HIGH DATA RATE AUDIO STEGANOGRAPHY ON DIFFERENT COVER FILES

Thesis submitted in partial fulfillment of the requirements for the award of degree of

Master of Engineering

in

Information Security

Submitted by

Amneet Kaur

(Roll No. 801533002)

Under the supervision of

Dr. Sangita Roy

Lecturer

Miss. Rajanpreet Kaur Chahal

Lecturer

COMPUTER SCIENCE AND ENGINEERING DEPARTMENT

THAPAR UNIVERSITY

PATIALA – 147001

JULY 2017

CERTIFICATE

I hereby certify that the work which is being presented in the thesis entitled, "*High Data Rate Audio Steganography On Different Cover Files*", in partial fulfillment of the requirements for the award of degree of Master of Engineering in Information Security submitted in Computer Science and Engineering of Thapar University, Patiala, is an authentic record of my own work carried out under the supervision of Dr. Sangita Roy and Miss. Rajanpreet Kaur Chahal and refers other researcher's work which are duly listed in the reference section.

The matter presented in the thesis has not been submitted for award of any degree of this or any other University.

Amneet Kaur.

(Amneet Kaur)

This is to certify that the above statement made by the candidate is correct and true to the best of my knowledge.

(Miss. Rajanpreet Kaur Chahal)
Lecturer , CSED

(Dr. Sagnita Roy)
Lecturer, CSED

ACKNOWLEDGEMENTS

The successful completion of any task would be incomplete without acknowledge the people who made it possible and whose constant guidance and encouragement secured the success.

First of all I wish to acknowledge the benevolence of omnipotent God who gave me strength and courage to overcome all obstacles and showed me the silver lining in the dark clouds. With the profound sense of gratitude and heartist regard, I express my sincere feeling of indebtednes to my guide **Dr. Sangita Roy**, Lecturer, Computer Science and Engineering Department, Thapar University and coguide **Miss. Rajanpreet Kaur Chahal,** Lecturer, Computer Science and Engineering Department, Thapar University for their positive attitude, constant encouragement, keen interest, invaluable cooperation and above all their blessings. He has been a source of inspiration for me, I am grateful to **Dr. Maninder Singh,** Head of department and **Dr.**

Shreelekha Pandey, PG coordinator, Computer Science and Engineering Department, Thapar University for the motivation and inspiration for the completion of this thesis. I will be failing in my duty id I do not express my gratitude to **Dr. S. S. Bhatia,** Senior Professor and Dean of academics affair in the university for making provision of infrastructure such as library facilities, computer labs occupied with internet facility, immensely useful fort he learner to equiped themselves with latest in the field.

Later but not the least I would like to express my heartfelt thanks to my parents and my friends who with their thought provoking views and whole hearted cooperation helped me in doing this thesis.

(Amneet Kaur)

ABSTRACT

Steganography is the art and science of secret message. The secret message or plain text may be hidden in one various ways. The media with hidden information are called stego media and without hidden information are called cover media. Steganography can use for hide both legal and illegal information. It is the technique of hiding information in digital media in order to conceal the existence of the information. To make the system more secured this system uses most powerful algorithm in the first level of security which encrypts the data. In the second level the encrypted data is embedded in to the audio file using modified LSB algorithm. This system ensures more security. To conceal a secret message we need a wrapper or container as a host file. Different wrappers or host files or cover medium are used to

hide the secret message e.g. image, audio, video, text. Audio files and signals make appropriate mediums for steganography due to the high data transmission rate and the high level of redundancy. Hiding data in real time communication audio signal is not a simple mission. Steganography requirements as well as real time communication requirements are supposed to be met in order to construct a useful and useful data hiding application. In this paper aims at enhancing the provision of audio steganography by introducing one LSB(least significant bit) coding technique. We design a high bit rate LSB audio watermarking method that reduces embedding distortion of the host audio with increases capacity of secret text. By using standard and proposed algorithm, watermark bits are embedded into higher LSB layer, resulting in increased robustness against noise addition which is limited by perceptual transparency.

TABLE OF CONTENTS

CHAPTER 1

LIST OF FIGURES

LIST OF TABLES

ABBREVIATION

AES	Advanced Encryption Standard
AIFF	Audio Interchange File Format
AVIS	Advanced VoIP Steganography System
AWGN	Added Substance White Gaussian Noise
BER	Bit Error Rate
EAS	Enhanced Audio Steganography
GA	Genetic Algorithm
HAS	Human Auditory System
HLLAS	Higher LSB Layer Based Audio Steganography
LSB	Least Significant Bit
MSB	Most Significant Bit
SNR	Signal To Noise Ratio
SPNR	Signal To Perceived Noise Ratio
SS	Spread Spectrum
WAV	Windows Audio Visual

CHAPTER 1

INTRODUCTION

1.1 Steganography

The term steganography is characterized as a procedure of composing concealed messages by utilizing a few methods that nobody else once the presence of the message. PC based steganography enables modify to be made to what are referred to as advanced transporters, for example, content, pictures, sound, video, or convention, the progressions speak to the concealed message, however conclusion if effective in no perceptible modify to the carrier.

On steganography, in the recent past the hiding procedure, the sender must pick an fitting message carrier, those hidden message, and the secret key likewise; those sender Might send those shrouded message of the authority toward using at whatever of the electronic correspondence strategies What's more steganography calculations that must have those limit should scramble those message every last one of a greater amount effectively. In the inverse side, resulting to getting those message those beneficiary unscrambles the hidden message using those extraction figuring What's more a secret key[1].

Those elementary objective about steganography is with abstain from attracting keenness in regards those transmission for shrouded information to finish those security of the secret message, in the intend time, Assuming that the programmers saw any conformity in the sender message At that point this onlooker will endeavor will knows that disguised information inside those message [2],[3].

The undisclosed data bit can be embedded by marginally moving the binary arrangement of audio file. Accessible audio steganography programming can embbed messages in .wav sound documents. Infusing the secret data bits in audio record is normally a more troublesome errand than infusing data bits in other media, as computerized pictures. To implant the secret data in computerized sound distinctive

sorts of strategies are utilized. For audio steganography, the techniques that are normally utilized incorporate Parity coding, LSB coding, Spread range, Echo hiding, Phase coding. Most much of the time utilized system for audio steganography contains bitwise control of the cover question embed the secret data bits. For bitwise steganography, Least Significant Bit (LSB) Steganography is a good approaches, where the secret data bits to be covered up into the LSBs of the covered question [4].

In the event that the LSB is changed, it won't irritate the normal for the sample and furthermore the cover information that is sound. The benefit of the LSB contrasted and alternate bits in the example is insignificant. It will happen some noise, however the discovered sound level ought to be kept beneath a limit. In moderate strategy, it is simple for the stalker to extricate the message from the stego signal.

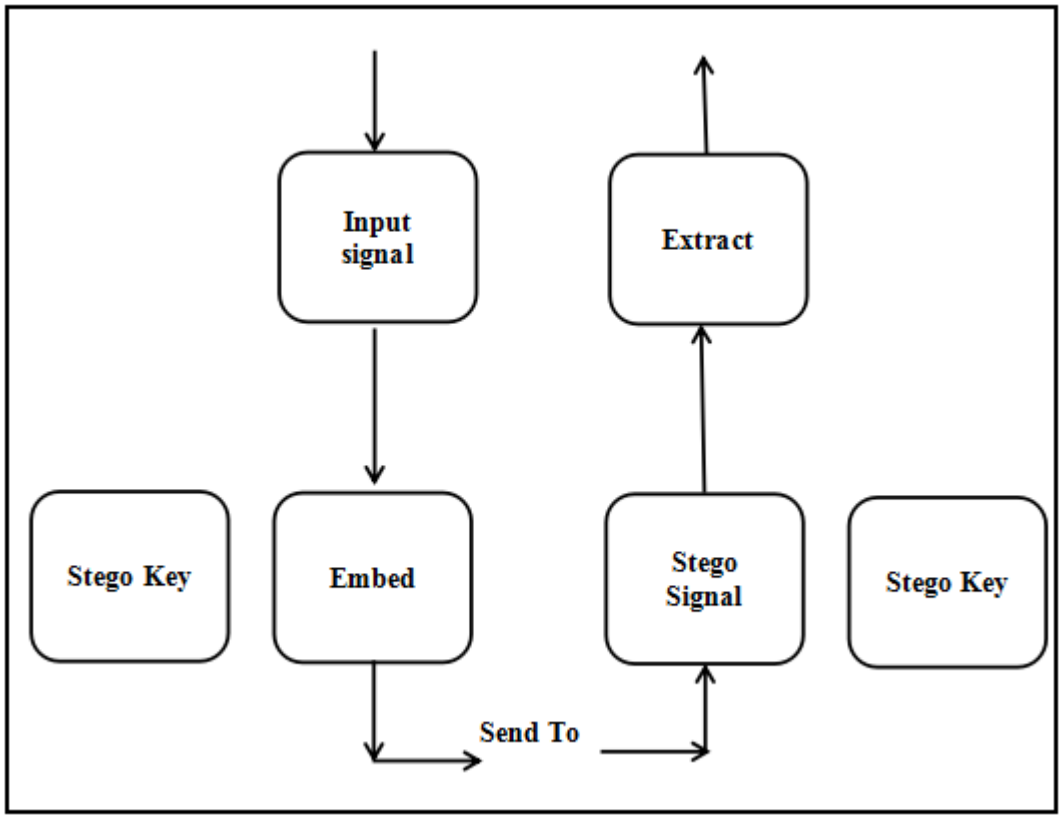


Fig. 1.1: Basic Steganography Approach

Figure 1.1 demonstrates the essential steganographic approach. In this a secret information is embed inside an info signal to create the stego signal. A security key is typically required the inserting procedure. The precise a stego key is utilized by the

senders for the installing procedure. A similar key is utilized by the recipient to remove the stego motion in order to see the secret information. The stego signal is looked practically indistinguishable into the information signal.

1.1.1 Structures of Steganography:-

Given the expanded general consideration over steganography strategies and practices, few basic phrasing that the majority of the application have in like manner has been examined and determine[5]. The things conceded to:

- **Embedded(m):-** some data information or signal to be hidden, in other media.
- **Stego Message(s):-** The output of the steganography procedure which is the signal, record or information that has the installed message hidden in it.
- **Cover Object(c):-** The contribution to the data concealing procedure which speaks to the blameless transporter flag or document.
- **Stegokey(k):-** This is extra unembedded mystery information which might be required in the data concealing procedure. Specifically, this key is regularly expected to extricate the installed message again in the last goal.

