an object. Some of them are

Ø Copyright Protection : For the protection of intellectual property, the data owner can embed a stegono representing the copyright information in his data.

Ø Fingerprinting: To trace the source of illegal copies, the owner can use a fingerprinting technique. This requires the owner to embed different information onto copied of the work provided to different customers. The information embedded can be a serial number, customer id etc.

Ø Data Authentication: Introducing fragile stego into the data can help ensure that the data is not processed or modified in anyway by the user.

Ø Indexing: Introducing watermarks in video mail, movies, news items can be used to index the data.

Ø Data Hiding: stego may be used to embed longer bits of information in the data. The earliest form of this is was in ancient Greece, where an author could hide his name in the text of the literary work. The term used to describe data hiding ,'LSB techinique'originated in Greece. This was also used by the Germans/Allies in WWII to send sensitive information to outposts by hiding it in postcards.

Ø Medical Safety: Stego containing the name of the patient can be embedded onto the X-Rays, MRI Scans & other test results help in instant identification of the result as belonging to a patient and thus avoid mix-ups which can lead to catastrophic consequences.

Ø Robustness: Robustness is a measure of the ability of the embedding algorithm to introduce the watermark in such a way that it is retained in the image despite several stages of image processing. The image may be filtered ( high-pass or low-pass or median) rotated, translated, cropped , scaled etc. As part of image processing . A good watermarking algorithm embeds the stego in the spatial or frequency regions of the image, which would be least affected by such processing. Good correlation is possible between the recovered

Ø Security: Security of a stegotechnique can be judged the same way as with encryption techniques. Assuming that unauthorized parties know the algorithm used for the embedding, the security of the algorithm lies in the selection of key. Thus the algorithm is truly secure if knowing the exact algorithm to embed and extract data does not help an unauthorized party in actually recovering the data from the stego image.

Ø Payload of stego: The amount of information that can be stored in a stego depends on the application. For example, in copy protection purposes, a payload of one bit is more than sufficient. The latest proposal for audio stegonography standard specifies that an audio stegonography be at least 20 bits per second. (This is however almost impractical and so will be reduced to only a few bits ). For intellectual hide such as ISBN or ISRC a length of 60-70 bits would be sufficient. "stegonographygranularity" is a term used to refer to the number of bits that are actually needed to represent the entire stego in the image. Generally for video information the watermarking information can be spread over a few frames. Although this decreases the robustness, this approach still suffices for most applications.

## 1.3 Stegonography techiniques

There are a number of steganographic schemes that hide secret message in an image file; these schemes can be classified according to the format of the cover image or the method of hiding. We have two popular types of hiding
Methods; spatial domain embedding and transform domain embedding.

1.viisible stegonography

2.invisible stegonography

3.audio stegonography

4.image stegonography

5.video stegonography

Stegono graphy techiniques over view:

The first recorded uses of steganography can be traced back to 440 BC when Herodotus mentions two examples of steganography in The Histories of Herodotus. 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 were in common use then as reusable writing surfaces, sometimes used for shorthand. Another ancient example is that of 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

### 1.3.1 PHYSICAL STEGANOGRAPHY

Steganography has been widely used, including in recent historical times and the present day. Possible permutations are endless and known examples include:

- Hidden messages within wax tablets: in ancient Greece, people wrote messages on the wood, then covered it with wax upon which an innocent covering message was written.
- Hidden messages on messenger's body: also used in ancient Greece. Herodotus tells the story of a message tattooed on a slave's shaved 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 invasion plans. 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.

- In WWII, the French Resistance sent some messages written on the backs of couriers using invisible ink.
- Hidden messages on paper written in secret inks, under other messages or on the blank parts of other messages.
- Messages written in Morse code on knitting yarn and then knitted into a piece of clothing worn by a courier.
- Messages written on the back of postage stamps.
- During and after World War II, espionage agents used photographically produced microdots to send information back and forth. Microdots were typically minute, approximately less than the size of the period produced by a typewriter. WWII microdots needed to be embedded in the paper and covered with an adhesive (such as collodion). This was reflective and thus detectable by viewing against glancing light. Alternative techniques included inserting microdots into slits cut into the edge of post cards.
- During World War II, a spy for Japan in New York City, Velvalee Dickinson, sent information to accommodation addresses in neutral South America. She was a dealer in dolls, and her letters discussed how many of this or that doll to ship. The stegotext was the doll orders, while the concealed "plaintext" was itself encoded and gave information about ship movements, etc. Her case became somewhat famous and she became known as the Doll Woman.
- Cold War counter-propaganda. In 1968, crew members of the USS Pueblo (AGER-2) intelligence ship held as prisoners by North Korea, communicated in sign language during staged photo opportunities, informing the United States they were not defectors but rather were being held captive by the North Koreans. In other photos presented to the US, crew members gave "the finger" to the unsuspecting North Koreans, in an attempt to discredit photos that showed them smiling and comfortable.

