International Journal of Trend in Scientific Research and Development (IJTSRD)
Special Issue – Active Galaxy
ISSN No: 2456 - 6470 | www.ijtsrd.com | Special Issue Publication

An Efficient Method For Text And File Encryption For Secure Data Transmission Through Audio Steganography

Dr S Hemalatha[1], Androse[2], E Sharmili[3]
[1]Professor/CSE, [2]Assistant Professor/CSE, [3]Student
Veltech Hightech Dr Rangarajan Dr Sakunthala Engineering College
Avadi, Chennai, India

ABSTRACT

Steganography is the skill and learning of script unseen messages in such a mode that apart from the transmitter and envisioned receiver even recognizes there is a unseen message. Steganography works by exchanging bits of unusable or idle data in systematic Audio file with bits of dissimilar, imperceptible information. This unknown material can be plain text or cipher text. In a computer-based audio Steganography structure, underground messages are surrounded in numeral sound. The furtive memo is surrounded by marginally moving the twofold order of a sound file. Implanting surreptitious messages in numeral sound is usually a more hard process than inserting messages in other media, such as numeral images. These procedures sort from quite modest algorithms that pullout gen in the form of gesture noise to more dominant methods that feat erudite signal processing techniques to pelt material. Thus the main persistence of this project is to enlighten using Audio Steganography we can direct texts or even transcript files secretly

Keywords: *Steganography, Cipher text, Embedding*

I. INTRODUCTION

People use cryptography to direct surreptitious messages to one alternative deprived of a third party administration the message. Steganography is a type of cryptography in which the undisclosed missive is unseen in a numeral sounds. While cryptography is anxious with the shield of the fillings of a missive or material, Steganography distillates on obscuring the very presence of such mails from recognition.

The time Steganography is modified from the Greek word steganographia, sense "roofed writing" and is taken in its current system to nasty the walloping of evidence secret other material. Obviously these methods date back during history, the key requests presence in couriering info during eras of war. With the discovery of numerical audio and pictures archives this has occupied on a complete new sense; making original methods for execution "alterable data hiding" as it is often named. This has many imaginable applications plus the patent watermarking of audio, video and still duplicate data. In digital media, Steganography is mainly leaning around the imperceptible broadcast of one form of evidence within another. In order for a facts hiding procedure to be successful it must adhere to two rules:

- The surrounded data must be invisible within its exporter medium (the audio file). The importer should display no properties that flag it as guarded, whether it is to the human visual/auditory organism or in better file size for the importer file.
- The embedded data must maintain its truthfulness within the carrier and should be easily removable, under the right surroundings, by the unloading party.

The current arrangement of Audio Steganography postures more boundaries on the selecting of audio files. User can excellent only wav files to encode. Further entrenching material into sound files is normally measured more tough than reports;

according to the human ear is enormously sensitive to worries in sound and can in fact detect such instability as low as one part in 10 million. The methods deliberated further afford users with a huge amount of choice and makes the technology more available to everybody.

II. OBJECTIVE

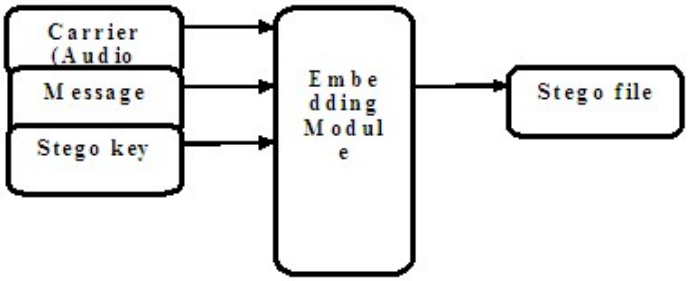

Fig. 1 Basic Audio Steganographic Model

The model for steganography is shown in Figure 1. Letter is the data that the dispatcher wishes to remain it isolated. Message can be bare text or cipher text type of file. Password is known as a stego-key, which authorizes that only the receiver who knows the agreeing translating key will be able to remove the message from a cover-file. The cover-filewith the furtive material is known as a stego-file.

