Implementation of ISS - IHAS (Information Security System – Information Hiding in Audio Signal) model with reference to proposed e-cipher Method

Prof. R. Venkateswaran
Department of CA, Nehru College of Management,
Research Scholar-Ph.D, Karpagam University
Coimbatore, TN, INDIA

Dr. V. Sundaram, Director
Department of CA, Karpagam College of Engineering
Affiliated to Anna University of Technology,
Coimbatore, TN, INDIA

***Abstract*— This paper shows the possibility of exploiting the features of E- cipher method by using both cryptography and Information hiding in Audio signal methods used to send and receive the message in more secured way. Proposed methodology shows that successfully using these Poly substitutions methods (Proposed E-Cipher) for Encode and decodes messages to evolve a new method for Encrypting and decrypting the messages.**

Embedding secret messages using audio signal in digital format is now the area in focus. There exist numerous steganography techniques for hiding information in audio medium.

In our proposed theme, a new model ISS-IHAS - Embedding Text in Audio Signal that embeds the text like the existing system but with strong encryption that gains the full advantages of cryptography. Using steganography it is possible to conceal the full existence of the original text and the results obtained from the proposed model is compared with other existing techniques and proved to be efficient for textual messages of minimum size as the size of the embedded text is essentially same as that of encrypted text size. This emphasis the fact that we are able to ensure secrecy without an additional cost of extra space consumed for the text to be communicated.

Keywords- Encryption; Decryption; Audio data hiding; Mono Substitution; Poly Substitution.

I. OBJECTIVES OF THE PROJECT

The main purpose of Audio steganography is to hide a message in some cover media, to obtain new data, practically indistinguishable from the original message, by people, in such a way that an eavesdropper cannot detect the presence of original message in new data. With computers and Networks, there are many other ways of hiding information, such as Covert channels, Hidden text within WebPages Hiding files in “Plain sight”, Null ciphers.

Today, the internet is filled with tons of programs that use steganography to hide the secret information. There are so many medias are used for digitally embedding message such as plaintext, hypertext, audio/video, still image and network traffic. There exists a large variety of steganographic techniques with varying complexity and possessing some strong and weak aspects.

Hiding information in text is the most popular method of Steganography. It is used to hide a secret message in every nth character or altering the amount of white space after lines or between words of a text message [1]. It is used in initial decade of internet era. But it is not used frequently because the text files have a small amount of redundant data. But this technique lacks in payload capacity and robustness. To hide data in audio files, the secret message is embedded into digitized audio signal. Audio data hiding method provides the most effective way to protect privacy. Key aspect of embedding text in audio files is that, no extra bytes are generated for embedding. Hence it is more comfortable to transmit huge amount of data using audio signal. Embedding the secret messages in digital sound is usually a very difficult process [2].

II. PROPOSED ISS – IHAS MODEL

The following IHAS Model provides a very basic description of the audio steganographic process in the sender side and receiver side.