### 1.3.2 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: Over 800 digital steganography applications have been identified by the Steganography Analysis and Research Center. Digital steganography techniques include:

- Concealing messages within the lowest bits of noisy 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 generates ciphertexts that look perfectly random if you don't have the private key).
- Chaffing and winnowing.
- Mimic functions convert one file to have the statistical profile of another. This can thwart statistical methods that help brute-force attacks identify the right solution in a ciphertext-only attack.
- Concealed messages in tampered executable files, exploiting redundancy in the targeted instruction set.
- Pictures embedded in video material (optionally played at slower or faster speed).
- Injecting imperceptible delays to packets sent over the network from the keyboard. Delays in keypresses in some applications (telnet or remote desktop software) can mean a delay in packets, and the delays in the packets can be used to encode data.
- Changing the order of elements in a set.
- Content-Aware Steganography hides information in the semantics a human user assigns to a datagram. These systems offer security against a non-human adversary/warden.
- Blog-Steganography. Messages are fractionalized and the (encrypted) pieces are added as comments of orphaned web-logs (or pin boards on social network platforms). In this case the selection of blogs is the symmetric key that sender and recipient are using; the carrier of the hidden message is the whole blogosphere.
- 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. The new representation of data is smaller in size. One of the possible schemes to achieve data compression is Huffman coding. Huffman coding assigns smaller length code words to more frequently occurring source symbols and longer length code words to less frequently occurring source symbols.

# INTRODUCTION TO SPEECH PROCESSING

## 2.1 Introduction to speech processing:

Since even before the time of Alexander Graham Bell's revolutionary invention, engineers and scientists have studied the phenomenon of speech communication with an eye on creating more efficient and effective systems of human-to-human and human-to-machine communication. Starting in the 1960s, digital signal processing (DSP), assumed a central role in speech studies, and today DSP is the key to realizing the fruits of the knowledge that has been gained through decades of research. Concomitant advances in integrated circuit technology and computer architecture have aligned to create a technological environment with virtually limitless opportunities for innovation in speech communication applications. In this chapter We present a comprehensive overview of digital speech processing that ranges from the basic nature of the speech signal. hence our goal is to provide a useful introduction to the wide range of important concepts that comprise the field of digital speech processing.

The fundamental purpose of speech is communication, i.e., the transmission of messages. According to information theory, a message represented as a sequence of discrete symbols can be quantified by its *information content* in bits, and the rate of transmission of information is measured in bits/second (bps). In speech production, as well as in many human-engineered electronic communication systems, the information to be transmitted is encoded in the form of a continuously varying (analog) waveform that can be transmitted, recorded, manipulated, and ultimately de coded by a human listener.

In the case of speech, the fundamental analog form of the message is an acoustic waveform, which we call the *speech signal*. Speech signals, as illustrated in Figure 1.1, can be converted to an electrical waveform by a microphone, further manipulated by both analog and digital signal processing, and then converted back to acoustic form by a loudspeaker, a telephone handset or headphone, as desired. This form of speech processing is, of course, the basis for Bell's telephone invention as well as today's multitude of devices for recording, transmitting, and manipulating speech and audio signals.

Although Bell made his invention without knowing the fundamentals of information theory, these ideas have assumed great importance in the design of sophisticated modern communications systems. Therefore, even though our main focus will be mostly on the speech waveform and its representation in the form of parametric models, it is nevertheless useful to begin with a discussion of how information is encoded in the speech waveform.

The purpose of speech is communication. There are several was of characterizing the communications potential of speech. One highly quantitative approach is in terms of information theory ideas as according to information theory, speech can be represented in terms of its message content, or information. An alternative way of characterizing speech is in terms of the signal carrying the message information, i.e., the acoustic waveform.

## 2.2 Digital Speech Processing

**Speech processing** is the study of speech signals and the processing methods of these signals.

The signals are usually processed in a digital representation, so speech processing can be regarded as a special case of digital signal processing, applied to speech signal.

Speech processing can be divided into the following categories:

- ❖ **Speech recognition**, which deals with analysis of the linguistic content of a speech signal.
- ❖ **Speaker recognition**, where the aim is to recognize the identity of the speaker.
- ❖ **Speech coding**, a specialized form of data compression, is important in the telecommunication area.
- ❖ **Voice analysis,** for medical purposes, such as analysis of vocal loading and dysfunction of the vocal cords.
- ❖ **Speech synthesis:** the artificial synthesis of speech, which usually means computer-generated speech.
- ❖ **Speech enhancement**: enhancing the intelligibility and/or perceptual quality of a speech signal, like audio noise reduction for audio signals.

The first step in most applications of digital speech processing is to convert the acoustic waveform to a sequence of numbers. Most modern A-to-D converters operate by sampling at a very high rate, applying a digital low pass filter with cut of set to preserve a prescribed bandwidth, and then reducing the sampling rate to the desired sampling rate, which can be as low as twice the cut of frequency of the sharp-cutoff digital filter.

This discrete-time representation is the starting point for most applications. From this point, other representations are obtained by digital processing. For the most part, these alternative representations are based on incorporating knowledge about the workings of the speech chain. As we will see, it is possible to incorporate aspects of both the speech production and speech perception process into the digital representation and processing. It is not an over-simplification to assert that digital speech processing is grounded in a set of techniques that have the goal of pushing the data rate of the speech representation to the left along either the upper or lower path.

## 2.3 Speech Coding

Perhaps the most widespread applications of digital speech processing technology occur in the areas of digital transmission and storage of speech signals. In these areas the centrality of the digital representation is obvious, since the goal is to compress the digital wave-form representation of speech into a lower bit-rate representation. It is common to refer to this activity as “speech coding” or “speech compression.

Because the digital representation at this point is often not directly related to the sampled speech waveform, $y[n]$ and $\hat{y}[n]$ are appropriately referred to as *data signals* that represent the speech signal. The lower path in Figure 1.2 shows the decoder associated with the speech coder. The received data signal $\hat{y}[n]$ is decoded using the inverse of the analysis processing, giving the sequence of samples $\hat{x}[n]$ which is then converted (using a D-to-A Converter) back to an analog signal $\hat{x}_c(t)$ for human listening. The decoder is often called a *synthesizer* because it must reconstitute the speech waveform from data that may bear no direct relationship to the waveform.