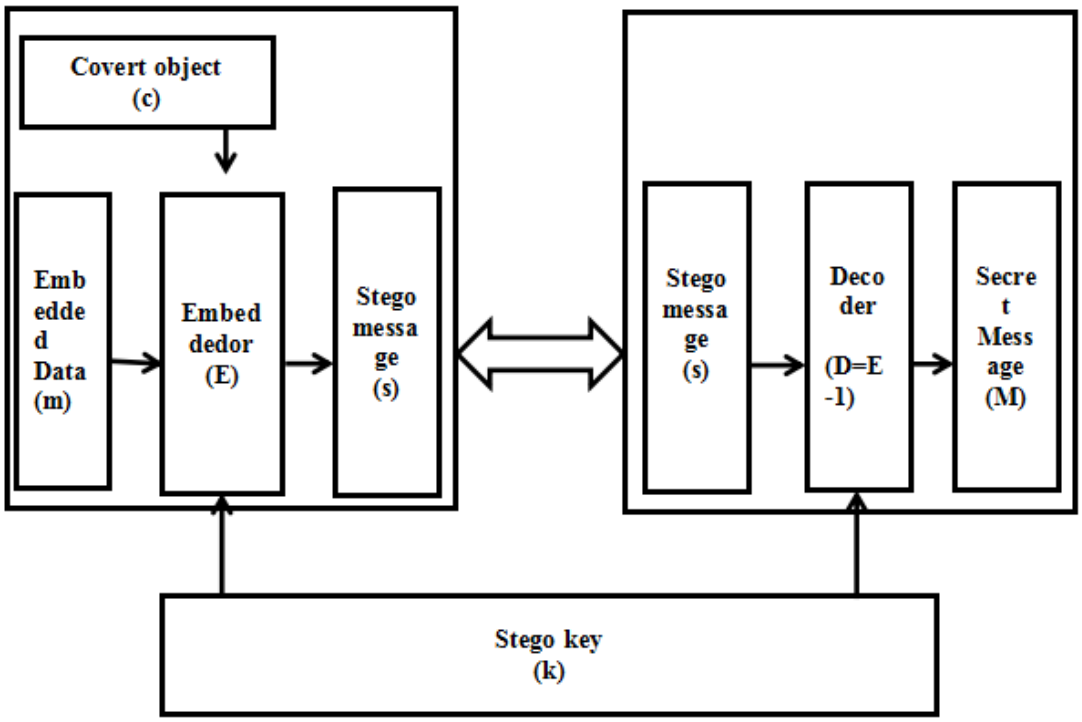


Fig 1.2: Steganography terminology

1.1.2 Hiding Methods:

1.1.2.1 Insertion-Based*:* In this sort we can store the data that we need to hide in those segments of a document which are disregarded by handling application. Because of this we abstain from adjusting those document bits that are significant to an end-client.To instance, for a couple records there is an EOF alternately end-of-file marker. This flag infers of the requisition that is examining the archive that it need attained the complete of the record and the requisition can stop taking care of the report. Stowed away information might afterward have the ability should a chance to be inserted after the EOF marker. Those end-client might not comprehend that the record holds additional disguised information.We can utilize an infusion strategy which changes record measure with measure of information covered up in document and if the record estimate expansive, it might stimulate doubt.

1.1.2.2 Substitution-Based: Done substitution we can supplant those slightest critical odds for majority of the data that makes the significant substance of the spread record for new information which makes those less measure from claiming twisting. In this the blanket record evaluate doesn't transform following the execution of the figuring. Confined measure for data we could conceal for this approach Similarly as there will be a compelled measure of irrelevant majority of the data On any provided for record.

1.1.2.3 Generation-Based: Furthermore and substitution, this kind doesn't require any current blanket archive. In this it makes an cover record to those sole inspiration behind hiding those message. The standard disservice of the consideration What's more substitution is those examination of the stego record with any former copy of the blanket report (which ought make An comparative record) Furthermore find contrasts between the both. You won't bring that issue when using an period approach, in this the Conclusion may be an interesting cover record and is sheltered to examination tests. [6][7][8][9].

Those information hiding system comprises about Emulating two stages:.

I. Straight off the bat, abundance odds to a cover-document would recognized. Overabundance odds are the individuals odds that could be balanced without obliterating the respectability and abusing the nature of the cover record.

II. Will insert the secret information (or information) in the disguise document, the abundance odds demonstrate in the disguise record will be supplanted toward those odds of the secret information.

The Steganography Method Used should have:

a) Imperceptibility: The video with information and unique information source ought to be perceptually indistinguishable

b) Robustness: The inserted information ought to survive any preparing operation the host signal experiences and safeguard its devotion.

c) Capacity: Maximum information implanting rate.

d) Secrecy: Extraction of hidden data from the video must not occur without earlier authorization of expected client having secret word.

e) Accuracy: The extraction of the hidden information from the medium ought to be precise and solid.

1.1.3 Steganography Measures

A)Imperceptibility: An steganographic system will be ambiguous when mankind's eye can't remember the disguise picture and the stego picture.

B) Payload: it indicates the measure for mystery information that can a chance to be embedded in the cover picture. Those implanting rate may be provided for over aggregate estimation, for example, those period of the secret message.

C) measurable Attacks: The approach to uprooting the secret information starting with the stego protest may be known as measurable assault. The algo used for steganography must a chance to be robust to measurable strike.

d) Security: Security of a steganographic framework are characterized regarding imperceptibility, which is guaranteed when the statistical tests can't recognize the cover and the stego-picture..

e) Computational Cost: Information hiding and Data recovery are the two parameters used to figure computational cost of any steganography approach. Data hiding time suggests the time required to embed data inside a cover video edge and data recuperation insinuates extraction time of riddle message from the stego

f) Perceptual Quality: Expanding the payload debase the nature of the video so approach ought to be utilized to such an extent that the quality ought to stay in place to maintain a strategic distance from it from getting in locate.

1.1.4 Uses of Steganography:

The three the vast majority common Also inquired regarding utilizations for steganography to a open frameworks condition are undercover channels, embedded majority of the data and propelled watermarking. Undercover channels can be make greatly important for At whatever secured correspondences needs completed open frameworks, to example, those web. Eventually perusing implanting those stowed away data under those cover message Furthermore sending it, you can be pick dependent upon a feeling that every one is great for the planet incidentally that no one knows you need sent more than a harmless message other than those recommended beneficiaries advanced watermarking is basic in the area Furthermore prosecution from claiming modifying privateers/computerized hoodlums. Steganography is used Toward a few present printers, including hp What's more Xerox mark shading laser printers.

1.1.5 Applications:-

Steganography is appropriate to, however not restricted to, the accompanying regions.

1) Confidential correspondence and secret information putting away

2) Protection of information modification

3) Access control framework for advanced substance dispersion

4) Media Database frameworks. [10]

1.1.6 Attacks on Steganography:

Emulating may be the rundown about some could reasonably be expected attacks:.

- **File only:-**In this , the assailant need right of the document What's more ought to determine if those information is stowed away done it or not.
- **File What's more first Copy:-**If the assailant need An duplicate of the unique record What's more pre-encoded record that point the genuine address is the thing that the assailant will do for those mystery message(destroy hidden information, extricate hidden data , trade it).
- **Compression Attack:-**One of the simplest assault will be will layer those record holding the concealed data. Layering calculations attempt should uproot the superfluous majority of the data from a file, and "hidden" is proportional to "extraneous".
- **Destroy All that Attack:-**In this, assailant Might essentially obliterate those entire message.
- **Reformat Attack:-**One of the could be allowed assault is on transform those organization of the document. Different record formats don't store those information precisely in the same way(JPEG, GIF). □
- **Random Tweaking Attacks:-**An assailant Might essentially include small, irregular tweaks in place with wreck those message.
- **Structural Attack:-**Steganographic calculations by and large clear out An trademark structure of the information. The association of the majority of the data archive is notable when information may be embedded under it. Those attacker might without significantly of a stretch recognize the closeness of the secret message by dissecting those true profile of the odds. These progressions of the majority of the data record for those The greater part piece fall into effortlessly perceptible illustration that provides for An sign of a stowed away message[11][12].
- **Visual Attack:-**The visual ambush is a stego-just attack that strips out bit of the address Previously, lifestyle that takes under attention An human on search for visual peculiarities. The The greater part well-known attack may be should indicate the least tremendous bit of a protest; advanced sorts for gear, to example, cameras are not immaculate Also consistently clear out echoes in the least incredulous odds. These completely discretionary commotions show the vicinity of a disguised message. Those ordinary ear might get inconspicuous contrast for

sound. Make that Likewise it may, this may be moderate What's more unreasonable attack[13][14].

1.1.7 Merits of Steganography:

Steganography includes making the substance of the mystery message indistinguishable same time not keeping non exceptional spectators will take its existence[15]. The essential objective of steganography will be with hidden those secret message same time cryptography will be on aggravate information understand it.

Few attributes to measure the quality of the steganography:

High Capacity

Resistance

Confidentiality

Accurateness

No detections

Visibility

Imperceptibility

1.2 Types of Steganography

Over cutting edge approach, contingent upon those way for spread object, steganography can be make isolated under four types:.

1.2.1 Text Steganography: content steganography could be attained toward adjusting the content formatting, or toward adjusting sure qualities from claiming text based components (e.g.characters). It incorporates line-shift coding, word-shift coding What's more characteristic coding.

Distinctive embedding systems to content:-

- **Modifying Spaces:**-Data could a chance to be concealed Previously, a blanket quick Eventually Tom's perusing modifying the plain spaces Previously, quick. Appending person or two spaces of the conclusion for every offering may be Additionally a basic information hidden method. An statement processor could change those inter word spaces to An sentence.

- **Semantic Methods:-**In this method, information is inserted utilizing uncommon expressions use. The sender What's more recipient both will concur upon utilizing certain on the web thesaurus. Those decoder will peruses those cover quick expression by expressions Also searches those thesaurus for event about each saying. Assuming that no such saying will be found, the decoder expects that no information is concealed over it.

Advantage –

They can not be detected by re typing or OCR methods

Disadvantage–

Smart reader having huge knowledge of words can discover it easily.

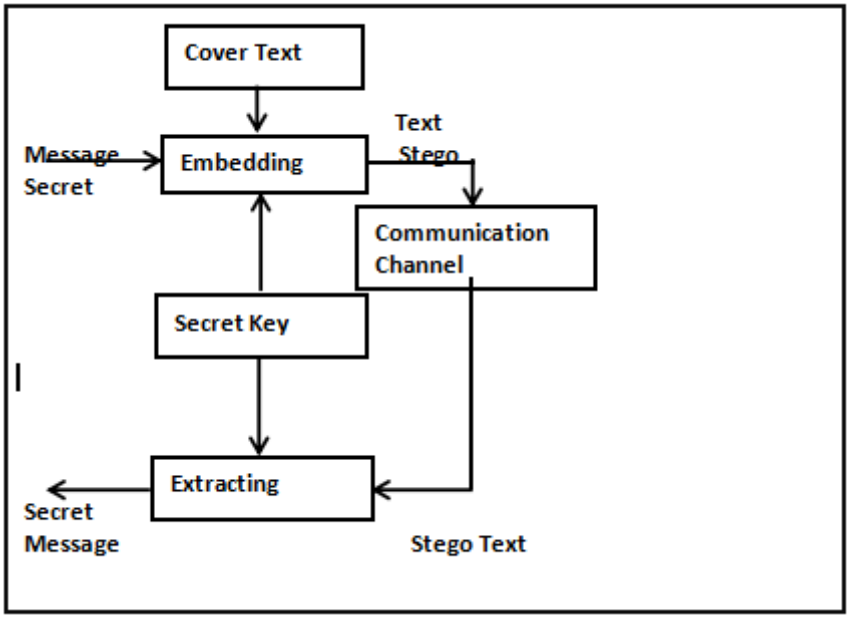


Fig 1.3. Text Steganography

- **Syntactic Methods**:-These techniques are In light of modifying the text such-and-such its importance is safeguarded. This methodology is that's only the tip of the iceberg safer, harder will execute Similarly as workstations need aid notoriously terrible In “understanding” those text.

Advantage–

The amount of information to be hided in this method is trivial.

Disadvantage–

Smart reader can easily find the hided information in this methods.

1.2.2. Image and Video Steganography:- Pictures need aid those the majority well known spread Questions utilized to steganography. In the Web-domain about advanced pictures a significant number separate document formats exist Furthermore for these document formats diverse calculations exist. These separate calculations utilized need aid any rate as critical spot insertion, masker What's more filtering, excess design Encoding, scramble What's more Scatter, calculations Furthermore transformations.