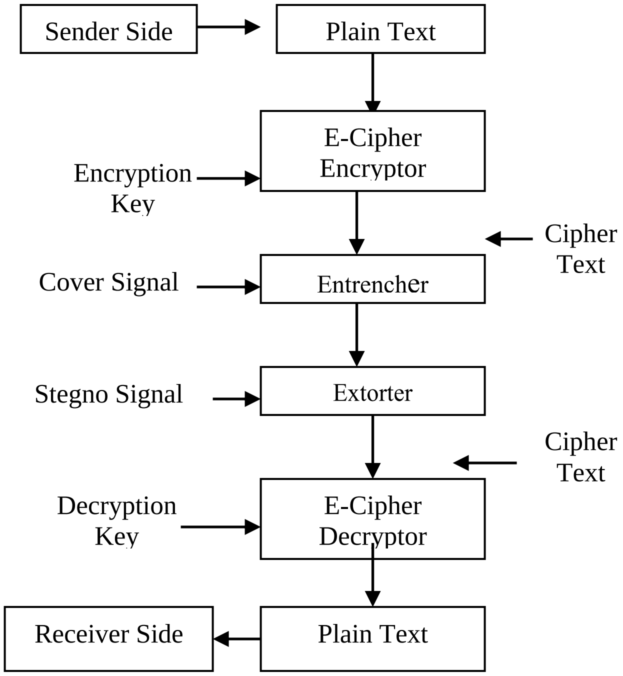
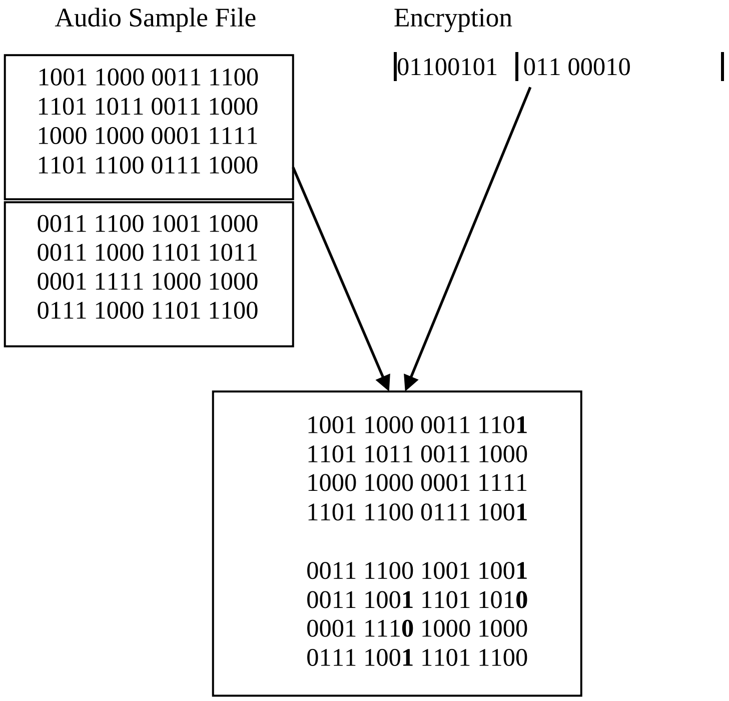


Fig 2.1 System Flow – ISS- IHAS model

The original text encrypted by E-Cipher using an encryption key. The model implements E-Cipher encryption as it proves to be more efficient. The encrypted text is passed on to Entrencher that embeds the encrypted text inside the cover signal which is in audio format *.wav resulting in stego signal. This process happens at sender side. This stego signal is communicated using Network medium. At the receiver side the stego signal is passed on to Extorter module that extracts embedded text from the audio signal that was used a s cover medium,. The resultant cipher text is then decrypted using E-cipher Decryptor module. The final plain text can then be used for further processing.



1001 1000 0011 1100
1101 1011 0011 1000
1000 1000 0001 1111
1101 1100 0111 1000

0011 1100 1001 1000
0011 1000 1101 1011
0001 1111 1000 1000
0111 1000 1101 1100

1001 1000 0011 110**1**
1101 1011 0011 1000
1000 1000 0001 1111
1101 1100 0111 100**1**

0011 1100 1001 100**1**
0011 100**1** 1101 101**0**
0001 111**0** 1000 1000
0111 100**1** 1101 1100

Fig. 2.2 ISS- IHAS encoding format

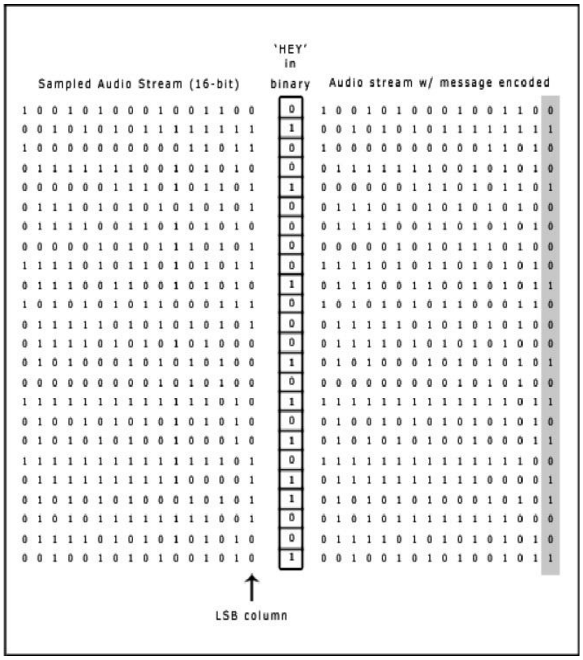
To hide a letter A & B to an digitized audio file where each sample is represented with 16 bits then the LSB bit of sample audio file is replaced with each bit of binary equivalent of the letter A & B[4].