The evidence whacking method involves of following two steps:

i. Documentation of dismissed bits in a cover-file. Dismissed bits are those bits that can he adapted without humiliating the eminence or abolishing the integrity of the cover-file.
ii. To entrench the furtive material in the concealment file, the dismissed bits in the concealment file is swapped by the bits of the furtive info.

III. DETAILED DESIGN

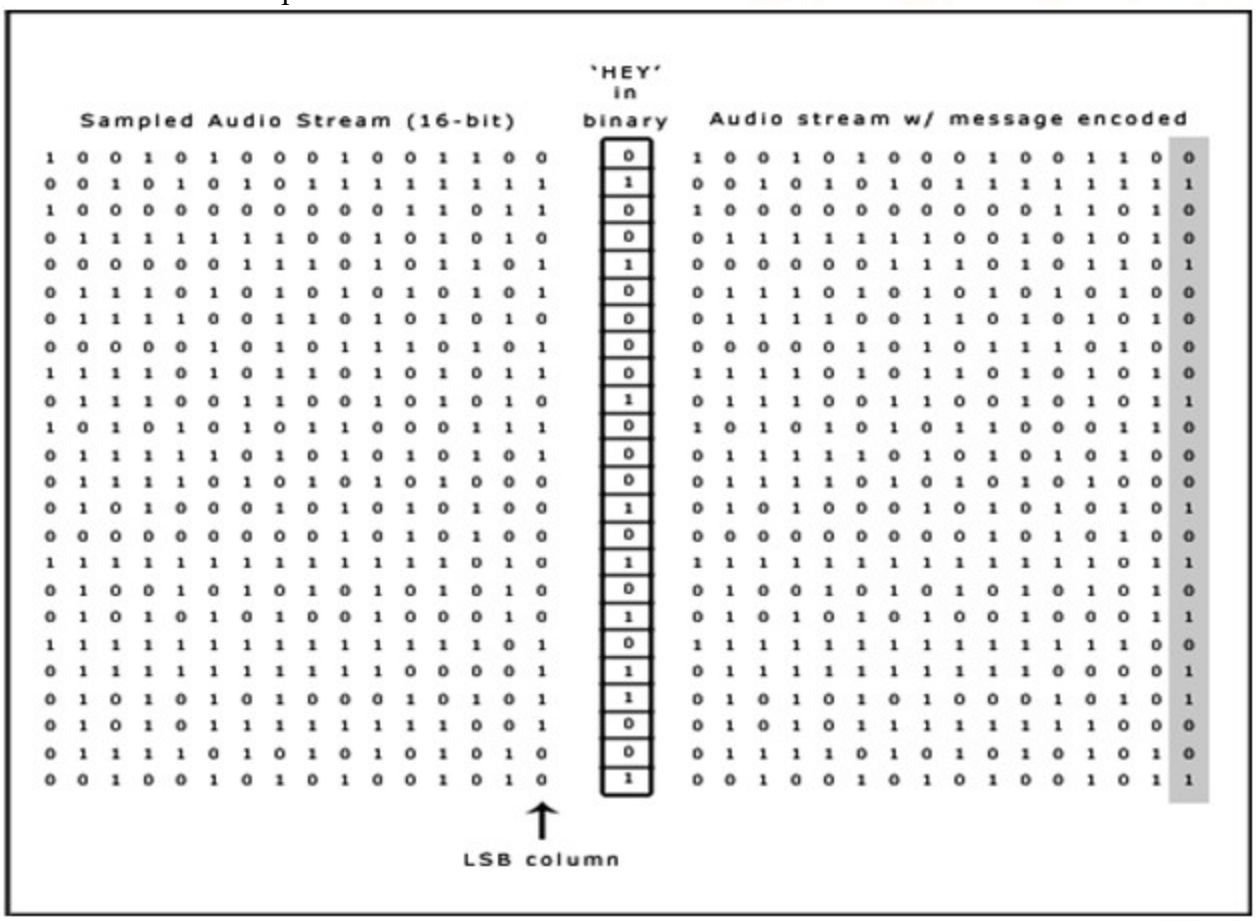

Fig 2. LSB Coding Example

This segment offering some joint means used in audio Steganography.