With carefully designed error protection coding of the digital representation, the transmitted ($y[n]$) and received ($\hat{y}[n]$) data can be essentially identical. This is the quiet essential feature of digital coding. In theory, perfect transmission of the coded digital representation is possible even under very noisy channel conditions, and in the case of digital storage, it is possible to store a perfect copy of the digital representation in perpetuity if sufficient care is taken to update the storage medium as storage technology advances.

This means that the speech signal can be reconstructed to within the accuracy of the original coding for as long as the digital representation is retained. In either case, the goal of the speech coder is to start with samples of the speech signal and reduce (compress) the data rate required to represent the speech signal while maintaining a desired perceptual fidelity. The compressed representation can be more efficiently transmitted or stored, or the bits saved can be devoted to error protection.

Speech coders enable a broad range of applications including narrowband and broadband wired telephony, cellular communications, voice over internet protocol (VoIP) (which utilizes the internet as a real-time communications medium), secure voice for privacy and encryption (for national security applications), extremely narrowband communications channels (such as battlefield applications using high frequency (HF) radio), and for storage of speech for telephone answering machines, interactive voice response (IVR) systems, and pre-recorded messages. Speech coders often utilize many aspects of both the speech production and speech perception processes, and hence may not be useful for more general audio signals such as music.

Coders that are based on incorporating only aspects of sound perception generally do not achieve as much compression as those based on speech production, but they are more general and can be used for all types of audio signals. These coders are widely deployed in MP3 and AAC players and for audio in digital television systems.

## Speech recognition

Another large class of digital speech processing applications is concerned with the automatic extraction of information from the speech signal. Most such systems involve some sort of pattern matching. Figure 1.3 shows a block diagram of a generic approach to pattern matching problems in speech processing. Such problems include the following: speech recognition, where the object is to extract the message from the speech signal; speaker recognition, where the goal is to identify who is speaking; speaker verification, where the goal is to verify a speaker's claimed identity from analysis of their speech

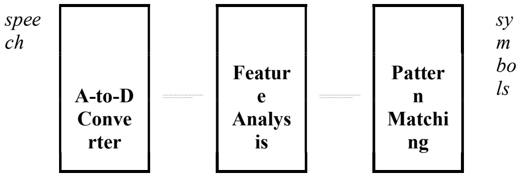

**Fig. 2.3 : Block diagram of general pattern matching system for speech signals.**

signal; word spotting, which involves monitoring a speech signal for the occurrence of specified words or phrases; and automatic indexing of speech recordings based on recognition (or spotting) of spoken keywords.

The first block in the pattern matching system converts the analog speech waveform to digital form using an A-to-D converter. The feature analysis module converts the sampled speech signal to a set of feature vectors. Often, the same analysis techniques that are used in speech coding are also used to derive the feature vectors. The final block in the system, namely the pattern matching block, dynamically time aligns the set of feature vectors representing the speech signal with a concatenated set of stored patterns, and chooses the identity associated with the pattern which is the closest match to the time-aligned set of feature vectors of the speech signal. The symbolic output consists of a set of recognized words, in the case of speech recognition, or the identity of the best matching talker, in the case of speaker recognition, or a decision as to whether to accept or reject the identity claim of a speaker in the case of speaker verification.

Although the block diagram of Figure 1.3 represents a wide range of speech pattern matching problems, the biggest use has been in the area of recognition and understanding of speech in support of human– machine communication by voice. The major areas where such a system finds applications include command and control of computer software, voice dictation to create letters, memos, and other documents, natural language voice dialogues with machines to enable help desks and call centers, and for agent services such as calendar entry and update, address list modification and entry, etc.

Pattern recognition applications often occur in conjunction with other digital speech processing applications. For example, one of the preeminent uses of speech technology is in portable communication devices. Speech coding at bit rates on the order of 8 Kbps enables normal voice conversations in cell phones. Spoken name speech recognition in cell phones enables voice dialing capability that can automatically dial the number associated with the recognized name. Names from directories with upwards of several hundred names can readily be recognized and dialed using simple speech recognition technology.

Another major speech application that has long been a dream of speech researchers is *automatic language translation.* The goal of language translation systems is to convert spoken words in one language to spoken words in another language so as to facilitate natural language voice dialogues between people speaking different languages. Language translation technology requires speech synthesis systems that work in both languages, along with speech recognition (and generally natural language understanding) that also works for both languages; hence it is a very dificult task and one for which only limited progress has been made. When such systems exist, it will be possible for people speaking different languages to communicate at data rates on the order of that of printed text reading!

## 2.5 Speech Processing Applications

The range of speech communication applications is illustrated in Figure 1.4. As seen in this figure, the techniques of digital speech processing are a key ingredient of a wide range of applications that include the three areas of transmission/storage, speech synthesis, and speech recognition as well as many others such as speaker identification, speech signal quality enhancement, and aids for the hearing- or visually-impaired.

usually achieved by transforming the speech signal into an alternative representation (that is motivated by our understanding of speech production and speech perception), operating on that representation by further digital computation, and then transforming back to the wave-form domain, using a D-to-A converter.

One important application area is *speech enhancement*, where the goal is to remove or suppress noise or echo or reverberation picked up by a microphone along with the desired speech signal. In human-to-human communication, the goal of speech enhancement systems is to make the speech more intelligible and more natural; however, in reality the best that has been achieved so far is less perceptually annoying speech that essentially maintains, but does not improve, the intelligibility of the noisy speech. Success *has* been achieved, however, in making distorted speech signals more useful for further processing as part of a speech coder, synthesizer, or recognizer.

