HONEY CIPHER STRUCTURE DATAHIDING IN SPEECH SIGNAL USING STEGANOGRAPHY AND CRYPTOGRAPHY

M. RAMBABU[1]*, Dr. RAMAN NAGAVELLI[2]
[1]Anurag Engineering College, Ananthagiri,Suryapeta,Telangana,India.
[2]Kakatiya University, Warangal, Telangana, India.
[1]rams.crypto@gmail.com, [2]ramanauce.ku@gmail.com.

ABSTRACT:

My Proposed Research study is in the area of speech signal using cryptography and stealth steganography. I have identified the Honey Cipher Structure as one of the most secured techniques in cryptography. This model providesmore security for the plain text than the conventional ones.TheASCII decimal values which are converted into characters to provide more security. The technique is that the obtained three numbered digit from Honey Cipher Structure is converted into ASCII Character symbol, thus original messages are converted into honey cipher text.This cipher text is kept hidden in speech signal usingaudio steganography. This proposal puts forward a different approach for data hiding in speech signals. A ten-digit number within speech signal using audio steganography and encrypting it with a unique key for better security. At the receiver end the same unique key is used to decrypt the received signal and then hidden numbers are extracted. The proposed approach performance can be evaluated by PSNR, MSE, SSIM and bit-error rate. The simulation results give better performance.

Key Points: Honey Structure, Honey Cipher Structure, Cryptography, Steganography,unique key, SB, data hiding.
DOI Number: 10.48047/NQ.2022.20.4.NQ22325 **NeuroQuantology2022;20(4): 1014-1021**

1. INTRODUCTION:

Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. Cryptography includes techniques such as microdots, merging words with images, and other ways to hide information in storage or transit. However, in today's computer-centric world, cryptography is most often associated with scrambling plaintext. Honey Cipher Structure is one of the secured techniques in cryptography. This is the new technique I would like consider in the cryptography also can apply steganography; the technique is converting the plain text into cipher text. Some of the techniques convert only characters, but this structure converts numeric's (0,1,2,3,4,5,6,7,8,9) along with the alphabets. The creation of the password includes mixed texts. This created password is filled in the first row of the honey form, the repeated characters are omitted and fill next character in the password, and after filling the password uncovered characters are filled in the rest of the levels [2][4],[6]. Do the same process for numerics also, after reaching the last level. Generated expression is convert this honey form into honey cipher structure. This structure is associated with Ascii Table. In this Ascii Table Ascii values are converted into Ascii Characters. These Ascii Characters are known as cipher text [7].

eISSN 1303-5150

OBJECTIVES:

- To gain new understanding of Security models and techniques, in order to face current and future security challenges in Honey Cipher Structure.
- To consolidate and strengthen the scientific excellence of cryptography and Steganography using honey cipher
- It is not possible to hacking, it is multi way translation to convert the security
- Cryptography and Steganography security system isto protect information resources at less cost than the value of the information that is being protected.
- Determining acceptable costs involve weighing the cost of the security versus the benefits of the security.

2. PROPOSED METHODOLOGY:

Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it [2]. Cryptography includes techniques such as microdots, merging words with images, and other ways to hide information in storage or transit. However, in today's computer-centric world, cryptography is most often associated with scrambling plaintext. Stegnography is one of the Hiding techniques, which can hide the text in an image.Honey Cipher Structure is one of them secured technique in cryptography [4], [6], [7].

When we create the honey structured form, this form is convert into honey cipher structure. This Cipher structure follows the three digits number this is called as honey cipher structure. This cipher structure values are consider as ASCII decimal values, this ASCII values are converted into hexadecimal representation [8], [9]. This hexadecimal form also containsone digits, which can produce the full cipher structure, this cipher structure is send to receiver. Receiver deciphers this in reverse order to get plain text, which is exactly sent by sender.

The encryption enables for data transfer where the data must only be accessed by authorized personal. It is in the scope of paper to provide an approach which delivers the speech signal in such a way that it would be known to receiver upon the information being modified, and in case of the signal being intercepted it would be encrypted there by allowing only authorized personal access to the hidden information.