III. PERSPECTIVE STUDY ON VARIOUS METHODS

In audio steganography, secret message is embedded into digitized audio signal which result slight altering of binary sequence of the corresponding audio file. There are several methods are available for audio steganography [3]. Some of them are as follows: -

LSB Coding:

Least significant bit (LSB) coding is the simplest way to embed information in a digital audio file. By substituting the least significant bit of each sampling point with a binary message, LSB coding allows for a large amount of data to be encoded. The following diagram illustrates how the message 'HEY' is encoded in a 16-bit CD quality sample using the LSB method:



Sampled Audio Stream (16-bit)	'HEY' in binary	Audio stream w/ message encoded
1 0 0 1 0 1 0 0 0 1 0 0 1 1 0 0	0	1 0 0 1 0 1 0 0 0 1 0 0 1 1 0 0
0 0 1 0 1 0 1 0 1 1 1 1 1 1 1 1	1	0 0 1 0 1 0 1 0 1 1 1 1 1 1 1 1
1 0 0 0 0 0 0 0 0 0 0 1 1 0 1 1	0	1 0 0 0 0 0 0 0 0 0 0 1 1 0 1 0
0 1 1 1 1 1 1 1 0 0 1 0 1 0 1 0	0	0 1 1 1 1 1 1 1 0 0 1 0 1 0 1 0
0 0 0 0 0 0 1 1 1 0 1 0 1 1 0 1	1	0 0 0 0 0 0 1 1 1 0 1 0 1 1 0 1
0 1 1 1 0 1 0 1 0 1 0 1 0 1 0 1	0	0 1 1 1 0 1 0 1 0 1 0 1 0 1 0 0
0 1 1 1 1 0 0 1 1 0 1 0 1 0 1 0	0	0 1 1 1 1 0 0 1 1 0 1 0 1 0 1 0
0 0 0 0 0 1 0 1 0 1 1 1 0 1 0 1	0	0 0 0 0 0 1 0 1 0 1 1 1 0 1 0 0
1 1 1 1 0 1 0 1 1 0 1 0 1 0 1 1	0	1 1 1 1 0 1 0 1 1 0 1 0 1 0 1 0
0 1 1 1 0 0 1 1 0 0 1 0 1 0 1 0	1	0 1 1 1 0 0 1 1 0 0 1 0 1 0 1 1
1 0 1 0 1 0 1 0 1 1 0 0 0 1 1 1	0	1 0 1 0 1 0 1 0 1 1 0 0 0 1 1 0
0 1 1 1 1 1 0 1 0 1 0 1 0 1 0 1	0	0 1 1 1 1 1 0 1 0 1 0 1 0 1 0 0
0 1 1 1 1 0 1 0 1 0 1 0 1 0 0 0	0	0 1 1 1 1 0 1 0 1 0 1 0 1 0 0 0
0 1 0 1 0 0 0 1 0 1 0 1 0 1 0 0	1	0 1 0 1 0 0 0 1 0 1 0 1 0 1 0 1
0 0 0 0 0 0 0 0 0 1 0 1 0 1 0 0	0	0 0 0 0 0 0 0 0 0 1 0 1 0 1 0 0
1 1 1 1 1 1 1 1 1 1 1 1 1 0 1 0	1	1 1 1 1 1 1 1 1 1 1 1 1 1 0 1 1
0 1 0 0 1 0 1 0 1 0 1 0 1 0 1 0	0	0 1 0 0 1 0 1 0 1 0 1 0 1 0 1 0
0 1 0 1 0 1 0 1 0 0 1 0 0 0 1 0	1	0 1 0 1 0 1 0 1 0 0 1 0 0 0 1 1
1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 1	0	1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0
0 1 1 1 1 1 1 1 1 1 1 0 0 0 0 1	1	0 1 1 1 1 1 1 1 1 1 1 0 0 0 0 1
0 1 0 1 0 1 0 1 0 0 0 1 0 1 0 1	1	0 1 0 1 0 1 0 1 0 0 0 1 0 1 0 1
0 1 0 1 0 1 1 1 1 1 1 1 1 0 0 1	0	0 1 0 1 0 1 1 1 1 1 1 1 1 0 0 0
0 1 1 1 1 0 1 0 1 0 1 0 1 0 1 0	0	0 1 1 1 1 0 1 0 1 0 1 0 1 0 1 0
0 0 1 0 0 1 0 1 0 1 0 0 1 0 1 0	1	0 0 1 0 0 1 0 1 0 1 0 0 1 0 1 1