# LITERATURE SURVEY

## 3.1 DATA ENCRYPTING IN A BINARY IMAGE BASE ON MODIFIED DATA HIDING METHOD

This encryption method manipulates sub-divided blocks using modified bit position to replace a secret bit. The sub-divided block contains three or more pixels of the host binary image. For every block decides to hide a secret bit. By finding the pixel position to insert a secret bit for each block, the image quality of the overt binary image can be improved.

## 3.2 ENCRYPTING PROCESSES

### 3.2.1 MODIFIED DATA HIDING METHOD

Let H be the host binary image of MXN pixels and C be the mXn-bit secret data. For pixel value h(i,j) of H, a new pixel value is defined as h'(i,j). The following processes are executed to hide a data bit.

1. For a given H. Select a sub-divided block Buv with size pXq for hiding a secret data bit.
2. Summing all pixels of Buv.
3. If **S**(**B**uv) is equal to 0 or pXq, is not used to store a secret data bit in the block.
4. If mod(**S**(**B**uv),2) is equal to the **C**(z), then do not make a change and save the data bit in this block.
5. If mod(**S**(**B**uv),2) is not equal to the **C**(z),

### 3.2.2 ENCRYPTING PROCESSES

Let **H** be a host binary image and let **H*** be an overt binary image modified from **H**. The elements of the overt image **H*** contain encrypted codes and the codes are classified into five groups of codes. The identification codes are used to determine if the codes encrypted in **H*** use the encrypted method proposed in this paper or not; the initial position codes are used to assign the initial position of the top-left of the sub-divided block; the sub-divided block dimension codes are used to indicate the size of the sub-divided block; the covert binary image dimension codes are used to indicate the size of the covert binary image; (all the above-mentioned codes locate at the first row to the second one of **H***) the information codes are used to decrypt covert binary image (locate at the third row to the last one of **H***). Identification codes are like passwords and they are used to determine whether an overt image contains codes proposed in this paper or not.

Identification codes are composed of 20-bit of pseudo-random binary codes, e.g. 10011000010000100001. Initial position codes are used to assign the initial position of the top-left of the sub-divided block and they need two sets of 4-bit binary codes. The first set shows the number of the row position and the second set shows the number of the column position. The codes 0000, 0011, 0111, and 1111 are used to represent number of 1, 4, 8, and 16, respectively. Other number codes can be used similarly.

**MERITS**

- PSNR value was high.
- Easy to encrypt binary image.

**DEMERITS**

- If there was any change in the binary information, we cannot reconstruct the encrypted data

## 3.3 VISUAL CRYPTOGRAPHIC STEGANOGRAPHY IN IMAGES

Cryptography involves converting a message text into an unreadable cipher. On the other hand, steganography embeds message into a cover media and hides its existence. Both these techniques provide some security of data neither of them alone is secure enough for sharing information over an unsecure communication channel and are vulnerable to intruder attacks. In this paper we propose an advanced system of encrypting data that combines the features of cryptography, steganography along with multimedia data hiding. This system will be more secure than any other these techniques alone and also as compared to steganography and cryptography combined systems.

**1. Encryption Algorithm:** The message will first be encrypted using Asymmetric Key Cryptography technique. The data will be encrypted using basic DES algorithm. This cipher will now be hidden into a multimedia file. The cipher will be saved in the image using a modified bit encoding technique by truncating the pixel values to the nearest zero digit (or a predefined digit) and then a specific number which defines the 3-D representation of the character in the cipher code sequence can be added to this number. For every character in the message a specific change will be made in the RGB values of a pixel. (This change should be less than 5 for each of R, G and B values) This deviation from the original value will be unique for each character of the message. This deviation also depends on the specific data block (grid) selected from the reference database. For each byte in the data one pixel will be edited. Thus one byte of data will be stored per pixel in the image. In this method the cipher sequence can be decoded without the original image and only the edited image will be transmitted to the receiver. In the first few lines of image properties, the attributes of the image will be encrypted and saved so as to provide us the information if the image is edited or modified or the image extension has been changed like jpg to gif. These properties can be used in the decoding (identifying the correct block of data from the data grid). So only the correct encrypted image in the correct format will produce the sent message. For decryption, the receiver must know which image to decode and in which format as changing the image format changes the color distribution of the image. Every image gives a random data on decryption that has no meaning. But only the correct format decryption gives the original message. After hiding the data in the image, the image will be sent to the receiver. The receiver should have the decryption key (private key) which will be used to decode the data.

**2. Decryption Algorithm:** The message can be decoded using an inverse function (as used in traditional techniques) using the receiver's private key. This key can be a part of the image or a text or any attribute of the image. The receiver's private key is used to identify the reference grid from the reference database. After selecting the correct grid, the x and y component of the image can define the block that has been used to encrypt the message and the RGB values can point to the data in the block identified by the x, y component. The cipher is retrieved by obtaining the difference in the pixel value from the closest predefined value (zero truncation). These numbers will now define the saved bit and will form the cipher text. This cipher can now be decrypted using an inverse function of the DEA algorithm to get the message text.

**MERITS**

- We can hide text data in any image.
- Easy to handle.

**DEMERITS**

- Easy to hack.
- Computational complexity was high.