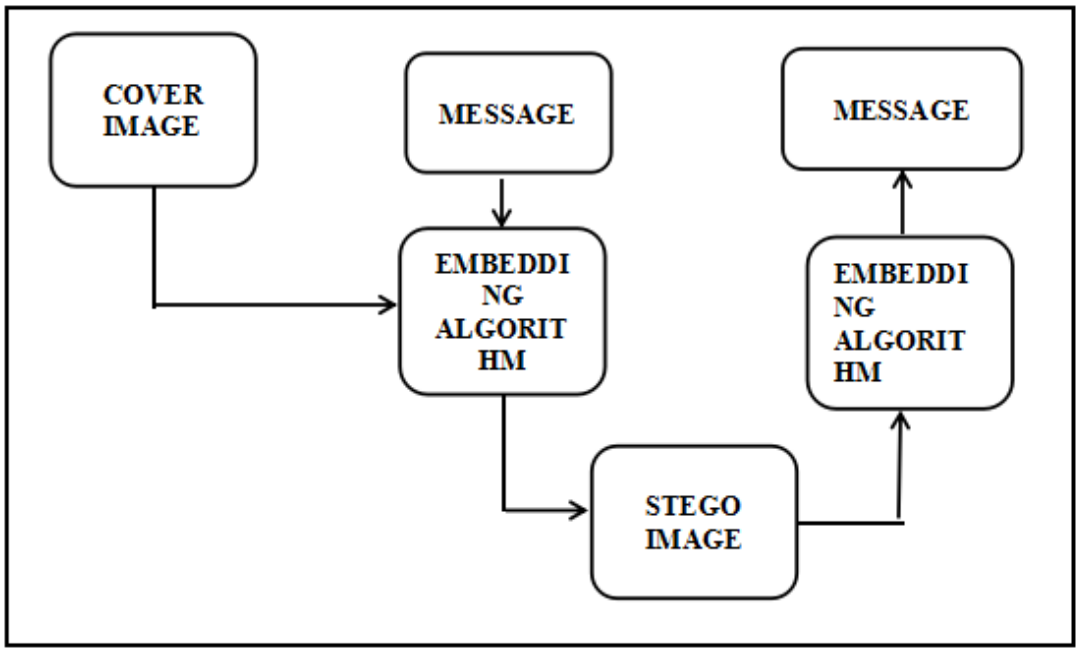


Fig 1.4. Image steganography

video files would for the most part an accumulation for pictures and sounds, thus practically of the exhibited systems with respect to pictures Furthermore sound can be connected will feature files a really. Those extraordinary favorable circumstances for feature would those expansive sum of information that might make stowed away inside and the way that it is a moving stream about pictures Furthermore resonances.

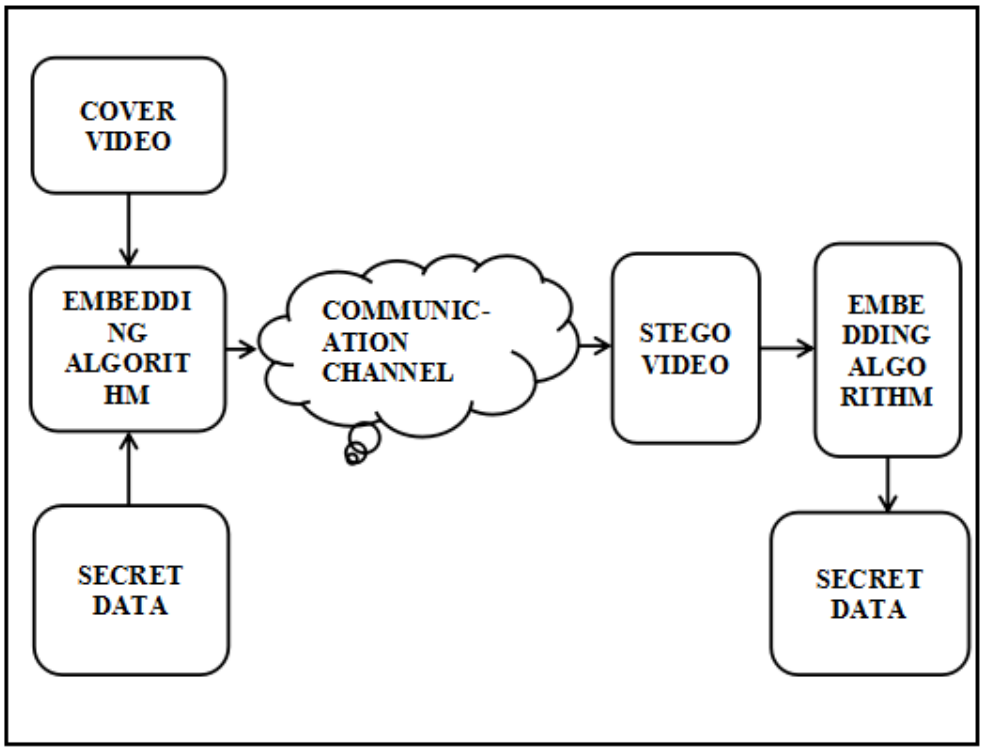


Fig 1.5. Video Steganography

Separate information embedding systems utilized for image/video:.

- **Masking and sifting:-**It will be the system Eventually Tom's perusing which information is hided Toward denoting those picture. These methods implant the data under the that's only the tip of the iceberg foremost domains so that closeness from claiming majority of the data could not be separated Likewise contradicted on hiding it under the clamor level.

Advantages-.

This system may be more strong over LSB supplanting for turns about layering Similarly as message may be hided in the noticeable parts of the picture.

Disadvantages-.

This strategy can be connected will ash scale pictures main.

- **Transform space Technique:-**This is the strategy for which mystery majority of the data will be inserted under the change space for spread. It may be the Amazingly mind boggling strategy to hiding the majority of the data. This is a greater amount psyche boggling sort about hiding the mystery data under the picture. Change Web-domain method have favorable element through LSB strategy as they shroud the information under the regions about picture which would lesquerella uncovered on cropping , image transforming.

Convert Web-domain systems are comprehensively arranged under :.

A. Discrete fourier change procedure (DFT).

B. Discrete cosimo the senior change system (DCT).

C. Discrete Wavelet change procedure (DWT).

Advantages-

Helter skelter spot rate information concealing.

It will be alter safe.

Hides mystery odds looking into both vertical and dialog edges from claiming spread picture.

Disadvantages-

Hides those information done free frames.

The utilization from claiming piece DCT might bring about blocking artifacts in the stego-video.

In spite of quantization about mystery picture declines the measure of the secret information yet all the it influences those caliber of the retrieved picture.

- **Distortion Techniques:-**Distortion systems necessity the finish learning of the disguise networking amid those translating methodology on the fact that those decoder needs to weigh the initial disguise picture and the turned disguise picture will restore those mystery message[16][17]. In the occasion that those attacker endeavors with alters those stego-picture by trimming or turning it , those authority could without a great part of a stretch recognize it.
- **Information hidden systems done IPv4 Header:-**To safely transmit the information through those organize the Vasudevan et al. utilized those Similarity of the jigsaw riddle. They intimate should part the information under variable sizes As opposed to altered span such as those riddle What's more annex every part of information with An pre-shared message Confirmation code (MAC) What's more an arrangement number Along these lines that the recipient can be validate What's more consolidate the gained pieces under a solitary message.

1.2.3. Sound Steganography: To sound steganography, mystery message may be installed under digitized sound sign which effect slight adjusting about double arrangement of the comparing sound record. There would a few strategies like LSB coding, period coding, spread spectrum, reverberation concealing which would utilized to sound steganography

1.3 Audio steganography

In this sort for steganography we could implant secret messages under advanced digital audio over sound steganography. It will be more perplexing methodology Concerning illustration contrast with embedding messages clinched alongside different networking. This steganography strategy could implant messages for WAV, au furthermore actually MP3 sound files[18][19]. Those sound steganography comprises of transporter alternately sound file, message and watchword. Transporter will be otherwise called a cover-file, which conceals those secret majority of the data.

On steganography model the secret message that those sender sends needs will stay it mystery. Message can make of any sort might a chance to be text, image, sound or any kind for file,. In secret stego key which just those collector knows those comparing deciphering way will have the ability with extricate those message from an cover-file. Those cover-file. With the secret data may be known as a stego-file.

Hidding transform will be comprises for two steps[20]. On principal steps ID number from claiming excess odds Previously, An cover-file. Excess odds are the individuals spot that could he changed without ruining those personal satisfaction alternately destroying those integument of the cover-file. Previously, second venture embedding those mystery information in the disguise file, those excess odds in the spread record is traded by the odds of the mystery information. Likewise same as audio alongside report images, we could change sound files On such an approach that they hold numerous hidden data, such as copyright data, we might settle on information altered Previously, such an approach should not wreck those indicator. For sound steganography we could implant data Previously, callous files for those assistance from claiming human sound-related framework (HAS). Those need perceives the added substance irregular clamor and Additionally the perturbations Previously, An heartless document might Additionally make distinguished. In any case there need aid some ―holes‖. Those advanced callous may be acquired starting with those simple heartless Toward converting it with advanced space. Those renowned record formats to resonances would those Windows Audio-Visual (WAV) and the sound compatibility document organization (AIFF).

There are also layering calculations for example, such that the worldwide principles association movement portraits master Group-Audio (ISO MPEG-AUDIO). Same time execute information hidden strategy for audio, we might 1st check An situations of the callous sign will travel between encoding and deciphering. Change will occur On 2 sorts of region which we think about. For capacity earth or advanced signal, other will be transmission way of the indicator might travel. Following secret messages hide effectively a portion routines need aid utilized for embedding information in advanced sound These routines extent implant majority of the data in the structure of indicator clamor should more capable routines that makes a secure alternately capable indicator transforming systems on conceal information.

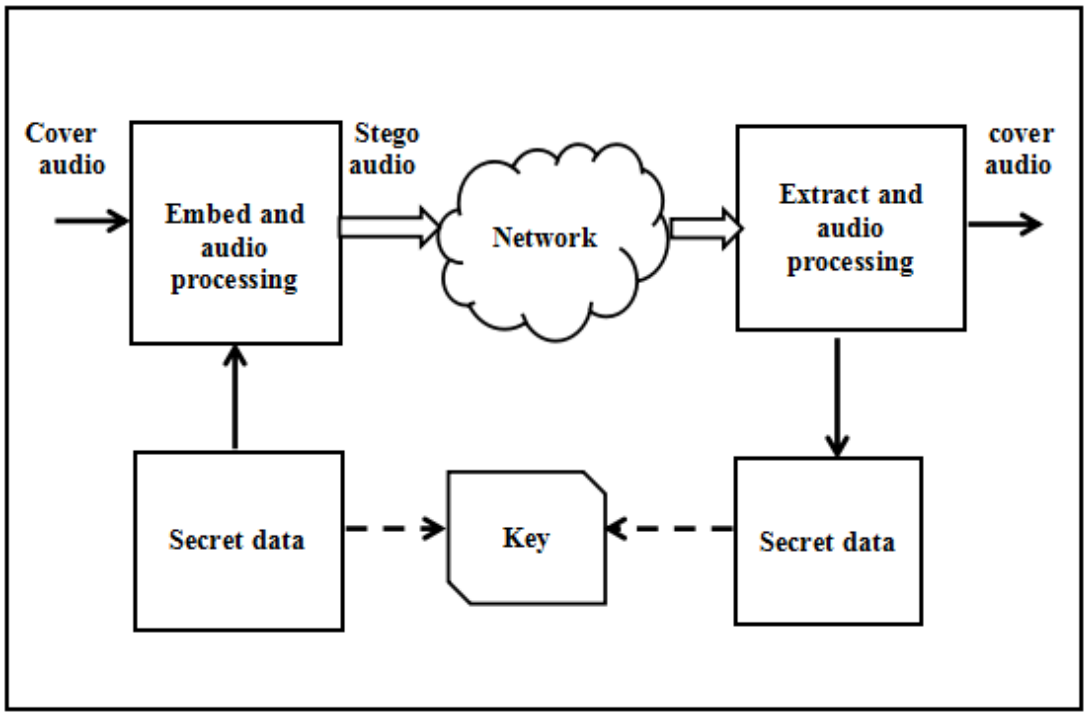


Fig. 1.6 Basic audio steganographic model

As an innovation of change over correspondence, steganography can insert secert to the open cover in broad daylight correspondence mode. It is concealing the data substance as well as hiding the presence of this conduct. The term covering up embroils the way toward making data undetectable to inmates.even however every one of these strategies shroud the message, every one varies in their own motivation and applications from each other.