Fig.3.1. Message 'HEY' is encoded in a 16-bit CD quality sample using the LSB method

In LSB coding, the ideal data transmission rate is 1 kbps per 1 kHz. In some implementations of LSB coding, however, the two least significant bits of a sample are replaced with two message bits. This increases the amount of data that can be encoded but also increases the amount of resulting noise in the audio file as well. Thus, one should consider the signal content before deciding on the LSB operation to use. For example, a sound file that was recorded in a bustling subway station would mask low-bit encoding noise. On the other hand, the same noise would be audible in a sound file containing a piano solo [9].

To extract a secret message from an LSB encoded sound file, the receiver needs access to the sequence of sample indices used in the embedding process. Normally, the length of the secret message to be encoded is smaller than the total number of samples in a sound file. One must decide then on how to choose the subset of samples that will contain the secret message and communicate that decision to the receiver. One trivial technique is to start at the beginning of the sound file and perform LSB coding until the message has been completely embedded, leaving the remaining samples unchanged. This creates a security problem, however in that the first part of the sound file will have different statistical properties than the second part of the sound file that was not modified. One solution to this problem is to pad the secret message with random bits so that the length of the message is equal to the total number of samples. Yet now the embedding process ends up changing far more samples than the transmission of the secret required. This increases the probability that a would-be attacker will suspect secret communication [8].

Parity Coding

Instead of breaking a signal down into individual samples, the parity coding method breaks a signal down into separate regions of samples and encodes each bit from the secret message in a sample region's parity bit. If the parity bit of a selected region does not match the secret bit to be encoded, the process flips the LSB of one of the samples in the region. Thus, the sender has more of a choice in encoding the secret bit, and the signal can be changed in a more unobtrusive fashion.

Using the parity coding method, the first three bits of the message 'HEY' are encoded in the following figure. Even parity is desired. The decoding process extracts the secret message by calculating and lining up the parity bits of the regions used in the encoding process. Once again, the sender and receiver can use a shared secret key as a seed in a pseudorandom number generator to produce the same set of sample regions.

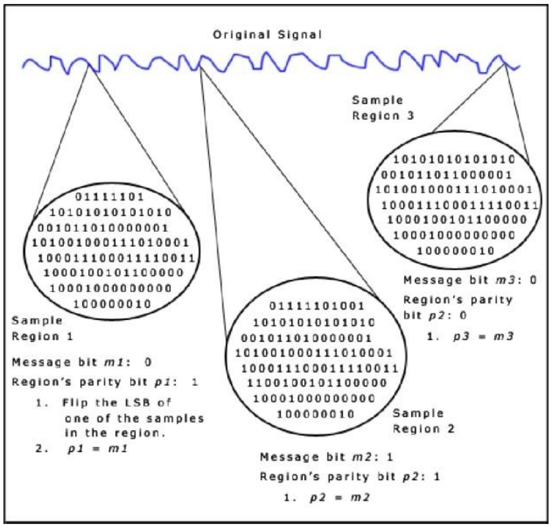


Fig.3.2. First three bits of the message 'HEY' are encoded using Parity coding method