## 3.4 IMAGE STEGANOGRAPHY USING MOD-4 EMBEDDING ALGORITHM BASED ON IMAGE CONTRAST

In order to improve the capacity of the hidden secret data and to provide an imperceptible stego image quality, a new image steganography method based on image contrast is presented. A group of 2×2 blocks of non-overlapping spatially adjacent pixels is selected as the valid block for embedding the secret message. The modulo 4 arithmetic operation is further applied to all the valid blocks to embed a pair of binary bits using the shortest route modification scheme. Each secret message is also encrypted by RSA encryption algorithm to provide the system with more security.

Encryption: In this section we propose a RSA public key encryption for encrypting the secret message before embedded into cover image. RSA can be used for both encryption and decryption. In public key encryption the sender will use the public key during the encoding process and only the private key, which has a direct mathematical relationship with the public key, can decipher the secret message. Public key encryption is the most secure type of steganography. It also has multiple levels of security in that unwanted parties must first suspect the use of steganography and then they would have to find a way to crack the algorithm used by the public key system before they could intercept the secret message.

**Data Hiding:** In this section we propose a mod-4 embedding method for information hiding within the spatial domain of any gray scale image. This method can be considered as the improved version of. The input messages can be in any digital form, and are often treated as a bit stream. Embedding pixels are selected based on some mathematical function which depends on the pixel intensity value of the valid blocks in an image. Before embedding a checking has been done to find out whether the selected embedding pixels lies at the boundary of the image or not. Data embedding are done by mapping each two bits of the secret message in each of the valid block based on some features of that pixel.

**Data Hiding Model:** The input messages can be in any digital form, and are often treated as a bit stream. The input message is first converted into encrypted form through proposed encryption method. This encrypted message generates the secret key which may be used as a password before starting of the embedding or extracting operation for increasing another level of security. Second the image is reshaped to the 2×2 blocks of non-overlapping spatially adjacent pixels. Then the valid blocks are selected from these blocks. Block Q is valid if the average difference between the gray level values of the pixels of that and it's mean (C) exceeds a threshold (minimum contrast)

**MERITS**

- Image contrast was enhanced and data was hidden.

- We cannot identify the given image was data hidden image.

**DEMERITS**

- For improving contrast, the pixel values in the given image were changed. This makes change in the data.
- Data bits in the image can change.

## 3.5 IMPLEMENTATION AND ANALYSIS OF THREE STEGANOGRAPHIC APPROACHES

This paper proposes the enhance security system by combining these two techniques. In this system, the encrypted message is embedded in a BMP image file. In proposed system, three LSB steganographic techniques have been implemented and analyzed. This proposed system intends for data confidentiality, data authentication and data integrity. This system not only enhances the security of data but also becomes more powerful mechanism. This system intends to support effective ways for protecting data. The primary goal of our system is to enhance the security of data and then to compare three steganographic techniques. Then we will use the optimized method for embedding. In this paper, we just present three steganographic approaches. In this system, data is encrypted with RC4 encryption algorithm and then embedded the encrypted text in the BMP image file using three steganogrpaphic methods.

**RC4 Encryption Algorithm:** In this paper, we use RC4 encryption algorithm. It is a variable key size cipher and symmetric key algorithm. Variable key size is from 1 to 256 bit to initialize a 256 bit state table. State table is used for subsequent generation of pseudo-random bits and then to generate a pseudo-random stream. The algorithm has two stages: initialization and operation.

**RIPEMD-160 hashing function:** Hash algorithms are important components in many cryptographic applications and security protocol suites. Hah functions, also called message digests and one way encryption, use no key. They are also employed by many operating systems to encrypt passwords. Therefore, it provides a measure of the integrity of a file. In this paper, we use RIPEMD-160 hash algorithms to provide higher protection. RIPEMD-160 has been designed by Hans Dobbertin, Antoon Bosselaers and Bart Preneel and produces a 160 bit output after performing five independent rounds. Each round is composed of 16 iterations resulting in 80 iterations in total.

**MERITS**

- This system uses cryptography and steganography to enhance the security. By combining these two techniques, it can enhance confidentiality and integrity of information.

**DEMERITS**

- Computation cost was high.
- Time complexity was high.

## 3.6 REVERSIBLE DATA HIDING IN ENCRYPTED IMAGE

This work proposes a novel reversible data hiding scheme for encrypted image. After encrypting the entire data of an uncompressed image by a stream cipher, the additional data can be embedded into the image by modifying a small proportion of encrypted data. With an encrypted image containing additional data, one may firstly decrypt it using the encryption key, and the decrypted version is similar to the original image.

A content owner encrypts the original uncompressed image using an encryption key to produce an encrypted image, and then a data-hider embeds additional data into the encrypted image using a data-hiding key though he does not know the original content. With an encrypted image containing additional data, a receiver may firstly decrypt it using the encryption key, and the decrypted version is similar to the original image. According to the data-hiding key, he can further extract the embedded data and recover the original image from the decrypted version.

**Image Encryption:** Assume the original image is in uncompressed format and each pixel with gray value falling into [0, 255] is represented by 8 bits. Denote the bits of a pixel as $b_{i,j,0}$,$b_{i,j,1}$,…,$b_{i,j,7}$ where indicates the pixel position, and the gray value as $p_{i,j}$.

**Data Embedding:** With the encrypted data, although a data-hider does not know the original image content, he can embed additional message into the image by modifying a small proportion of encrypted data.

**Data Extraction and Image Recovery:** When having an encrypted image containing embedded data, a receiver firstly generates $r_{i,j,k}$ according to the encryption key, and calculates the exclusive-or of the received data and $r_{i,j,k}$ to decrypt the image. We denote the decrypted bits as $b_{i,j,k}$.