Steganography is a specialty of concealing data in an interactive media protest, for example, picture, sound and video objects. The primary reason for steganography is to

draw the consideration of illicit clients frame the stego-record by choosing a harmless cover media. The name of the steganography strategy relies on upon the kind of cover media question utilized for disguising secert information. Among these sound steganography is all the more difficult contrasted with the picture and video steganography.

Steganography fills done Concerning illustration a techniques for private, secure Also every so often pernicious correspondence. Steganography will be the workmanship to cover the exceptionally closeness for correspondence Eventually Tom's perusing implanting those mystery message under those innocuouslooking spread networking items, to example, portraits using the human's visual, aural excess alternately networking articles' measurable excess. Steganography will be a fit instrument flying which assembles security over majority of the data trading.

In the steganographic situation, the mystery data is To begin with camouflaged inside another address which is known as "cover protest", on shape "stego question" Also then afterward that this new protest camwood a chance to be transmitted or saved. Using different methods, we could send mystery data Likewise An music record alternately much An feature report by implanting it under the bearer record, encircling An stego banner. Sound steganography could be performed in the run through space Also Additionally repeat region. Existing sound steganography modifying might be embed messages On WAV, AU,and considerably MP3 callous documents.

Those target of steganography is will stow away secert information inside An cover-media such-and-such others can't watch the closeness of the shrouded secert information.

Our side of the point is with cover those best approach that correspondence will be happening. This is consistently refined by using a sort of broad spread archive What's more insert those reasonably short mystery message under this blanket record. Those Conclusion will be An looking report which may be those stego record that holds the mystery message.

ADVANTAGES:

1. Sound based Steganography need those possibility on hide All the more information:.

A. Sound files need aid by bigger over pictures.

B. Our listening to can be effortlessly fooled.

C. Slight transforms for plentifulness can be store Incomprehensible measures about data.

2. The adaptability of sound Steganography may be makes it exceptionally conceivably capable.

3. An alternate part about sound Steganography that makes it thereabouts alluring is its capacity will consolidate for existing cryptography innovations.

4. A lot of people sources Furthermore sorts makes measurable examination that's only the tip of the iceberg challenging.

DISADVANTAGES:

1. Embedding extra data under sound successions will be An additional dully undertaking over that from claiming images, because of dynamic matchless quality of the need again human visual framework.

2. Robustness: copyright denote hidden On sound tests utilizing substitution Might make effectively manipulated alternately wrecked Assuming that An villain goes with realize that majority of the data is stowed away along these lines.

3. Popularized sound Steganography bring Hindrances that the presence from claiming concealed messages might a chance to be undoubtedly distinguished outwardly What's more just specific measured information could make hidden.

1.3.1 Data Hiding in Audio Files

Encoding secret messages for sound is the a large portion was troublesome framework with use when overseeing Steganography. This will be on the fact that those human sound-related schema (HAS) need such a changing range, to the point that it can tune in again. Annoyances in a sound report could a chance to be recognized Similarly as low Likewise person area for ten million. In any case there need aid a couple "openings" open in this viewpoint try the place data could be concealed. Same time those need an enormous range, it habitually need An minimal differential range. Subsequently,loud resonances tend should mask crazy tranquil resonances.

1.3.2 How data is hidden in sounds:-

Sound specimens need aid exceptionally nature, wrong appraisals of the right estimation of the sound unit at a particular moment on at whatever run through. The sound tests for. WAV records are set far Similarly as Possibly 8 alternately 16 touch qualities that inescapably get Run of the DA converters done your audio board. For 8 spot values this infers the characteristics could run between 0 on 255. 16 bit values try between 0 with 65535. At S-Tools can may be to spread those spot configuration that identifying with the archive that you require to conceal again those scarcest foremost odds of the callous example.

To instance, expect that a sound unit example needed those going with eight bytes about information in it a portion place:.

133 135 138 142 122 103 75 39

In parallel, this is:

10000101 10000111 10001010 10001110 1111010 1100111 1001011 100111

(LSB about each byte showed up over italics).

Expect that we have to hiddenite the double byte 11010110 (214) inside this grouping. We supplant those LSB for each illustration byte with those relate spot starting with those byte, we need aid endeavoring should conceal. So the over grouping will change to:

134 136 137 142 121 103 75 39

In double, this is:

10000110 10001000 10001001 10001110 1111001 1100111 1001011 100111

Concerning illustration you might evidently observe, the estimations of the sound tests bring transformed by, In most, one regard regardless. This will a chance to be

impalpable of the mankind's ear, we bring concealed 8 odds about information inside those samples. This will be the theory behind how S-Tools do its occupation.

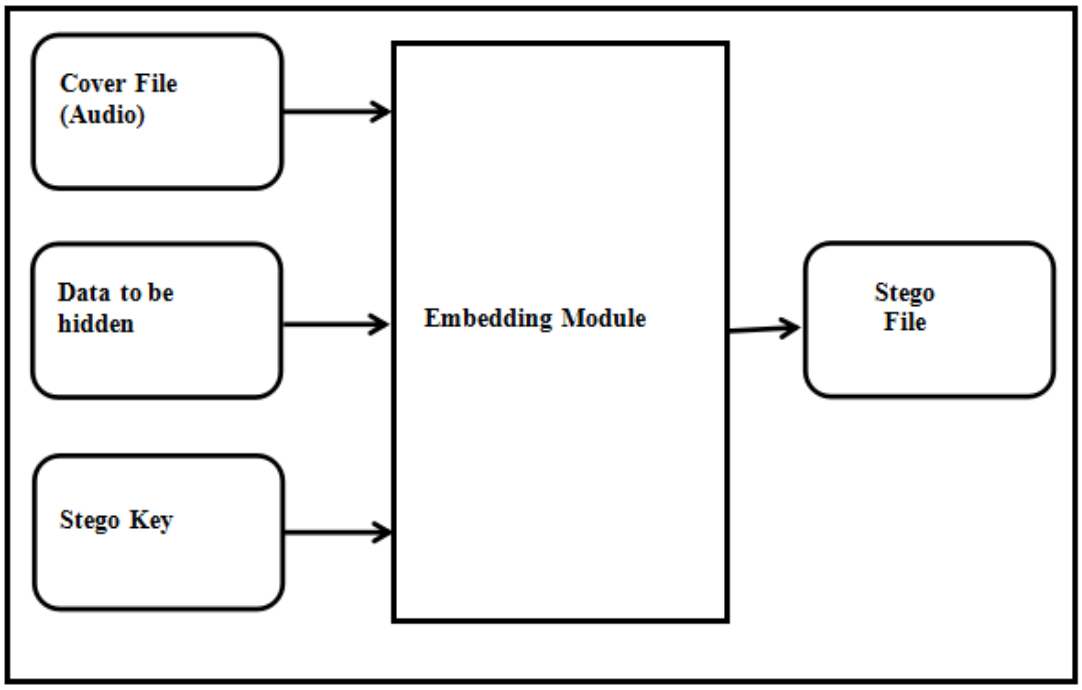


Fig 1.7. Basic audio steganography

1.4 Audio Steganography Techniques

There need been huge numbers systems to concealing data alternately messages for sound clinched alongside such an way that those alterations constructed of the sound document need aid perceptually indiscemible.

As a relatable point methodologies incorporate [21],[22]:

1.4.1 LSB Coding

A well known technique is those LSB (Least significant Bit) algorithm, which replaces those slightest critical bit to a few bytes of the cover record with hide an arrangement from claiming bytes holding the hidden information. That's as a rule a viable strategy to situations the place the LSB substitution doesn't result in huge quality degradation, for example, On 24-bit bitmaps.

Alongside computing, the any rate as critical touch (LSB) is those bit position On a double basic giving those units value, that is, deciding if the number is considerably

or odd. Those LSB will be Frequently alluded will Likewise those right-most bit, because of those gathering clinched alongside positional documentation for composing lesquerella huge digit further of the straight. It may be practically equivalent to of the any rate as huge digit of a decimal integer, which will be the digit in the ones (right-most) position.

1.4.2 Phase Coding

Phase coding addresses those Hindrances of the noise-inducing routines of sound Steganography. Period coding meets expectations by substituting those period for an introductory sound section with an reference stage that speaks to those data. This system depends on the reality that those period parts for sound need aid not as recognizable of the mankind's ear as commotion is. As opposed presenting perturbations, the method encodes the message odds as period shifts in the stage range of a advanced signal, accomplishing an quiet encoding As far as signal-to-perceived noise ratio (SPNR).[22]

1.4.3 Parity Coding

Equality coding is a standout robust those sound Steganographic systems. As opposed to separating an sign under distinctive samples, this system breaks a first sign under separate tests Also embeds each touch of the secret message starting with a equality bit. Whether the equality bit of a chose locale doesn't match those secret bit to be encoded, those transform inverts those LSB about a standout one of those samples in the district. Thus, those sender need a greater amount of an decision to encoding the secret bit[22].

Advantages–

In this , sender has more choices in encoding the secret bit.

Disadvantages-

It provides no robustness.

1.4.4 Echo data hiding

Reverberation information concealing arrangements for embedding from claiming quick (or information) On sound record Eventually perusing presenting an

reverberation of the first signal. The information then concealed Eventually perusing fluctuating three parameters of the echo:.

I. Starting amplitude,.

II. Decay rate,

III. Counterbalance.

Advantages–

Resilient to the lossy data compression algorithms used in this method.

Disadvantages-

It provides low security and capacity.

1.4.5 Spread Spectrum:-

On sound steganography, the essential spread range (SS) strategy endeavors on spread secret majority of the data crosswise over the recurrence range of the sound indicator utilizing a code which may be autonomous of the real signal. Two variants of spread range could make utilized within sound Steganography.

Direct-sequence: Direct-sequence (SS) endeavors with spread out the mystery message by a steady called the chip rate at adjusted with a pseudorandom sign Furthermore interleaved with those cover-signal[22].

Frequency-hopping schemes. Over frequency-hopping (SS), those recurrence range of sound files may be transformed thereabouts that it jumps quickly between frequencies.

Advantages-

It provides the better robustness as compared to other methods of audio steganography.

Disadvanatges-

It is vulnerable to time scale modifications.

Methods	**Embedding Techniques**	**Strengths**	**Weakness**	**Hiding Rate**
Least Significant Bit(LSB)	LSB of each sample in the audio is replaced by one bit of hidden information	Simple and easy way of hiding information with high bit rate.	Easy to extract and to destroy.	16 Kbps
Echo hiding	Embeds data by introducing echo in the cover signal.	Resilient to lossy data compression algorithm.	Low security and capacity.	40-50 Bps
Phase coding	Modulate the phase of the cover signal.	Robust against signal processing manipulation and data retrival needs the original signal.	Low capacity.	332 Bps
Parity coding	Break the signal into seperate samples and embeds each bit from secret message in sample region parity bit.	Sender has more of a choice in encoding the secret bit.	Not robust.	320 Bps.
Spread spectrum	Spread the data over all signal	Provide better robustness.	Vulnerable to time scale	20 Bps.

	frequencies.		modification.	

Table 1.1. Comparison of Audio Steganograph

CHAPTER 2

LITERATURE SURVEY

1. M. Asad et. al present the secret message will be transmitted will be Run through two layers in the recent past it will be introduced inside the spread message in the third layer[23]. The stego message is transmitted over those framework of the authority side and the secret message is recovered Eventually perusing performing opposite operations in rearrange organize. Those objective of the paper may be to guarantee the security of the secret message. They similarly inspected the utilization issues of the three layered model With respect to Different parameters similar to limit, straightforwardness Furthermore quality. Test hails around need exhibited that three layer hint at finished a banner to upheaval extent about 54. 78dB as opposed with 51. 12 db of universal LSB procedure.