There are two main disadvantages associated with the use of methods like LSB coding or parity coding. The human ear is very sensitive and can often detect even the slightest bit of noise introduced into a sound file, although the parity coding method does come much closer to making the introduced noise inaudible. Both methods share a second disadvantage however, in that they are not robust. If a sound file embedded with a secret message using either LSB coding or parity coding was resampled, the embedded information would be lost. Robustness can be improved somewhat by using a redundancy technique while encoding the secret message. However, redundancy techniques reduce data transmission rate significantly.

Phase Coding

Phase coding addresses the disadvantages of the noise-inducing methods of audio steganography. Phase coding relies on the fact that the phase components of sound are not as perceptible to the human ear as noise is. Rather than introducing perturbations, the technique encodes the message bits as phase shifts in the phase spectrum of a digital signal, achieving an inaudible encoding in terms of signal-to-perceived noise ratio.

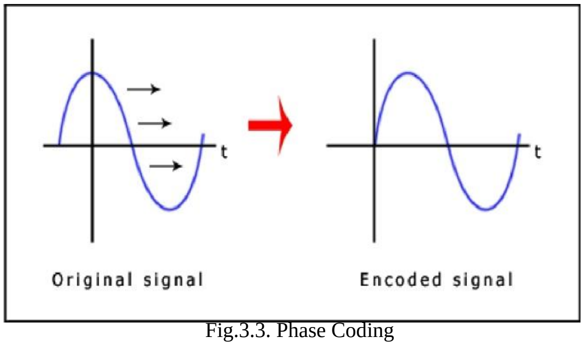


Fig.3.3. Phase Coding

To extract the secret message from the sound file, the receiver must know the segment length. The receiver can then use the DFT to get the phases and extract the information.

One disadvantage associated with phase coding is a low data transmission rate due to the fact that the secret message is encoded in the first signal segment only. This might be addressed by increasing the length of the signal segment. However, this would change phase relations between each frequency component of the segment more drastically, making the encoding easier to detect. As a result, the phase coding method is used when only a small amount of data, such as a watermark, needs to be concealed.

In a normal communication channel, it is often desirable to concentrate the information in as narrow a region of the frequency spectrum as possible in order to conserve available bandwidth and to reduce power. The basic spread spectrum technique, on the other hand, is designed to encode a stream of information by spreading the encoded data across as much of the frequency spectrum as possible. This allows the signal reception, even if there is interference on some frequencies. While there are many variations on spread spectrum communication, we concentrated on Direct Sequence Spread Spectrum encoding (DSSS). The DSSS method spreads the signal by multiplying it by a chip, a maximal length pseudorandom sequence modulated at a known rate. Since the host signals are in discrete-time format, we can use the sampling rate as the chip rate for coding. The result is that the most difficult problem in DSSS receiving, that of establishing the correct start and end of the chip quanta for phase locking purposes, is taken care of by the discrete nature of the signal.

Spread Spectrum

In the context of audio steganography, the basic spread spectrum (SS) method attempts to spread secret information across the audio signal's frequency spectrum as much as possible. This is analogous to a system using an implementation of the LSB coding that randomly spreads the message bits over the entire sound file. However, unlike LSB coding, the SS method spreads the secret message over the sound file's frequency spectrum, using a code that is independent of the actual signal. As a result, the final signal occupies a bandwidth in excess of what is actually required for transmission [6].

Two versions of SS can be used in audio steganography: the direct-sequence and frequency-hopping schemes. In direct-sequence SS, the secret message is spread out by a constant called the chip rate and then modulated with a pseudorandom signal. It is then interleaved with the cover-signal. In frequency -hopping SS, the audio file's frequency spectrum is altered so that it hops rapidly between frequencies.