**MERITS**

- High security.
- Computational complexity was low.

**DEMERITS**

- Since there was no separate key for data decode and decryption, any person can retrieve data and image if he got encrypted key.

## EXISTING SYSTEM

### 4.1 Cryptography:

Cryptography is an art of protecting the information by transforming into an unreadable and untraceable format known as cipher text. Only the person who possess the secret key can decipher or we can say decrypt the message into the original form. Cryptography is the technique by which one can send and share the information in a secret manner. Due the cryptography the information seems to be appearing like a garbage value and it is always almost impossible to find the information content lying under the image or a video file. The information looks like hidden inside the image or the video file. A very simplest and well known algorithm for cryptography is as shown in fig 2. The encryption key generator is used to generate the encryption key as well as the public key as shown in the below block diagram. By using the encryption key the information content to be sent gets encrypted by the encryptor. The encrypted information is then transmitted to the particular receiver. At the receiver end the cryptography decryptor is used which extracts the original information content mapped onto the image or a video file with the help of a public key provided by the transmitter section. By the use of the cryptography method only, the receiver which has the knowledge of the public key can retrieve the original information content from the image or a video file. So even if any unwanted person or a source gets the image or a video file with information content hidden in it, it cannot be extracted without proper public key. So public key plays a vital role in the whole cryptography process.

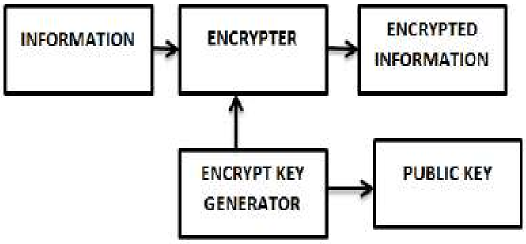

Fig.4.1. Cryptography encrypter

Technically in simple words "cryptographymeans hiding one piece of data within another". Modern cryptographyuses the opportunity of hiding information into digital multimedia files and also at the network packet level. Hiding information into a media requires following

elements. The cover media(C) that will hold the hidden data

- The secret message (M), may be plain text, cipher text or any type of data
- The stego function (Fe) and its inverse (Fe-1)
- An optional stego-key (K) or password may be used to hide and unhide the message .

Cryptography is the art or study of hiding information by inserting secret messages in other messages. Medium where information is inserted can be anything. This medium is called the cover object. Cryptography that is applied to hide information on the cover of digital objects is called Digital Cryptography. Cover objects that are used in digital cryptography can vary, for example in the image archive. Cryptography algorithms in the image archive have been widely developed. Meanwhile, cryptography algorithms in audio archive are relatively few. In recent years there are so many algorithm have been developed to provide more security, enhanced quality with easy implementation and faster calculations. Among them all of the techniques have their own drawbacks like computational complexity, time consumption and reconstruction of secret information etc., Here, in this proposal we implemented pixel mapping based video steganography, which is a very simple and easy calculations and also provide more security.

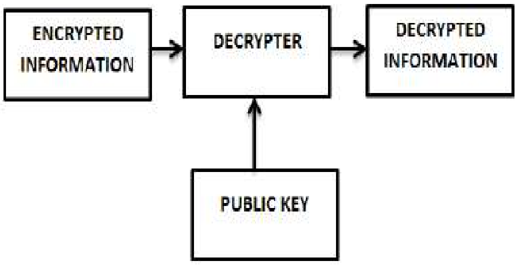

Fig.4.2.Cryptography decrypter

**Draw backs:**

1) Security is low.

2) Maximum capacity of data transfer does not possible.

3)In cryptography, in the encryption process, by using public key, any person can easily know the information.

4)In cryptography, we can hide the data and we can also know the data by applying reverse process

# Proposed system

## 5.1 Proposed system

A survey of steganographic techniques reveals that there have been several techniques for hiding information or messages in host messages in such a manner that the embedded data should be imperceptible.

Substitution system substitutes redundant parts of a cover with a secret message.

Spread spectrum techniques adopt ideas from spread spectrum communication. The statistical method encodes information by changing several statistical properties of a cover and use hypothesis testing in the extraction process. Distortion process stores information by signal distortion and measure the deviation from the original cover in the decoding step.

The cover generation method encodes information in the way a cover for secret communication is created. In case of hiding information in digital sound, phase Coding embeds data by altering the phase in a predefined manner. To a certain extent, modifications of the phase of a signal cannot be perceived by the human auditory system (HAS).

All these steganographic techniques deal with a few common types of steganography procedure depending on the variation of the host media. That means the cover object or the carrier object which will be used to hide the secret data. Different media like image, text, video and audio has been used as a carrier or host media in different times.

Using audio file as a cover object directs to Audio steganography. Practical audio embedding systems face hard challenges in fulfilling all three requirements due to the large power and dynamic range of hearing, and the large range of audible frequency of the .

The human auditory system (HAS) perceives sounds over a range of power greater than 109:1 and a range of frequencies greater than 103:1. The sensitivity of the HAS to the Additive White Gaussian Noise (AWGN) is high as well; this noise in a sound file can be detected as low as 70 dB below ambient level. On the other hand, opposite to its large dynamic range, HAS contains a fairly small differential range, i.e. loud sounds generally tend to mask out weaker sounds.

Additionally, HAS is insensitive to a constant relative phase shift in a stationary audio signal and some spectral distortions interprets as natural, perceptually non-annoying ones. Two properties of the HAS dominantly used in steganographic techniques are frequency masking and temporal masking.