2. L. Rana et. al implemented Audio Steganography to fulfill the two fold layer randomization methodology may be used[24]. Regardless layer of randomization may be finished Toward haphazardly picking those byte amount or tests. An additional layer of security is provided for Toward subjectively picking those spot position during which introducing may be completed in the decided tests. Using this recommended figuring the transparency What's more heartiness of the steganographic technique is stretched.

3. K.Gandhi et. al introduced LSB methods,However instead all the more powerlessness with make strike LSB strategy is not favoring. Rather two bits (second What's more third LSB's) are used for hiding message. This will Fabricate the majority of the data hiding cutoff excessively. A channel may be planned on cutoff those progressions happened for stego archive. Those stego report close by the divided record consequently procured may be used to process An a standout amongst a sort way. The separated record and the generated all the enter will make transmitted should collector. Those key will induce will separate those right message during collector's conclusion.

4. B.Priyanka.et. al implemented a novel approach of audio Steganography [26].Using inherited calculation, message odds need aid embedded under various and higher LSB layer esteems, bringing around stretched embedded. The quality might be extended against the individuals planned assaults which endeavor with uncover the disguised message Furthermore Besides a portion unintentional assaults like noise extension as well.

5. K.Gandhi et. al introduced LSB methods,However instead all the more powerlessness with make strike LSB strategy is not favoring. Rather two bits (second What's more third LSB's) are used for hiding message. This will Fabricate the majority of the data hiding cutoff excessively. A channel may be planned on cutoff those progressions happened for stego archive. Those stego report close by the divided record consequently procured may be used to process An a standout amongst a sort way. The separated record and the generated all the enter will make transmitted should collector

6. S.S. Divya et. al discussed a method of hiding text in audio using multiple LSB steganography and provide security using cryptography [28].To 16 bit for each case audio groupings the majority amazing number about odds that can wood a chance to be balanced for LSB audio steganography without influenced those nature for host sound sign may be 4 LSBs. Those investigation need recommended two novel methodologies about substitution framework from claiming audio steganography that enhances those breaking point for spread sound to implanting additional data. Here message odds are embedded under different What's more variable LSBs. These strategies use up should 7 LSBs to inserting data. From those results these systems enhances the breaking point for data information concealing for cover sound by 35% with 70% The point when contrasted with the standard LSB figuring which uses 4 LSBs to majority of the data implanting.

7. G. Nehru et. al study audio steganography techniques using LSB and genetic algorithm approach [29]. This investigation need examination of different methods from claiming audio steganography using different calculations like innate figuring approach Furthermore LSB methodology. It need endeavored A percentage methodologies that support in audio steganography. It need those workmanship also

examination for forming hidden messages such-and-such selective those sender Furthermore arranged beneficiary presumes the presence of the message.

8. A.Gadicha et. al implement a new 4th bit rate LSB audio Steganography method that reduces embedding distortion of the host audio [30]. Utilizing those recommended calculation, message odds would embedded under fourth LSB layers, bringing something like stretched robustness against upheaval development. Listening to tests showed that perceptual way from claiming sound will be higher by virtue of the suggested system over in the standard LSB method.

9. M. Zamani et.al described the problems of substitution technique and solution to the problems [31].Those elementary issue will be low robustness against attacks. Two sorts from claiming attacks would there. Particular case sort assault tries will uncover the concealed message also different tries to annihilate those concealed message. Clinched alongside standard LSB method secret message is embedded in the least significant bit. This system is that's only the tip of the powerless against assult. Thereabouts Toward inserting message for odds other than LSB more stupendous security can make finished. More control can be a chance to be refined though message will be introduced under a greater amount profound odds. Yet, those issue may be that Likewise you quit offering on that one move into the MSB's those host sound signal gets changed. This issue might a chance to be understood toward a keen computation which inserts the message odds in the msb furthermore transform separate odds should decrease the screw up. Using this adroit count message odds could be embedded under diverse MSB's with finish higher cutoff furthermore.

10. R. Sridevi et. al suggested an productive system for audio steganography toward altered LSB algorithm furthermore solid encryption way for improved security may be recommended [32]. Enhanced Audio Steganography (EAS) will be a mix from claiming audio Steganography What's more cryptography. EAS proceeds clinched alongside two stages: it uses successful encryption count in the elementary level and in the second level it uses an balanced LSB (Least significant Bit) count to embed those message under sound.

11. F. Djebbar et. al [33],Steganography has been proposed as another option system to implement information security. Of late, novel and adaptable sound steganographic strategies have been proposed. An immaculate sound Steganographic system go for

installing information in a subtle, powerful and secure way and afterward extricating it by approved individuals. Henceforth, avant-garde the fundamental test in computerized sound steganography is to acquire vigorous high limit steganographic frameworks. Inclining towards outlining a framework that guarantees high limit or strength and security of implanted information has prompted extraordinary differing qualities in the current steganographic procedures. In this paper, we exhibit a present condition of craftsmanship writing in advanced sound steganographic strategies. We investigate their possibilities and restrictions to guarantee secure correspondence. A correlation and an assessment for the checked on procedures is additionally introduced in this paper.

12. K. Gopalan et. al [34],A technique for installing a secretive sound message in a cover expression for secure correspondence is displayed. The clandestine message is spoken to in a packed shape with conceivably encryption and additionally encoding for included security. One piece in each of the sample of a given cover expression is changed as per the information bits and a key. A similar key is utilized to recover the implanted bits at the collector. The outcomes, in light of cover signals from a clean TIMIT articulation and a boisterous flying machine cockpit expression, demonstrate that the strategy meets a few noteworthy criteria for effective incognito correspondence.

13. G.Nehru et. al[35],This paper will be those examination of diverse methodologies for sound steganography using dissimilar algorithmic like genetic computation approach also LSB approach. We have endeavored a percentage methodologies that assistants for sound steganography. Concerning illustration we most likely am mindful it may be those craftsmanship What's more craft from claiming forming shrouded messages such-and-such nobody, aside from the sender Also recommended beneficiary, copartners the vicinity with those message, An sort for security through absence of clarity. Over steganography, those message used to hide mystery message will be known as bring message alternately blanket message. When those substance of the group message alternately spread message are adjusted, those resultant message is known as stego message. Similarly as such, stego message is mix for host message Furthermore secret message. Audio steganography obliges An substance or sound secret message to a chance to be introduced inside An spread heartless message. Due

to approachability of excess, the disguise audio message in front of steganography, stego message following steganography sits tight same. To information hidding.

14. Jayaram et. al[36],The present huge request of web applications expects information to be transmitted in a safe way. Information transmission out in the open correspondence framework is not secure on account of capture attempt and ill-advised control by meddler. Thus the engaging respond in due order regarding this issue may be Steganography, which is the craftsmanship Furthermore investigation for forming stowed away messages such-and-such nobody, aside starting with the sender Also arrange recipient, copartners those vicinity for those message, a sort of security through absence of meaning. Heartless steganography is those arrange of hiding those vicinity from claiming puzzle information Eventually perusing disguising it under another medium, for example, sound record. In this paper we for the most part examine diverse sorts of sound steganographic techniques, points of interest and inconveniences.

15. K. Pradhan et. al[37],Data transmission out in the open correspondence framework is inclined to the block attempt and dishonorable control by eavesdropper. Audio Steganography may be those procedure about hiding those vicinity for secret information Eventually perusing compacting it under an additional medium, for example, sound record. This paper investigates the inventive sound Steganography strategy to the sum intents Also purposes keeping clinched alongside brain those limit objective should blanket those favoring information. The proposed framework utilizes LSB (least significant bit) procedure for installing content into a sound document. The content is scrambled utilizing AES (Advanced encryption standard) encryption work and md5 hash function which is utilized for checking information respectability of the sound document. The execution of this framework is assessed through a more secure process in light of heartiness, security and information concealing limit.

CHAPTER 3

PROBLEM STATEMENT

As the web is developing step by step secure transmission of the information is exceptionally critical. Along these lines, secure transmission of data must be hidden and in addition secure. Web correspondence is fundamental piece of correspondence now a days. In this way, we can expand the classification of information by applying the security strategies and steganography to give greater security to the information. At the point when computerized data is transmitted over the web, it can be altered or altered by the assailants. This issue yields the greatest worry throughout the most recent couple of years. In this way, the unapproved access of the transmitted data and responsibility for archive should be ensured.

The present work is centered around enhancing the security of the archive while it is been exchanged over the general population organize So, that no assailant can alter it inside the transmission. In this work, cryptographic and steganography method has been utilized to deal with this worry. We have connected Audio steganography procedure utilizing LSB (Least Significant Bit) Method and ascertained their separate Bit error rate The concentration of this examination work is the audio steganography especially with the WAV documents, in this way not changing the measure of the sound flags even after the installing procedure.

By utilizing these diverse strategies:-

- It is conceivable to implant the concealed message with the four change of the individual bits that make up a sound record.
- Any systems which tries to enhance the implanting payload and strength should save subtlety.
- Different inserting payload may affect sound quality.
- The longer payload or the bytes of the shrouded message is greater, at

that point it will change the first sound quality and get distinctive impacts.

- Thus, a few strategies will be utilized to look at the impacts on sound Quality utilizing distinctive inserting payload.

3.1 Research Methodology:-

Our proposed LSB technique explained in the following process:

1.Read one example from the wave document.

2.Get the following two bits from the present message byte.

3.Place it in the current fourth and third piece of the example.

4.Flip the rest two bits.

5.If the fourth and third piece is equivalent to test bit

At that point no adjustment in test bit

Else

Change in test bit

6.If the fourth and third piece is not equivalent to test bit.

At that point flip the second and first piece of test

Else

Not flip the second and first piece of test

7. At that point locate the base estimation of test which is flip or not flip.

3.2 Research Objectives

Order of audio archives as bearing hidden data or not is a security issue tended to with regards to steganalysis. A cover sound question can be change into a stego-sound protest by means of steganographic strategies. In this exploration work a statistical techniques will be proposed which will compute the impact of steganography on audio signs. The accentuations are to propose a method which put least impact on sound signals. As each steganography strategy thinks of a few overheads and

furthermore brings about expanding the span of audio flags so overheads and optimality is additionally considered in this exploration work. Distinctive measurements will be figured which will be utilized to contrast proposed ideal system and accessible techniques. To do execution correlation the consequence of proposed calculation will be contrasted and some notable sound acknowledgment calculation.

CHAPTER 4

IMPLEMENTATION

4. LSB (LEAST SIGNIFICANT BIT)

Least Significant bit (LSB) coding is the not difficult approach to embed information clinched alongside an sound document. Eventually substituting the scarcest gigantic bit of every looking at side of the point with a double message, LSB coding takes under attention a considerable measure about majority of the data should a chance to be encoded. Information transmission rate clinched alongside LSB coding will be 1 kbps for every khz. Clinched alongside A percentage about LSB coding usage, two any rate as huge odds of a test need aid substituted supplanted with two message odds. This stretches those measure of majority of the data that could be encoded also expands the measure for hailing something like noise in the sound document Additionally[38].

With remove an secret message starting with an LSB encoded sound file, those collector needs get of the tests about course of action are used as a and only those introducing technique. Typically, those secret message period to make encoded may be more diminutive over those aggregate amount for tests alongside an sound record. One must decide that how to lift the subset of tests that will holds those secret message and pass on that decision of the recipient.