Echo Hiding:

In echo hiding, information is embedded in a sound file by introducing an echo into the discrete signal. Like the spread spectrum method, it too provides advantages in that it allows for a high data transmission rate and provides superior robustness when compared to the noise inducing methods. To hide the data successfully, three parameters of the echo are varied:

Amplitude, decay rate, and offset (delay time) from the original signal. All three parameters are set below the human hearing threshold so the echo is not easily resolved. In addition, offset is varied to represent the binary message to be encoded. One offset value represents a binary one, and a second offset value represents a binary zero.

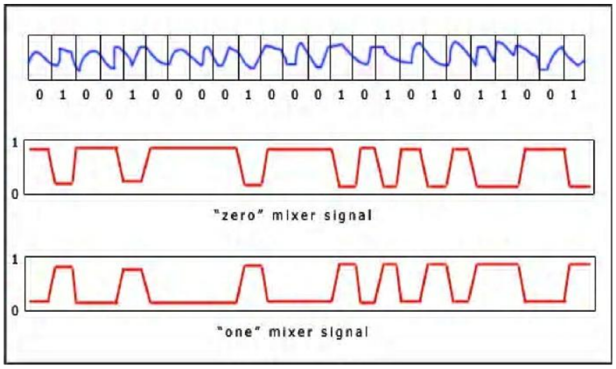


Fig.3.4. Echo Hiding

IV. Methodology

Proposed E-Cipher E & D Algorithm [5]

i. Take three key e1, e2, e3 and assign a character e1 be ‘a’ and e2 be ‘D’ and e3 be‘s’.

ii. Let ASCII value of e1 be 1 and e2 be 2 and e3 be 3 and take the text , add ASCII value of e1 to value of first character, and e2 to second character and e3 to third character, alternatively add the value of e1 , e2, e3 to consecutive characters.

iii. Three layers to be applied to each three consecutive letters and same to be continued thru the remaining text.

iv. After adding ASCII value of all values of given text, the resultant text is an encrypted message, and it generate a combination of 3* (256 * 256 * 256) letters encrypted coded text with 128 bit manner.

v. Transposition takes place in each character after all the process is over that is moves or change one bit either LSB or MSB, the end result is increasing security.

vi. Reverse process of the above algorithm gives the actual plain text without any error.

V. Methodologies

ISS- IHAS Sender Algorithm

Input: Audio file, Key and Original message Output: Mixed Data.

Algorithm

```
Step 1: Load the audio file (AF) of size 12 K.
Step 2: Input key for encryption
Step 3: Convert the audio files in the form of bytes and this
        byte values are represented in to bit patterns.
Step 4: Using the key, the original message is encrypted using
        E-Cipher algorithm.
Step 5: Split the audio file bit patterns horizontally into two
        halves.
Step 6: Split the Encrypted message bit patterns vertically into
        two halves.
Step 7: Insert the LSB bit of the vertically splitted encrypted
        text file (TF) into the LSB bit of the horizontally
        splitted audio file.
Step 8: Repeat Step 7 for the remaining bits of encrypted text
        file.
Step 9: If size (AF) ≥ size (TF) then
        embedding can be done as explained above
        else
        The next higher order bit prior to previous bit position
        can be used
        Until it is exhausted.
```

ISS- IHAS Algorithm - at the Receiver side:

Input: Mixed data, Key Output: Original message, audio file.

Algorithm

```
Step 1: Load the Stegno signal
Step 2: Extract the hidden data and audio files bit patterns
        from mixed data [9]
// Reverse process of step 7 of ISS-IHAS algorithm at sender
side.

Step 3: Input key for decryption (as used in encryption)
Step 4: Combine the two halves of audio files bit patterns.
Step 5: Combine the two halves of encrypted messages bit
pattern.
Step 6: Using Key, decrypt the original message.
```

VI. EVALUATION AND ANALYSIS REPORT

	Plain Text	Image	Audio	Video
Invisibility	Medium	High	High	High
Payload Capacity	Low	Low	High	High
Robustness against Statistical Attacks	Low	Medium	High	High
Robustness against Text Manipulation	Low	Medium	High	High
Variation in file size	Medium	Medium	High	Medium

Table 5.1 shows the different levels of satisfaction Level.