A. LSB CODING

Least significant bit (LSB) coding is the humblest technique to insert material in a cardinal audio file. By relieving the least substantial bit of every selection

point with a double missive, LSB coding consents for a huge total of data to be determined. The subsequent plot explains how the note 'HEY' is preset in a 16-bit CD quality model by the LSB method:

B. Standard LSB ALGORITHM:

It performs bit level handling to scramble the memorandum. The resulting steps are

1. Obtains the audio file in the form of bytes and transformed in to moment pattern.
2. Each appeal in memo is transformed in bit pattern.
3. Exchanges the LSB bit since audio with LSB bit from appeal in the memo

Algorithm: Improved/ Modified LSB embedding

if host sample a>0
if bit 0 is to be embedded
if ai−1=0 then ai−1ai−2...a0=11...1
if ai−1=1 then ai−1ai−2...a0=00...0 and
if ai+1=0 then ai+1=1
else if ai+2=0 then ai+2=1
...
else if a15=0 then a15=1
else if bit 1 is to be embedded
if ai−1=1 then ai−1ai−2...a0=00...0
if ai−1=0 then ai−1ai−2...a0=11...1 and
if ai+1=1 then ai+1=0
else if ai+2=1 then ai+2=0
...
else if a15=1 then a15=0

if host sample a<0
if bit 0 is to be embedded
if ai−1=0 then ai−1ai−2...a0=11...1
if ai−1=1 then ai−1ai−2...a0=00...0 and
if ai+1=1 then ai+1=0
else if ai+2=1 then ai+2=0
...
else if a15=1 then a15=0
else if bit 1 is to be embedded
if ai−1=1 then ai−1ai−2...a0=00...0
if ai−1=0 then ai−1ai−2...a0=11...1 and
if ai+1=1 then ai+1=0
else if ai+2=1 then ai+2=0
...
else if a15=1 then a15=0

In LSB coding, the ideal data broadcast amount is 1 kbps per 1 kHz. In specific implementations of LSB coding, though, the two slightest significant bits of a model are changed with two memo bits. This rises the total of facts that can be determined but also growths the quantity of causing sound in the audio file as well, one should contemplate the indication content previously determining on the LSB process to use. For example, a complete file that was verified in a hurried subway station would mask low-bit training noise. On the extra hand, the identical sound would be audible in a sound file covering a piano solo.

The main gain of the LSB coding process is low-slung computational complication of the procedure while its chief shortcoming : As the sum of cast-off LSBs during LSB coding increases or, equivalently, depth of the modified LSB layer becomes larger, chance of making the rooted memorandum statistically measurable growths and perceptual clearness of stego articles is declined. Low Bit Training is therefore an uninvited manner, generally due to its disaster to meet the Steganography prerequisite of being invisible.

IV. PHASE CODING

Phase coding talks the hitches of the noise-inducing approaches of audio Steganography. Phase coding trusts on the detail that the part mechanisms of complete are not as noticeable to the mortal ear as noise is. Slightly than announcing worries, the technique encodes the memo bits as phase shifts in the point band of a digital signal, realizing an quiet training in terms of signal-to-perceived sound ratio.