LSB coding, a chance to be that Similarly as it may, the two any rate as critical odds of a tests are substituted for two message odds. This extends the measure for data that might make encoded, also assembles those measure for advancing around noise in the sound record. Accordingly, you quit offering on that one ought on Think as of the indicator content preceding settling on the LSB operation should use. For instance, a sound record that might have been recorded done a clamoring metro station might blanket low-piece encoding upheaval. On the inverse side, an comparative commotion might a chance to be discernable done an audio record holding a piano solo.

The collector Additionally need entry of the secret key enter also data of the pseudo discretionary number generator, empowering the unpredictable progression of example should be remade. Checks must a chance to be set up, be that Likewise it may, should stay with the pseudo discretionary amount generator starting with making a comparative illustration rundown twice.

A crash might happen the place an test authoritatively modified for some part of the message will be balanced yet again[39]. The issue about crashes might a chance to be succeed Toward checking each a standout amongts the sample that bring been used existed. Another methodology will be with figure the subset for tests Eventually perusing method for an pseudo discretionary phase of the entire situated utilizing a secured hash fill in. This system show that a comparable record may be never made more than once.

Audio Stream Sample(16-bits)	"Hi" in binary	Stego audio stream(w embedded message)
1101111011001001	0	1101111011001000
0001100001100110	1	0001100001100111
1110010111011010	0	1110010111011010
0001100001100000	0	0001100001100000
1110000111010110	1	1110000111010111
0000101100100000	0	0000101100100000
1111100011000111	0	1111100011000110
0100111101011010	0	0100111101011010
0100000001100011	0	0100000001100010
0011101101001110	1	0011101101001111
0110000000110010	1	0110000000110011
1000110101011100	0	1000110101011100
0110001010100010	1	0110001010100011
1100100001000000	0	1100100001000000
0000001011111011	0	0000001011111010
1101110011000101	1	1101110011000101

Fig 4.1. LSB Audio coding example

Fig 1. 8 illustrates how the message "Hi" is encoded clinched alongside An 16-bit caliber sound example utilizing the LSB strategy. Here those secret majority of the data may be "Hi" and the blanket record may be an sound document. "Hi" is on be

installed inside the sound document. Initial the secret data “Hi” and the sound record would changed over under touch stream. The any rate as noteworthy section of the sound document will be displaced Toward those spot stream for mystery majority of the data “Hi”. The coming about record following embedding mystery data “Hi” is known as Stego-file.

4.1. Standard LSB

Information hide at all audio bits odds about sound samples in the the long haul space may be a standout amongst the simplest calculations with high information rate about extra data. The LSB watermark encoder Typically selects an subset from claiming every one accessible group sound tests select by a secret enter.

The substitution operation on the LSB is performed for this subset, the place the odds should a chance to be disguised content the primary bit values. Extraction handle effortlessly recovers those watermark by examining those estimation of these odds starting with those callous stego documents protest[40]. In this manner, the decoder needs each a standout amongst the examples of the stego heartless record that were used amid those inserting technique. Those unpredictable determination of the samples used for introducing displays low force included substance white gaussian clamor (AWGN). That actuality limits those amount for LSB that camwood make modified amid watermark implanting.

The vital point of view of the LSB coding method may be an watermark channel bit rate; usage of just a absolute LSB of the host sound samples provides for cutoff for 44.1 kbps Also a low computational quality. Those undeniable obstacle is significantly low robustness, due to truth that clear unpredictable transforms of the LSB obliterate the coded watermark.

Likewise those amount of used LSB amid LSB coding additions or, equally, profundity of the balanced LSB layer winds up detectably bigger, probability for making the introduced message factually perceptible increases Also perceptual straightforwardness from claiming stego articles is reduced. There will be a most distant purpose for those profundity of the used LSB layer On each sample for group callous record that could make used for information concealing.

Subjective tuning in test exhibited that, the practically amazing LSB profundity that might be used to LSB built watermarking without bringing over perceptible perceptual bending is the fourth LSB layer when 16 odds to every example would used to heartless successions. Those tests were performed with an broad amassing of audio example wave What's more people with Different framework Furthermore melodic background. None of the attempted sound plans needed perceptual antiques At the fourth LSBs need been used for majority of the data stowing away, despite the certainty that to specific music styles, those most distant side of the point is respectably higher over those fourth LSB layer. Quality of the watermark, embedded use those LSB coding strategy, increases with augment of the LSBs profundity used to information sound. Along these lines, transform about watermark quality obtained Eventually Tom's perusing increase for profundity of the used LSBs layer is compelled by perceptual straightforwardness bound, which may be those fourth LSB layer for those standard LSB coding count.

4.2 Modification LSB

This method could move the side of the point about restriction to clear majority of the data coating dependent upon to heartless starting with the fourth LSB layer of the 6th LSB layer, using a two-stage approach[41]. In the introductory step, An watermark touch is introduced under the ith LSB layer of the group heartless using a LSB coding procedure. In the second step, those inspiration noise achieved Eventually Tom's perusing watermark introducing will be shaped keeping clinched alongside personality those end objective to change its sound properties.

The standard LSB coding procedure essentially replaces those exceptional group callous bit in the ith layer (i=1,…..,16) with the bit from the watermark touch stream. For those circumstances when those 1st What's more watermark bit would dissimilar What's more ith LSB layer is used for introducing those confuse achieved by watermarking may be 2i[1] quantization steps (QS)(amplitude go is [-32768, 32767]).

The introducing screw up may be certain Assuming that the To begin with bit might have been 0 Furthermore watermark touch is 1what's more, the opposite best approach around. The magic considered perfect those suggested LSB count is watermark bit implanting that reasons unimportant inserting bowing of the group

callous. Obviously, In only a solitary of 16 odds in An example will be settled Also proportional of the watermark bit, exchange odds might make flipped with a particular limit objective will limit those inserting confuse.

To illustration, On those principal sample regard might have been (0. 01000)2=(8)10, and the watermark spot is zero is on make embedded under fourth LSB layer, as opposed regard (0. 00000)2=(0)10, that might those standard computation deliver, those suggested computation produces test that need regard (0. 00111)2=(7)10, which is essentially a greater amount closer of the interesting one. Nonetheless, those extraction figuring proceeds Concerning illustration before; it Exactly recovers the watermark spot Toward examining the touch a motivator starting with the predefined LSB layer in the watermarked heartless instance.

In the implanting calculation, those (i+1)th LSB layer (bit ai) will be primary transformed Toward consideration of the available message bit. Toward that point, the computation provided for underneath will be run. On the off possibility that that those touch ai oblige not a chance to be changed whatsoever because of constantly currently In a correct esteem, no action is brought with that flag sample.

To conceal a message done wave test get person bearer unit, place one spot of the message under the any rate fourth bit of the transporter unit, flip whatever is left particular case Furthermore create those changed unit of the objective stream.

LSB coding may be clarified in the taking after procedure:.

1. Read one example from the wave stream.

2. Get the following two odds from the present message byte.

3. Spot it in the present 4th Furthermore 3rd spot of the test.

4. Flip whatever is left 2 odds As needs be.

5. Duplicate whatever remains of those wave without progress.

4.3 PROPOSED LSB TECHNIQUE WITH INCREASED CAPACITY

4.3.1 Techniques and Algorithm

In the modified LSB encoded methodology we are seen that the fourth piece is set by the mystery message[42]. If the illustration bits are not comparable to the secret message bit we at that point basically flipped whatever is left of the bits of that given case. our proposed exhibit we reclaim to back two bits from the mystery message and as opposed to changing a solitary piece in a case we change two bits (fourth and third position) of the case. If there is change in this two bits we flip rest of the LSB for the most part there is no change. For example, if the one of a kind case regard was (0...01000)2=(8)10, and the watermark bits 01 are to be introduced into fourth and third LSB layer, the standard computation will convey the regard (0...00000)2=(0)10 to embed the principal watermark bit and for the second piece we require another specimen, the changed figuring produces test that has regard (0...00111)2=(7)10, which is fundamentally more closer to the first however here similarly we require another specimen to embed the second watermark bit. Our proposed computation will convey (0...00111)2 = (7)10 which is proportionate to the regard conveyed by balanced LSB methodology yet this case contains two watermark bit (here 0 and 1) instead of one piece. So we can express that with a comparable piece mistake we extended the farthest point of the case to conceal more secret message.

Clearly those recommended methodology displays more diminutive slip What's more higher limit Throughout water-mark inserting. The mystery message may be completely embedded At we would endeavoring two embed great to nothing qualities then again At we need aid introducing 1 touch regard that point final one 4 odds would not persuading whatever example should make inserted. On the off possibility that the fourth LSB layer may be utilized, the out and out lapse worth ranges from 1 on 4 QS, same time those standard system to comparable states reasons reliable out and out slip of 8 QS. Those typical vitality from claiming exhibited upheaval may be in this lifestyle 9. 31 db more diminutive On the suggested LSB coding system is used. Previously, development on reducing target personal satisfaction measure, communicated Likewise indicator to commotion proportion (SNR) value, suggested system presents, in the second venture for implanting, upheaval shaping keeping clinched alongside mind the limit objective on increase perceptual straightforwardness of the technique. An tantamount idea, known as slip dispersion

strategy is regularly used Similarly as a and only change about certified shading portraits will palette built shading portraits. For our calculation, introducing lapse is spread of the four again should go examples, Likewise example that would precursors of the display example can't make altered on the fact that information odds need Similarly as from claiming Right away been introduced under their LSBs. Tell e(n) imply those introducing slip of the case a(n). To those occurrence for inserting under those fourth LSB layer, the Emulating four consecutive example of the host heartless are transformed agreeing to these expressions:.

$$a(n+1)=a(n+1)+be(n)c \quad a(n+3)=a(n+3)+be(n)c/3$$

$$a(n+2)=a(n+2)+be(n)c/2 \quad a(n+4)=a(n+4)+be(n)c/4$$

The place (bAc) signifies carpet operation that adjusts An of the closest entirety amount not precisely or equal on a. Slip scattering shapes enter drive clamor, exhibited by LSB inserting, Eventually spreading it Also evolving its assignment will a perceptually better-tuned person. Effect may be practically underscored amid tranquil times about audio also on parts for low progression e.g. Broad essentials or maximums. The both introducing steps commonly augment those subjective nature of heartless stego address. Thusly, we anticipate that, using the recommended two-stage calculation, we might expand those profundity of watermark inserting additional inaccessible over those fourth LSB layer What's more for in way augment calculation's generosity towards noise extension.