The concept using the perceptual holes of the HAS is taken from wideband audio coding (e.g. MPEG compression 1, layer 3, usually called mp3). In the compression algorithms, the holes are used in order to decrease the amount of the bits needed to encode audio signal, without causing a perceptual distortion to the coded audio. On the other hand, in the information hiding scenarios, masking properties are used to embed additional bits into an existing bit stream, again without generating audible noise in the audio sequence used for data hiding.

Some of the audio steganographic techniques are Lossless Adaptive Digital Audio Steganography, LSB based Audio Steganography, Audio Steganography using bit modification etc.

Some of the considerations to be kept in mind for efficient steganography techniques

- ❖ The cover media should not be degraded by the embedded data.
- ❖ It should appear that the cover media does not look distorted. It should not have a noticeable change in color composition, or that of the luminance. Frequently a cover media's size becomes enlarged; this can look very suspicious.
- ❖ Embedded data should be directly embedded into the cover media not in the header or wrapper. The embedded data needs to remain intact across different file formats.
- ❖ The embedded data should be immune to any manipulation. This ranges from any intentional modification or any modification through transmission.
- ❖ Error correcting codes should be inserted in the cover media to ensure integrity of data when or if the cover media is modified or tampered with.
- ❖ The embedded data should be recoverable and intact if only fragments of the cover media remain.

## 5.2 LSB based Audio Steganography

In the current Endeavour, an audio file with ".wav" extension has been selected as host file. It is assumed that the least significant bits of that file should be modified without degrading the sound quality. To do that, first one needs to know the file structure of the audio file. Like most files, WAV files have two basic parts, the header and the data. In normal wav files, the header is situated in the first 44 bytes of the file. Except the first 44 bytes, the rest of the bytes of the file are all about the data. The data is just one giant chunk of samples that represents the whole audio. While embedding data, one can't deal with the header section. That is because a minimal change in the header section leads to a corrupted audio file.

A program has been developed which can read the audio file bit by bit and stores them in a different file. The first 44 bytes should be left without any change in them because these are the data of the header section.

Then start with the remaining data field to modify them to embed textual information. For example, if the word “Audio” has to be embedded into an audio file one has to embed the binary values of the word “Audio” into the audio data field.

Consider the following table:

**TABLE 5.1**

**LETERS WITH ASCII VALUES AND CORRESPONDING BINARY VALUES :**

| **Letter** | **ASCII Value** | **Corresponding Binary Value** |
|---|---|---|
| A | 065 | 01000001 |
| U | 117 | 01110101 |
| D | 100 | 01100100 |
| I | 105 | 01101001 |
| O | 111 | 01101111 |

From the table, one can come to a point that to embed the word “Audio” into the host audio file actually the corresponding eight bit binary values have to be embedded into the data field of that audio file.

## 5.3 BLOCK DIAGRAMS:

### EMBEDDING PROCESS:

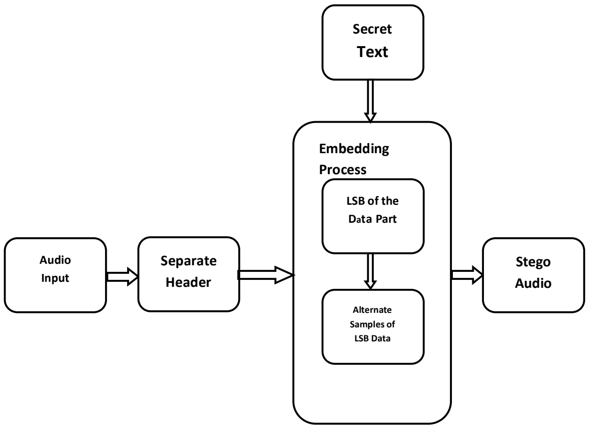

**FIG.5.1 : Block diagram of embedding process**

### EXTRACTION PROCESS:

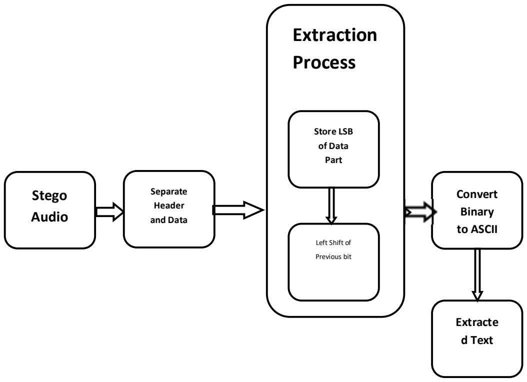

**FIG 5.2: Block diagram of Extraction Process**

### 5.3.1 EMBEDDING PROCESS DESCRIPTION:

By considering the Block diagram of embedding process, an audio file named “audio.wav” has been selected for this experiment in the first block of the embedding process. After checking the binary values of each sample, the samples were separated as first 44 samples were left without any changes for the header of the audio and remaining samples were left for the data part of the audio file.An audio file named “audio.wav” has been selected for this experiment. After checking the binary values of each sample, first 44 samples were left without any changes.

The data embedding with LSB modification has been started after the header section. If the data embedding process is started from 51st sample then the LSB value of the 51st sample should be modified. If the binary value of the corresponding sample is “01110100” then “1” should be modified. From Table I it can be observed that to

embed the letter “A”, the sender has to embed the binary value “01000001”. That is why according to the embedding algorithm “A” should be embedded according to Table 5.1.