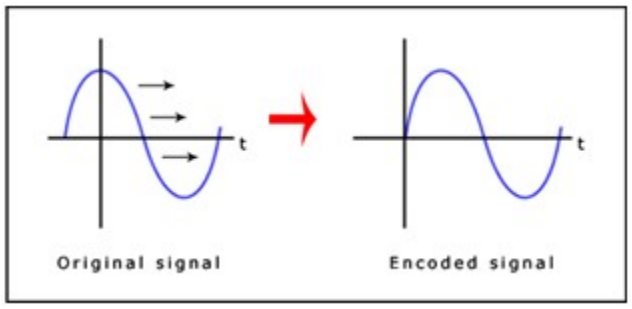

Fig 3. Phase Coding

The phase coding technique disruptions despondent the complete file into a sequence of N segments. A Discrete Fourier Transform (DFT) is applied to every section to generate a medium of the phase and magnitude. The phase alteration concerning every section is designed, the first segment (s0) has a reproduction complete phase of p0 created, and all extra sections have newly created phase frames. The new phase and original magnitude are combined to get the new segment, Sn. These new sections are then concatenated to generate the programmed production and the frequency remainders conserved. In demand to decrypt the secreted material the receiver must know the extent of the sections and the figures interval used. The first section is spotted as a 0 or a 1 and this directs where the communication starts.

This method has several gains over Low Bit Encoding, the supreme chief existence that it is imperceptible to the human ear. Like all of the systems designated so far nevertheless, its feebleness is still in its want of toughness to changes in the audio data. Any lone complete process or alteration to the documents would misrepresent the material and avoid its rescue.

A. ECHO HIDING

Echo hiding inserts its facts by making an resonance to the basis audio. Three limits of this Synthetic echo are used to hide the entrenched data, the stay, the decline rate and the preliminary generosity. As the suspension among the new foundation audio and the echo reduction it converts tougher for the human ear to differentiate among the two indications until ultimately a shaped shipper sound's resonance is just gotten as extra reverberation.

In addition, balance is diverse to signify the double message to be programmed. One counterbalance value signifies a binary one, and a second balance worth signifies a binary zero. If only one echo was formed from the innovative sign, only one bit of material could be programmed. Therefore, the creative indicator is wrecked down into chunks before the encrypting process begins. Once the training process is finalized, the chunks are concatenated back organized to create the absolute signal.

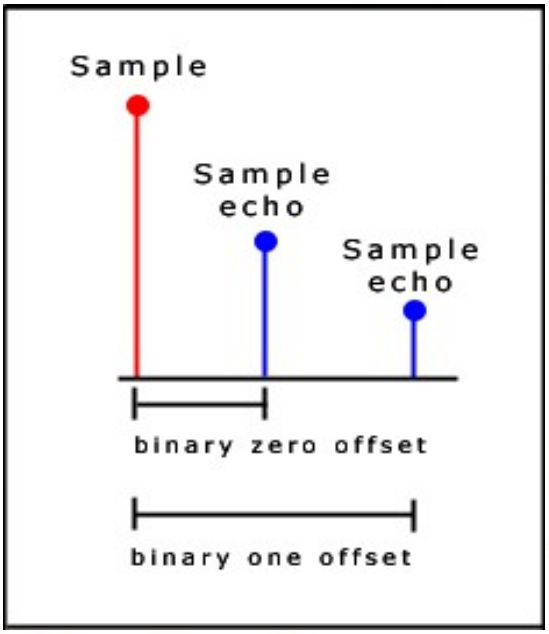

Fig. 4 Echo Hiding

Then the following algorithm (illustrated through pseudo code) is used to encode each block:

```
init(Block blocks[]) {
  for (int i=0; i < blocks.length; i++) {
    if (blocks[i].echoValue() == 0)
      blocks[i] = offset0(blocks[i]);
    else
      blocks[i] = offset1(blocks[i]);
  }
}
Block offset0(Block block) {
  return (block + (block - OFFSET_0));
}
Block offset1(Block block) {
  return (block + (block - OFFSET_1));
}
```

The chunks are recombined to produce the concluding signal. The "one" resonance signal is then grown by the "one" mixer signal and the "zero" echo signal is reproduced by the "zero" blender signal.