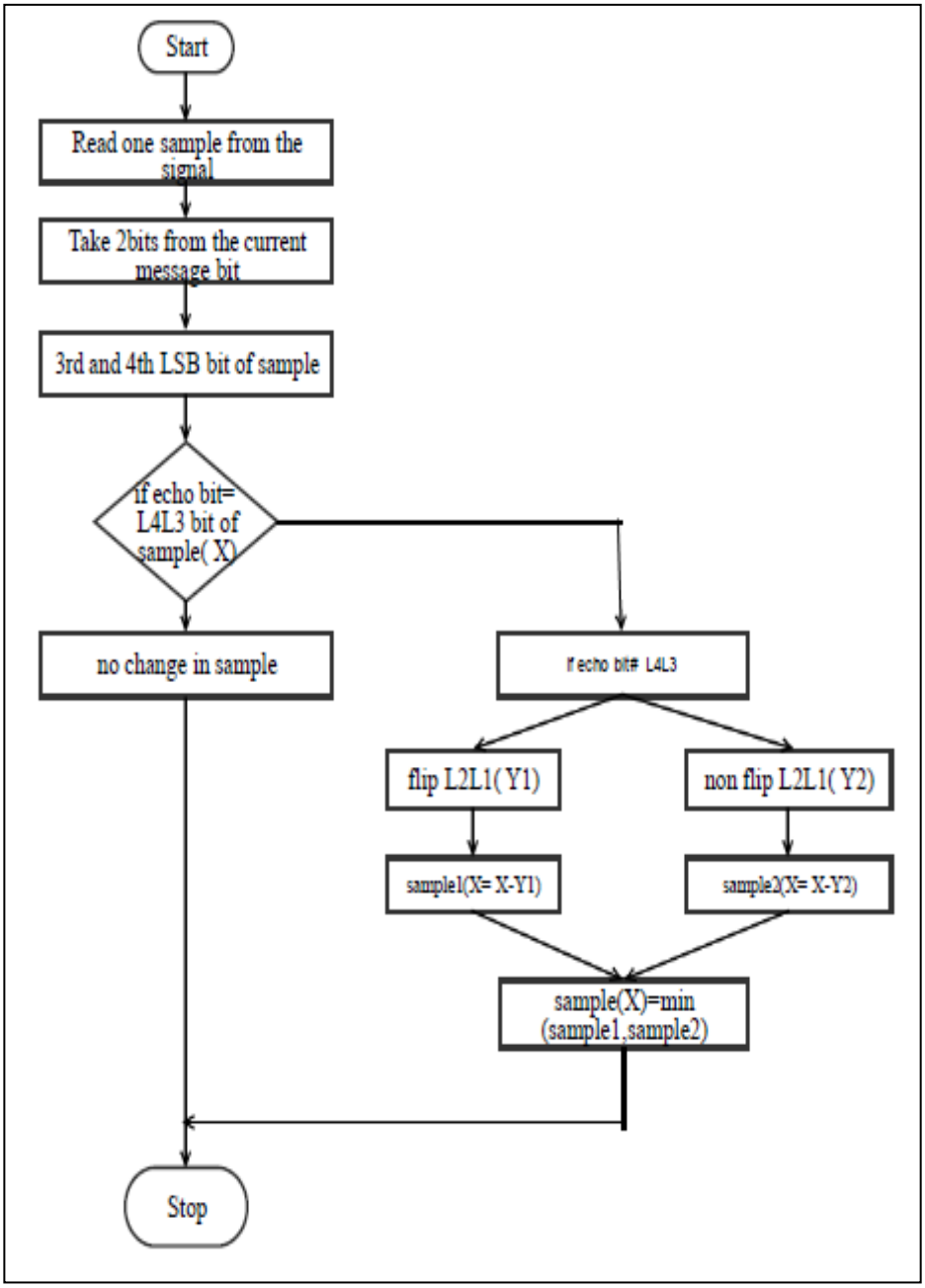


Fig 4.2. Flow chart of proposed Algorithm using LSB Techniques

4.3.2 flipping and non-flipping the bits of audio file

```
% Flipping Operation %

for i=1:r

    if i==r

        break;
```

```
        end
        if stego_bit(1)==X(3) | stego_bit(2)==X(4)
            Y1(i)=X(i);
% No Flip
            sample1(i)=X(i)-Y1(i);
            bit_error_embedd(i)=sqrt((X(i)-sample1(i))^2)/sample_rate;
            set(handles.axes1,'Visible','on');

        else

% Flipping
            Y2(i)=X(i+1);
            Y2(i+1)=X(i);
            sample2(i)=X(i)-Y2(i);

            if i==2
                if sample2(i)<0
                    sample2(i)=0;
                else
                    sample2(i)=1;
                end
            end
```

```
        if i==2
            if sample2(i)<0
                sample2(i)=0;
            else
                sample2(i)=1;
            end
        end
        bit_error_embedd(i)=sqrt((X(i)-sample2(i))^2)/sample_rate;
    end
end
```

For example:-

let the original audio signal be **1001**

let the stego bit (echo) be **10**

Case 1: L4L3 =Stego bit

No change in the sample

i.e L4L3 are the fourth and third bit of the original audio sample.

Case 2: If L4L3 not equal to Stego bit

Two cases will arise

Case 1: flip L2L1 bits of the original audio sample

Case 2: no flip of L2L1 bits of the original sample

Original audio signal **1001**

Case 1: The stego bit to be added is **00**

After adding, two outputs will come

i.e **001(no flip case) and 0010 (flip case)**

Case 2: The stego bit to be added is **01**

After adding, two outputs will come

i.e **0101(no flip case) and 0110(flip case)**

Case 3: The stego bit to be added is **10**

After adding, two outputs will come

i.e **1001(no flip case) and 1001(flip case)**

Case 4: The stego bit to be added is **101**

After adding, two outputs will come

i.e **1101(no flip case) and 1110(flip case)**

CHAPTER 5

EXPERIMENTAL RESULTS

Adjusted LSB watermarking figuring was attempted on different sound courses of action from different music different styles (pop, shake,Guitar, jazz). The sound parts are picked with the objective that they address a sweeping extent of music sorts, i.e. sound catches with different dynamic and spectual qualities. All music sample have been watermarked using the proposed and balanced LSB watermarking computation. Fastens was 44.1 kHz inspected mono sound records, addressed by 16 bits for each specimen. Traverse of the examples stretched out from 10 to 15 seconds.

Wave file	**Bit Rate**	**First bit Stego of errors**	**Second bit Stego of errors**	**1bit stego for bit error rate**	**2bit stego for bit error rate**
1	64	27	20	.0814	.0595
2	64	21	31	.0626	.0939
3	64	41	09	.1251	.0251
4	64	16	31	.0460	.0939
5	64	26	31	.0782	.0939
6	87	46	12	.1407	.0345
7	87	25	25	.0751	.0751
8	175	22	21	.0718	.0595
9	177	38	15	.1157	.0438
10	177	27	18	.0812	.0532
11	177	41	13	.1251	.0376

Table 5.1. Comparison between 1st and 2nd bit embedding

Outcomes of subjective tests seen that the bit mistake rate is high when we are using 64 kbps test sound for proposed LSB. In any case, when we are going for the higher bits kbps test sound then the bit rate is lesser and it is restricted distinguishably. Likewise, a basic change in control against flag planning control can be obtained, as the shrouded bits can be embedded two LSB layers more distant than in the standard LSB procedure. Take a gander at the quality of the proposed count and the standard one, included substance white Gaussian noise was added to the examples of watermarked sound and bit error rate (BER) measured.

5.1 wave file:- Guitar

Total length of character 40

Text is :- I am amneet kaur I am amneet kaur

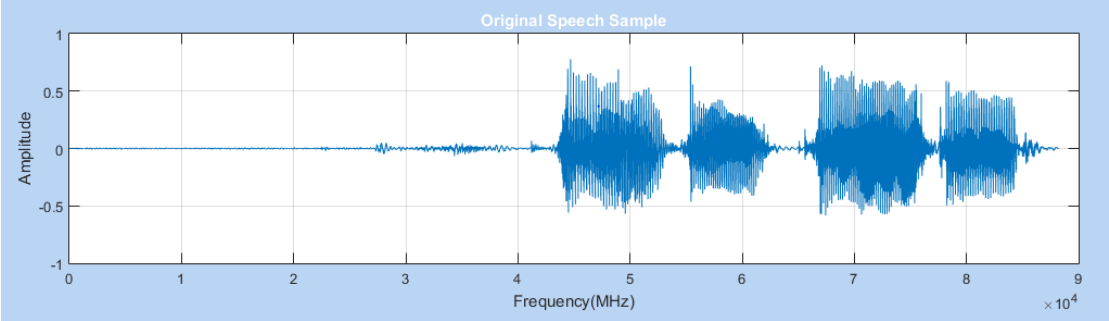


Fig 5.1. Original wave file of guitar

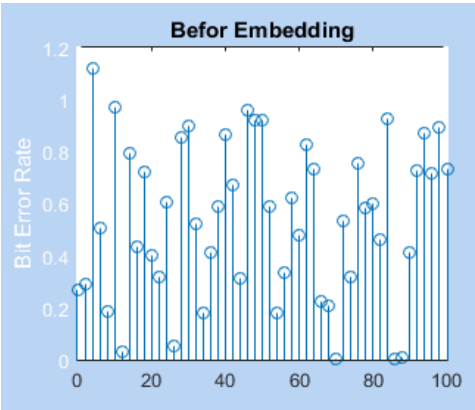


Fig 5.2. Befor Embedding wave file

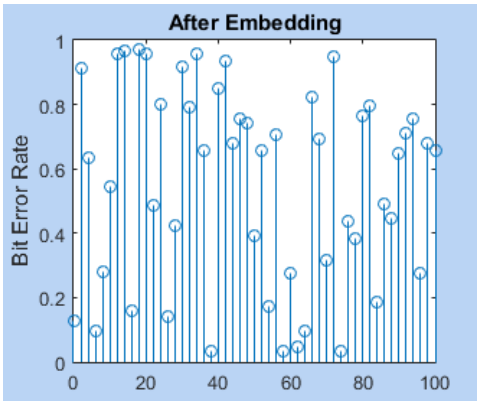


Fig 5.3. After Embedding wave file

5.2 wave file:- Piano

Total length of character 40

Text is :- I am amneet kaur I am amneet kaur

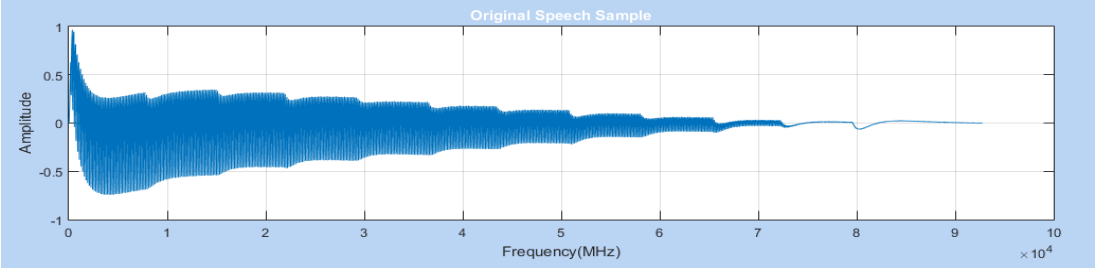


Fig 5.4. Original wave file of piano

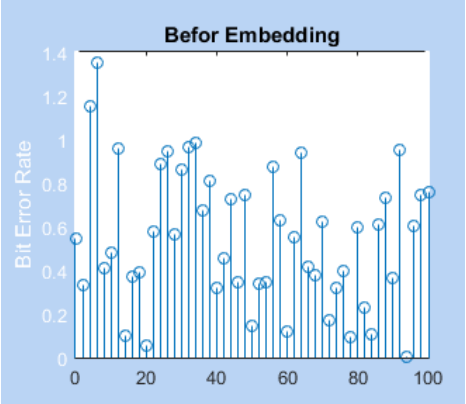


Fig 5.5. Before Embedding wave file

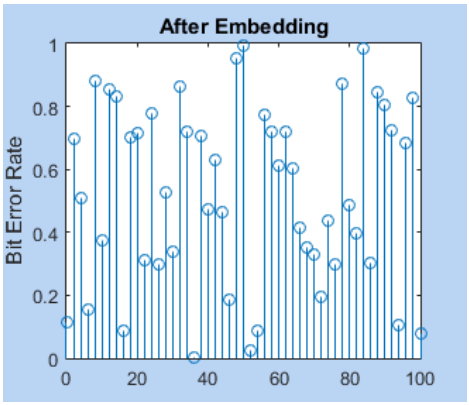


Fig 5.6. After Embedding wave file

5.3 wave file:- Pop

Total length of character 40

Text is :- I am amneet kaur I am amneet kaur

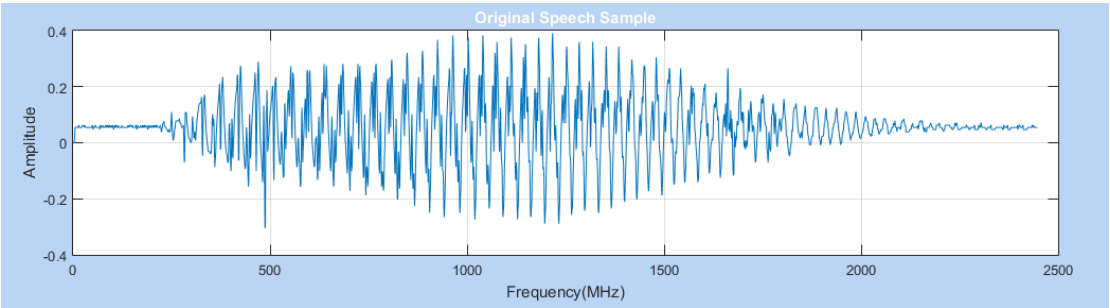
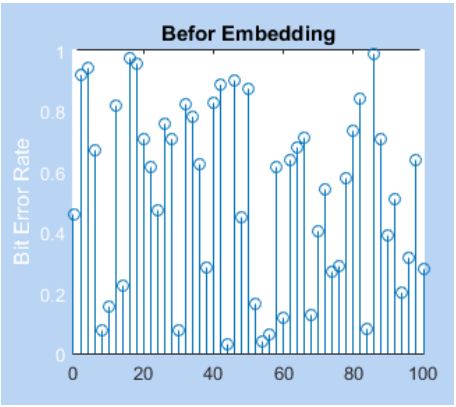