VII. CONCLUSION

In this paper we have introduced a robust method of imperceptible audio data hiding. This system is to provide a good, efficient method for hiding the data from hackers and sent to the destination in a safe manner. This proposed system will not change the size of the file even after encoding and also suitable for any type of audio file format. Thus we conclude that audio data hiding techniques can be used for a number of purposes other than covert communication or deniable data storage, information tracing and finger printing, tamper detection

This proposed system provides an efficient method for hiding the data from the eavesdropper. LSB data hiding technique is the simplest method for inserting data into audio signals. ISS- IHAS model is able to ensure secrecy with less complexity at the cost of same memory space as that of encrypted text and the user is able to enjoy the benefits of cryptography and steganography [7] combined together without any additional overhead. This work is more suitable for automatic control of robotic systems used in military and defense applications that can listen to a radio signal and then act accordingly as per the instructions received. By embedding the secret password in the audio signal the robot can be activated only if the predefined password matches with the incoming password that reaches the robot through audio signal. It can then start functioning as per the instructions received in the form of audio signal. More such sort of applications can be explored but confined to audio medium usage.

REFERENCES

[1] Bethany Delman,'Genetic Algorithms in Cryptography' published in web; july 2004.

[2] Darrell Whitley,'A Genetic Algorthm Tutorial', Computer Science Department, Colorado State University, Fort Collins, CO 80523

[3] Nalani N, G. Raghavendra Rao,' Cryptanalysis of Simplified Data Encryption Standard via Optimisation Heuristics;IJCSNS, Vol.6 No.1B, January 2006.

[4] Sean Simmons,'Algebric Cryptoanalysis of Simplified AES', October 2009;33,4;Proquest Science Journals Pg.305.

[5] Sujith Ravi, Kevin Knight,'Attacking Letter Substitution Ciphers with Integer Programming',Oct 2009,33,4; Proquest Science Journals Pg.321.

[6] Verma, Mauyank Dave and R.C Joshi,'Genetic Algorithm and Tabu Search Attack on the Mono Alphabetic Substitution Cipher in Adhoc Networks; Journal of COmputer Science 3(3): 134-137, 2007.

[7] William Stallings,"Cryptography and Network Security: Principles and Practice",2/3e Prentice hall , 2008.

[8] Ingemar J. Cox, Ton Kalker, Georg Pakura and Mathias Scheel. "Information Transmission and Steganography", Springer, Vol. 3710/2005, pp. 15-29.

[9] K.Geetha , P.V. Vanthia muthu ," International journal of Computer Science and Engineering" vol 2 No.4 Pg No: 1308-1312 , Year 2010

AUTHORS PROFILE

R. Venkateswaran received his professional degree MCA and MBA (IS) from Bharathiar University, Tamilnadu, India, He received his M.Phil from Bharathidasan University, Tamilnadu, India, and He is currently a Ph.D Scholar in the Karpagam Academy of Higher Education, Karapagam University, Tamilnadu, India, in the field of Cryptography and Network Security. Presently he is working as an Asst. Professor of Computer Applications, Nehru College of Management, Coimbatore, Tamilnadu. He is the member of CSI and other IT forums. He had published two International Journals and Presented many papers in national and International conferences, seminars and workshops. His research interests are in Cryptography and network security, information security, Software engineering,

Dr. V. Sundaram received his professional degree M.Sc. in Mathematics from the University of Madras in the year 1967 and he received his Professional Doctoral Degree Ph. D in Mathematics from the University of Madras in 1989. And He is currently working as Director, Department of Computer Applications in Karpagam College of Engineering, Tamilnadu, India, He is a research Guide for Anna university, Bharathiar university as well as Karpagam University in the field of Computer applications. He published several papers in International Journals and Conferences and also published 13 books in the area of engineering mathematics and he is the life member of ISTE and ISIAM. His research interests are in Cryptography and network security, Applied Mathematics, Discrete Mathematics, Network etc.