Then the two outcomes are extra composed to get the concluding signal. The final sign is less hasty than the one gained using the chief echo smacking

application. This is because the two blender echoes are balances of each other and that rise conversions are used in each indicator. These two features of the mixer signs produce flatter evolutions between resonances.

The following diagram summarizes the second implementation of the echo hiding process.

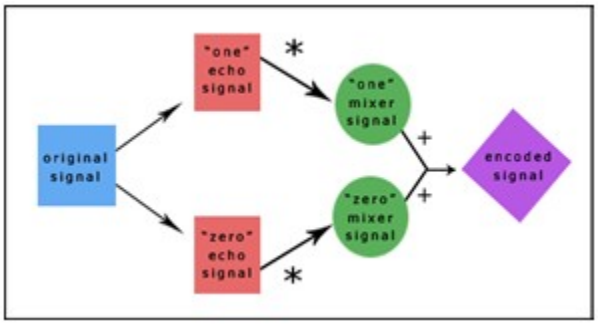

Fig. 5. Echo Hiding Concept

To excerpt the furtive missive from the stego-signal, the handset must be able to disruption up the signal into the same chunk arrangement used during the encrypting process. Then the autocorrelation purpose of the signal's range (the spectrum is the Forward Fourier Transform of the signal's frequency spectrum) can be used to interpret the memo since it discloses a spear at each echo time balance, agreeing the communication to be recreated.

Abundant like phase encoding this has significantly improved fallouts than Low Bit Encoding and types good use of exploration done so far in psychoacoustics. As with all audio file encoding, we find that employed in audio setups such as WAV is very costly, more so than with bitmap pictures in terms of the “file size to storage capacity” ratio. The program of audio files by e-mail or concluded the mesh is ample less prolific than pictures files and so is much further mistrustful in assessment. It permits for a tall data program rate and delivers greater strength once compared to the sound persuading methods.

B. SPREAD SPECTRUM

Spread spectrum organizations encrypt records as a dualistic sequence which audio like noise but which can be predictable by a receiver with the precise key. The system has remained used by the armed meanwhile the 1940s since the signals are rigid to jam or seize as they are mislaid in the contextual noise. Spread spectrum systems can be used for watermarking by identical the fine bandwidth of the surrounded data to the huge bandwidth of the medium.

Two varieties of SS can be castoff in audio Steganography: the direct-sequence and frequency-hopping structures. In direct-sequence SS, the top-secret message is blowout out by a endless called the chip rate and then tempered with a pseudorandom signal. It is then interweaved with the cover-signal. In frequency-hopping SS, the audio file's incidence spectrum is transformed so that it hops hurriedly between frequencies.

Spread Spectrum Steganography has substantial potential in secure infrastructures – marketable and military. Audio Steganography in aggregation with Spread Spectrum may deliver added layers of safety.

Spread spectrum programming practices are the most safe means by which to direct unseen messages in audio, but it can familiarize random sound to the audio thus generating the accidental of data loss. They have the possible to achieve better in selected areas than LSB coding, parity coding, and phase coding procedures in that it proposals a modest data show rate while also preserving a great level of sturdiness against exclusion performances