Fig 5.7. Original wave file of pop



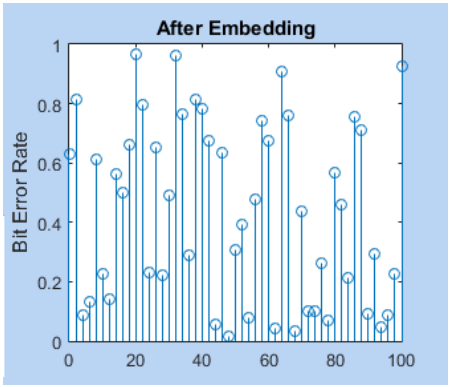


Fig 5.8. Before Embedding wave file

Fig 5.9. After Embedding wave file

CHAPTER 6

CONCLUSION AND FUTURE SCOPE

We show an adroit structure for steganography utilizing LSB encoding for sound information. The probability of the check may be that two watermark bits would embeddings which provides for the irrelevant mutilation of the settled period have sound for secondary most distant purpose. Tuning in test exhibited that depicted figuring wins Likewise will bringing no extraordinary positions should implant secret information without impacting those perceptual straightforwardness of the watermarked sound signal. Those conformity over control over vicinity about included substance change may be undeniable, as those recommended check gets to a general feeling cut down bit screw up rates over the standard estimation for a sharp outline work, the place the layer will a chance to be Therefore picked Eventually Tom's perusing the structure Furthermore a solitary position will be used to spread data, so we needed more no for test on hidden the puzzle substance.

Future Scope:-

Steganography has various disadvantages when contrasted with encryptions.

- It require a tone of overheads to conceal a moderately some bits of data.
- Once a framework is found its moves toward becoming essentially useless.
- This issue also can be overcome if the additional technique relies upon some kind of key.
- On the other hand a message can be first encoded and afterward shrouded utilizing steganography

REFERENCES

[1] W, Peter. "*Disappearing Cryptography: Information Hiding: Steganography & Watermarking*", (second edition). San Francisco: Morgan Kaufmann. pp.192-213, march 1992.

[2] Fabien, A. P. Petitcolas, R. J. Anderson, M. G. Kuhn,"*Attacks on Copyright*", University of Cambridge, April 1998.

[3] H. Wu, H. Wang, C. Tsai and C. Wang, "*Reversible image steganography scheme via predictive coding*". June (2010), ISSN: 01419382, pp. 35-43.

[4] Chandrakar, Pooja, M. Choudhary, and C. Badgaiyan. *"Enhancement in Security of LSB based Audio Steganography using Multiple Files*." International Journal of Computer Applications 73 (2013).

[5] Singh, P. Kumar, H. Singh, and K. Saroha. "*A survey on Steganography in Audio*", National Conference on Computing for Nation Development, Indiacom. 2009.

[6] P. N. Basu, T. Bhowmik,'On Embedding of Text in Audio – A case of Steganography' International Conference on Recent Trends in Information, Telecommunication and Computing.

[7]Kumar, H.; Anuradha "Enhanced LSB technique for audio steganography". Computing Communication & Networking Technologies (ICCCNT), 2012 Third International Conference o*n,* On page(s): 1 - 4.

[8] Keeping Secrets Secret: Steganography with .NET – http://www.devx.com/dotnet/Article/22667.

[9] Cole, Eric. - "Hiding in Plain Sight: Steganography and the Art of Covert Communication".

[10] "Steganography FAQ" - Aelphaeis Mangarae [Zone-H.Org] March 18th 2006, http://www.infosecwriters.com/text_resources/pdf/ Steganography_AMangarae.pdf.

[11] M. Pooyan, A. Delforouzi, *"LSB-based Audio Steganography Method Based on Lifting WaveletTransform",* in Proc. 7th IEEE International Symposium on Signal Processing and Information Technology (ISSPIT'07), December 2007, Egypt.

[12] Brian, J., Yuliya K. and Andrew, L.Fröhlich.2006. audio Steganography Dec 13.

[13] Cedric, T., Adi, R.,Mcloughlin, I.: Data concealment in audio using a nonlinear frequency distribution of PRBS coded data and frequency domain LSB insertion, Proc. IEEE Region 10 International Conference on Electrical and Electronic Technology, Kuala Lumpur, Malaysia, 275-278.

[14] Sridevi, R., A. Damodaram, and S. V. L. Narasimham. "*Efficient method of Audio steganography by modified LSB algorithm and strong encryption key with enhanced security*". Journal of Theoretical & Applied Information Technology 5.6 (2009).

[15] Cedric, T., Adi, R., Mcloughlin, I. Data concealment in audio and frequency domain LSB insertion, Proc. IEEE Region 10 International Conference on Electrical and Electronic Technology, Kuala Lumpur, Malaysia, 275-278.

[16] R. Anderson, F. Petitcolas: *On the limits of the steganography,* IEEE Journal Selected Areas in Communications, VOL .16, NO. 4, MAY 1998.

[17] Fridrich, J., Goljan, M., Du, R.: 2002 Lossless Data Embedding – New Paradigm in Digital Watermarking, Applied Signal Processing, 2002, 2, 185-196.

[18] S. Kumar, B. Barnali, G. Banik," *LSB Modification and Phase encoding Technique of Audio Steganography Revisited*". Vol.1 (4) IJARCCE 2012.

[19] N. T. Delgarm, "*Speech Watermarking*", M.Sc. Thesis, Comptuer Engineering Department, Sharif University of Technology, Tehran, IRAN, May 2006.

[20] I. Cox, M. Miller and J. Bloom, 2003.Digital Watermarking Morgan Kaufmann Publishers, San Francisco, CA, 2003.

[21] Bender W, Gruhl D & Morimoto N (1996) "Techniques for data hiding". IBM systems Journal 35(3): p 313–336.

[22] "audio steg: methods", Internet publication on www.snotmonkey.com"http://www.snotmonkey.com/work/school/405/methods.html"

[23] M. Asad, J. Gilani, A. Khalid, “Three Layered Model for Audio Steganography”, 2012 International Conference on Emerging Technologies (ICET).

[24] L. Rana, S. Banerjee, “Dual Layer Randomization in Audio Steganography Using Random Byte Position Encoding” , International Journal of Engineering and Innovative Technology, Volume 2, Issue 8, February 2013.

[25] K. Gandhi, G. Garg, “ Modified LSB Audio Steganography Approach” International Journal of Emerging Technology and Advanced Engineering, Volume 3, Issue 6, June 2012, pp 158-161.

[26] B. Priyanka, K. Vrushabh, P. Komal, “Audio Steganography using LSB’’, International Journal of Electronics, Communication and Soft Computing Science and Engineering, March 2012, pp 90-92.

[27] A. Mane, G. Galshetwar, A. Jeyakumar, “Data Hiding Technique: Audio Steganography using LSB Technique”, International Journal of Engineering Research and Applications, Vol.2, No.4, May- June 2012, pp 1123-1125.

[28] S. S. Divya, M. R. M. Reddy, “Hiding Text In Audio Using Multiple LSB Steganography And Provide Security Using Cryptography“, International Journal of Scientific &Technology Research, Vol. 1, pp. 68-70, July 2012.

[29] G. Nehru and P. Dhar, “A Detailed Look Of Audio Steganography Techniques Using LSB And Genetic Algorithm Approach”, International Journal of Computer Science (IJCSI), Vol. 9, pp. 402-406, Jan. 2012.

[30] A. B. Gadicha, “Audio wave Steganography”, International Journal of Soft Computing and Engineering (IJSCE), Vol. 1, pp. 174-177, Nov. 2011.

[31] M. Zamani et.al , “A Secure Audio Steganography Approach”, International Conference for Internet Technology and Secured Transactions 2009.

[32] R. Sridevi, A. Damodaram and S. Narasimham, “Efficient Method of Audio Steganography by Modified LSB Algorithm and Strong Encryption Key With Enhanced Security”, Journal of Theoretical and Applied Information Technology, pp. 771-778, 2009.

[33] F. Djebbar, B. Ayad, K. A. Meraim and H. Hamam" Comparative study of digital audio steganography techniques" Djebbar *et al. EURASIP Journal on Audio, Speech, andMusic Processing* 2012.

[34] G. Nehru, P. Dhar "A Detailed look of Audio Steganography Techniques using LSB and Genetic Algorithm Approach" IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 1, No 2, January 2012.

[35] Jayaram P, Ranganatha H R and Anupama H S, "information hiding using audio steganography ",The International Journal of Multimedia & Its Applications (IJMA) Vol.3, pp. 86-96, Aug. 2011.

[36] Anderson, R, Bowman, Petticolas, F. On the limits of Steganography. IEEE Journal selected areas in Communication,16, 4, 474-481.

[37] Bassia, P., Pitas I., Nikolaidis N. Robust audio watermarking in the time domain, IEEE Transactions on Multimedia 3, 2,\ 232-241.

[38] Krista, B., 2004. Linguistic steganography: survey, analysis and robustness concerns for hiding information in text, Center for Education and Research in Information Assurance and Security, Tech report 2004.

[39] Mobasseri, B. Direct sequence watermarking of digital video using m-frames Proc. International Conference on Image Processing, Chicago, IL, 399-403.

[40] Roy, S., Manasmita M., 2011. A novel approach to format based test stegonography, International conference on communication computing and security, ICCCS 2011,Procidings by ACM with ISBN-978-1-4503- 0464-rourkela, Odisha, India.

[41] "Steganography FAQ" Aelphaeis Mangarae, march 18 2006.

APPENDIX A

PUBLICATION

[1] Amneet kaur and Dr. Sagnita roy, "High Data Rate Audio Steganography On Different Cover Files",in the 10th international symposium on foundations & practice of security(FPS 2017),October 23-24-25 2017 / Nancy, France.(communicated)

[2] Amneet Kaur and Yashika Garg, " A Case Study on Steganography and its Attacks", in International Journal of Engineering trends and technology, volume 47 Number 8, May 2017.

APPENDIX B

VIDEO PRESENTATION LINK

https://youtu.be/4WqVvkFzuSg

APPENDIX C

PLAGIARISM REPORT

Thesis

ORIGINALITY REPORT

%17	%12	%12	%5
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Roy, Sangita, Jyotirmayee Parida, Avinash Kumar Singh, and Ashok Singh Sairam. "Audio steganography using LSB encoding technique with increased capacity and bit error rate optimization", Proceedings of the Second International Conference on Computational Science Engineering and Information Technology - CCSEIT 12 CCSEIT 12, 2012. Publication	%4