**SAMPLES OF AUDIO FILE WITH BINARY VALUES BEFORE AND AFTER EMBEDDING**

| Sample No. | Binary values to corresponding samples | Binary value to be embedded | Binary values after modification |
|---|---|---|---|
| 51 | 01110100 | 0 | 01110100 |
| 53 | 01011110 | 1 | 01011111 |
| 55 | 10001011 | 0 | 10001010 |
| 57 | 01111011 | 0 | 01111010 |
| 59 | 10100010 | 0 | 10100010 |
| 61 | 00110010 | 0 | 00110010 |
| 63 | 11101110 | 0 | 11101110 |
| 65 | 01011100 | 1 | 01011101 |

According to the same way the remaining consecutive letters of the word “Audio” is embedded in the file “audio.wav.”

Editing of the existing binary values with the intended binary values causes a minimal change in the audio file “audio.wav” that remains almost imperceptible to anyone other than the sender. When it comes to the point of data retrieving at the receiver’s end, the retrieving algorithm has to be followed:

**Algorithm (For Embedding of Data):**

- Leave the header section of the audio file untouched...

• Start from a suitable position of the data bytes. (For the experiment purpose the present start byte was the 51st byte). Edit the least significant bit with the data that have to be embedded.

• Take every alternate sample and change the least significant bit to embed the whole message. The data retrieving algorithm at the receiver's end follows the same logic as the embedding algorithm.

First, change the audio message into binary format that has come from the source as stego-object. Leave first 50 bytes with no change in them. Start from 51st bit, check the least significant bit, and store it in a queue. Check every alternate sample to collect the whole messages. Like 53rd, 55th and 57th and so on. Store the least significant bits of the alternate samples in the queue with left shift of previous bit. Convert the binary values to decimal to get back the ASCII from which the text can be retrieved. The whole retrieval process can be depicted with the following table more thoroughly:

The data embedding with LSB modification has been started after the header section. If the data embedding process is started from 51st sample then the LSB value of the 51st sample should be modified. If the binary value of the corresponding sample is "01110100" then "1" should be modified. It can be observed that to embed the letter "A", the sender has to embed the binary value "01000001". That is why according to the embedding algorithm "A" should be embedded.

According to the same way the remaining consecutive letters of the word "Audio" is embedded in the file "audio.wav."

Editing of the existing binary values with the intended binary values causes a minimal change in the audio file "audio.wav" that remains almost imperceptible to anyone other than the sender.

The output of the embedding process after embedding the audio file of .wav extension with respect to the AUDIO text file is named as stego audio.

Thus the basic steps taken here are firstly selecting the audio file of .wav format and separating the header and data of the audio with corresponding samples. Then by considering the text which has to be embedded has to be embedded corresponding to the LSB of the audio samples by modifying the bits. The embedded audio file is finally represented as a Stego Audio.

### 5.3.2 EXTRACTION PROCESS DESCRIPTION :

When it comes to the point of data retrieving at the receiver's end, the retrieving algorithm has to be followed:

First, change the audio message into binary format that has come from the source as stego-object. Leave first 50 bytes with no change in them. Start from 51st bit, check the least significant bit, and store it in a queue. Check every alternate sample to collect the whole messages. Like 53rd, 55th and 57th and so on. Store the least significant bits of the alternate samples in the queue with left shift of previous bit. Convert the binary values to decimal to get back the ASCII from which the text can be retrieved. The whole retrieval process can be depicted with the following table more thoroughly:

In the embedding process of the letter "A" was stated that is why, the retrieval process of "A" is depicted. Starting from the 51st sample, every alternate sample has been checked and the least significant bit has been stored into a queue with a left shift of previous bit.

After getting all the bits in the queue, start from the left hand side, take 8 bits and convert them into equivalent decimal to get the ASCII, from the ASCII retrieve the embedded textual message.

## 5.4 EXRACTION OF DATA FROM AUDIO FILE:

**Algorithm (For Extracting of Data):**

•Leave first 50 bytes.

• Start from the 51st byte and store the least significant bit in a queue.

• Check every alternate sample and store the least significant bit in the previous queue with a left shift of the previous bit.

• Convert the binary values to decimal to get the ASCII values of the secret message.

• From the ASCII find the secret message.

| Sample No. | Binary values with embedded secret data | Bits that are stored in the Queue |
|---|---|---|
| 51 | 01110100 | 0 |
| 53 | 01011111 | 01 |
| 55 | 10001010 | 010 |
| 57 | 01111010 | 0100 |
| 59 | 10100010 | 01000 |
| 61 | 00110010 | 010000 |
| 63 | 11101110 | 0100000 |
| 65 | 01011101 | 01000001 |

From the extraction process, it is clearly observed that after getting 01000001 in the queue it is converted into the equivalent decimal that is 65, the ASCII of “A”. Thus “A” is retrieved. Like the same way, the next letters also have been retrieved and hence the complete word “Audio.”

Thus the basic steps taken here is to considering the stego audio and separating the header and data samples and storing the LSB of the stego audio data part in a queue and left shifting the corresponding previous bits of the sample.then the final data from the queue is converted in to the ASCII with respect to the binary values of the sample in the queue and the text is extracted.

To develop this algorithm multiple bits of each sample of the file have been changed or modified to insert text data in it. It has also been observed the degradation of the host audio file after modification of the bits. The bit modification was done by various ways, like 1, 2, 3, 4 bits were changed in turn. But after going through all the modification it has been observed that 1 bit change in LSB gave the best result.

Thus, data can be embedded according to the following algorithm.