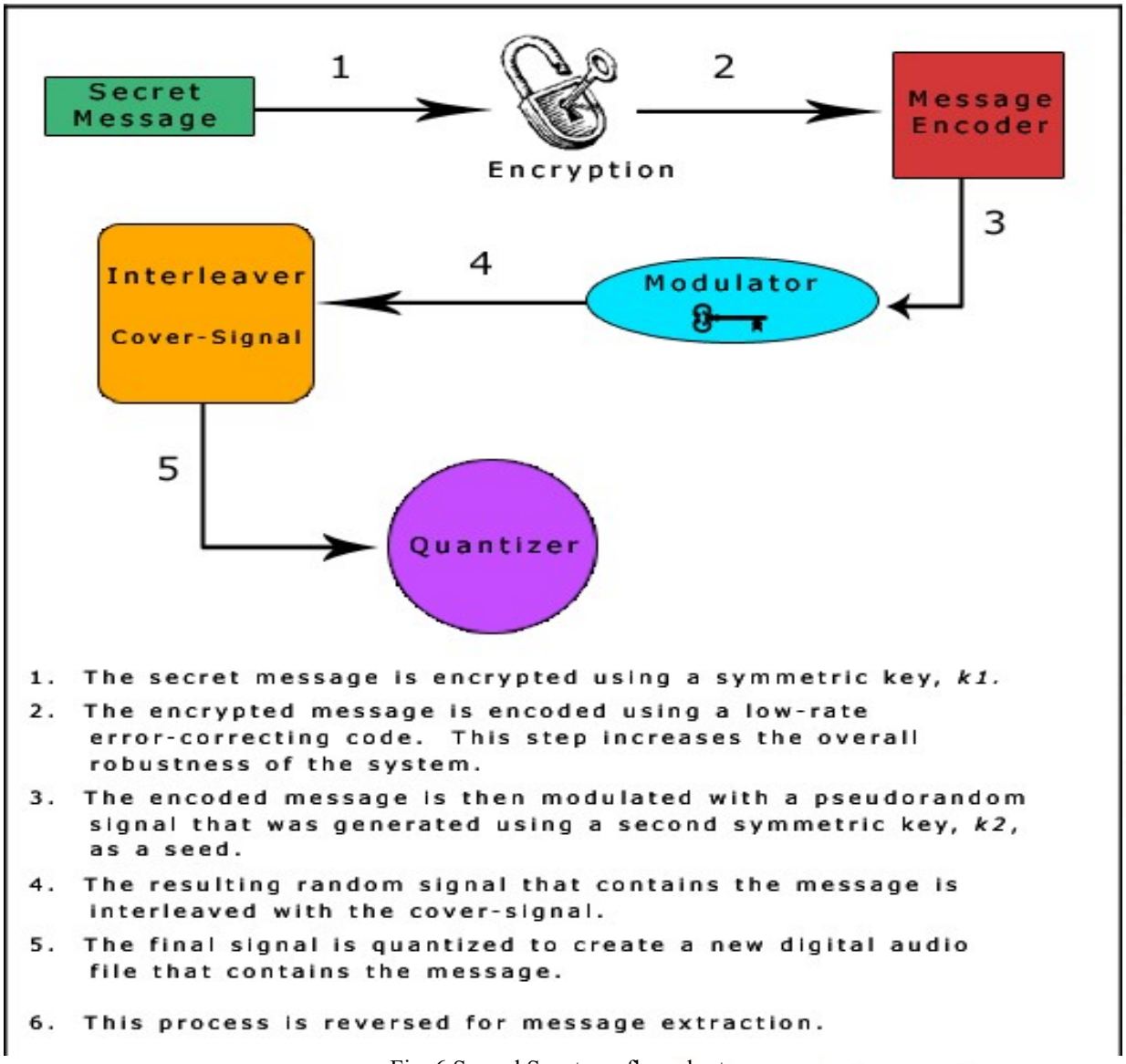

Fig. 6 Spread Spectrum flow chart

V. PROPOSED WORK

Audio based Steganography has the impending to obscure added information:

- Audio files are normally larger than pictures.
- Our hearing can be effortlessly tricked
- Insignificant fluctuations in plenty can store vast quantities of information
- The flexibility of audio Steganography is makes it very hypothetically powerful :
- The systems discussed afford users with a bulky amount of choice and makes the machinery more reachable to everyone. A party that demands to communicate can can, and noise loudness and then select the routine that best fits their qualifications. rank the significance of elements such as data communication rate, bandwidth, strength
- For example, two persons who just want to send the special secret message back and forward might use the LSB coding method that is easily executed. On the other hand, a large organization needing to protect its knowledgeable belongings from "digital pirates" may consider a more cultured method such as phase coding, SS, or echo hiding.
- Additional part of audio Steganography that makes it so clever is its ability to syndicate with remaining cryptography talents.
- Users no extended have to rely on one method alone. Not only can figures be encrypted, it can be hidden altogether.
- Many sources and types makes numerical analysis more difficult :
- Greater volumes of information can be embedded without audible degradation

- Many attacks that are mischievous against image Steganography algorithms (e.g. geometrical distortions, spatial scaling, etc.) cannot be applied against audio Steganography systems. Therefore, embedding information into audio seems more secure due to less steganalysis techniques for attacking to audio.
- As importance placed on the areas of copyright security, privacy safeguard, and observation increases, Steganography will continue to grow in significance as a safeguard appliance.
- Audio Steganography in certain addresses key issues brought about by the MP3 format, P2P software, and the need for a secure diffusion scheme that can maintain the confidentiality of the communicated information, even when passing through unconfident channels.

VI. EVALUATION

Steganography is not proposed to exchange cryptography but pretty to complement it. If a communication is encrypted and hidden with a steganographic method it provides an additional layer of security and decreases the chance of the hidden message being detected.

Steganography is still a fairly new thought to the common public although this is likely not true in the world of silence and surveillance. Digital watermark technology is currently being used to track the exclusive rights and rights of digital content. Efforts to expand the robustness of the watermarks are basic to ensure that the watermarks and embedded information can securely protect against watermarking attacks. With continuous improvements in technology it is ordinary that in the near future more effective and advanced practices in steganalysis will appear that will help law implementation to better detect illicit materials conveyed through the Internet.

Steganography goes well beyond simply hiding text material in an audio. Steganography spread on not only to digital audios but to other media as well, such as image files, communication channels, and other text and binary files.

VII. CONCLUSION AND FUTURE SCOPE

Thus a project with text encrypted via cryptography with DES algorithm. And a knowledge which is more controllable to everyone, along side a vast amount of texts can be hidden(approximately 200-250 char). With its skill to syndicate with existing cryptography technologies. Therefore effectively like embedding information into sound files made easier to operators.

Future Scope of this paper is the potentials of developments in audio steganography system with respect to dissimilar technique of data hiding in audio. This paper mostly thinks on only .wav format of audio files and can prolonged to a level such that it can be used for the dissimilar types of audio wave file formats like .au, .mp3, wma etc.,

REFERENCES

1. Ajay.B.Gadicha1, November 2011 “Audio Wave Steganography”, and International Journal of Soft Computing and Engineering (IJSCE), ISSN: 2231-2307, Volume-1, Issue-5.
2. MA Ahmed, LM Kiah, BB Zaidan, AA Zaidan, A Novel Embedding Method to Increase Capacity and Robustness of Low-bit Encoding Audio Steganography Technique Using Noise Gate Software Logic Algorithm.J. Appl. Sci.
3. Bandyopadhay, S. K.; Datta, B.; Dutta, K., 2011. “Information Hiding in Higher LSB Layer in an Audio Image”,International Journal of Advanced Research in Computer Science, Vol. 2, No. 3.
4. N Cvejic, T Seppiinen, Increasing the capacity of, LSB-based audio steganography, IEEE Workshop on Multimedia Signal processing. (St. Thomas, USA 2002)
5. N Cvejic, T Seppanen, Increasing Robustness of, LSB Audio Steganography Using a Novel Embedding Method, Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC04). vol. 2, (Washington, DC, USA, 2004).
6. N Cvejic, T Seppanen, Reduced distortion bit-modification for LSB audio steganography. J. Universal Comput. Sci. **11**(1), 56–65 (2005)
7. Y Erfani, S Siahpoush, Robust audio watermarking using improved TS echo hiding. Digital Signal Process. **19**, 809–814 (2009)