There have been many methods followed to conceal a particular data in a speech signal. [1] Adopted to hide the data in the silence intervals of the speech. This is done by altering the number of samples in silence intervals. Audio watermarking was

eISSN 1303-5150

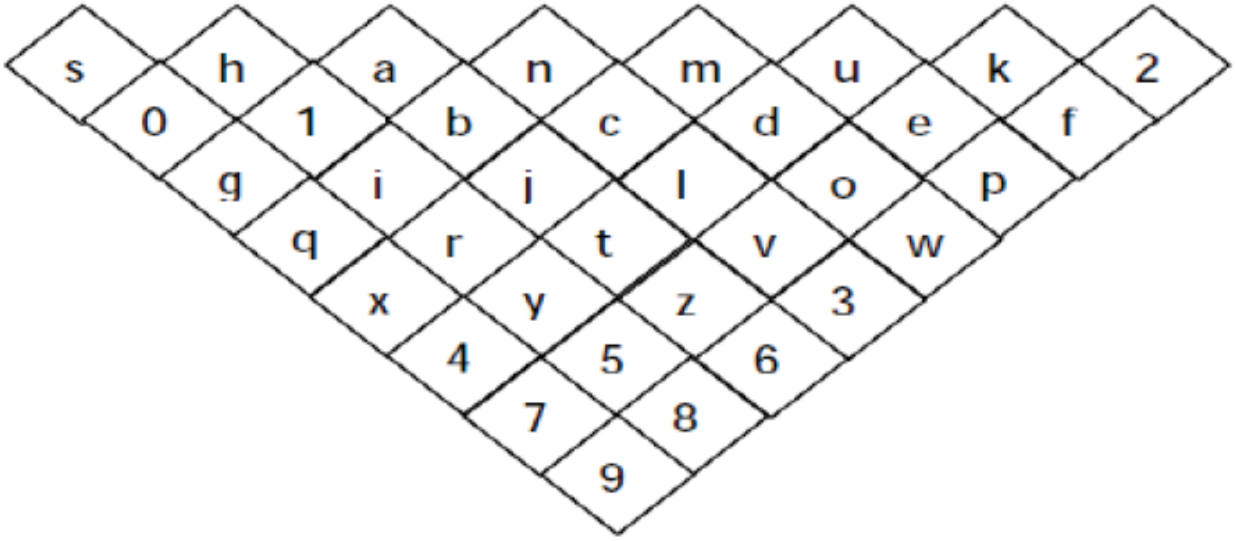
used to prevent the direct and indirect attacks on speaker recognition system from the unauthorized user [2]. [3] K. Vimal and S. A. kather discussed about extraction of data hidden in the silence region of speech signal by non-voiced detection algorithm. The methodology proposed by Subir and Dr. Amit M. Joshi [3] in their paper uses an innovative approach of Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) for the purpose of watermarking and they incorporated Arnold transformation and error correction technique [4] to increase functioning of the approach. Images are extensively used for process of hiding data in steganography, as audio steganography is perplexing because of higher precision in Human Auditory system (HAS) as compared to Human Visual System(HVS) [5].

Temporal and transform domain techniques are frequently exploited for audio steganography. Temporal domain contains LSB encoding, parity coding and echo hiding, whereas transform domain is associated with frequency and wavelet domain techniques. [6][7] Provides an inference that techniques in wavelet domain have higher hiding capacity and transparency. LSB method is employed in our algorithm. [8] Explains different audio steganography algorithms, which were developed to be the source of information hidden for different communication technologies. [9] It gives the summary of watermarking techniques on the basis of robustness and imperceptibility. [10] Explains the data hiding in the mid frequency of an image and generated the randomize key for encryption. This paper incorporates the method of steganography and encryption in speech signal. The input speech signal is divided into N number of frames. In the LSB of each frame information is hidden. The unique key which is known to authorize users is used for encryption of the stenographic signal. Then the proposed approach is compared with existing method.

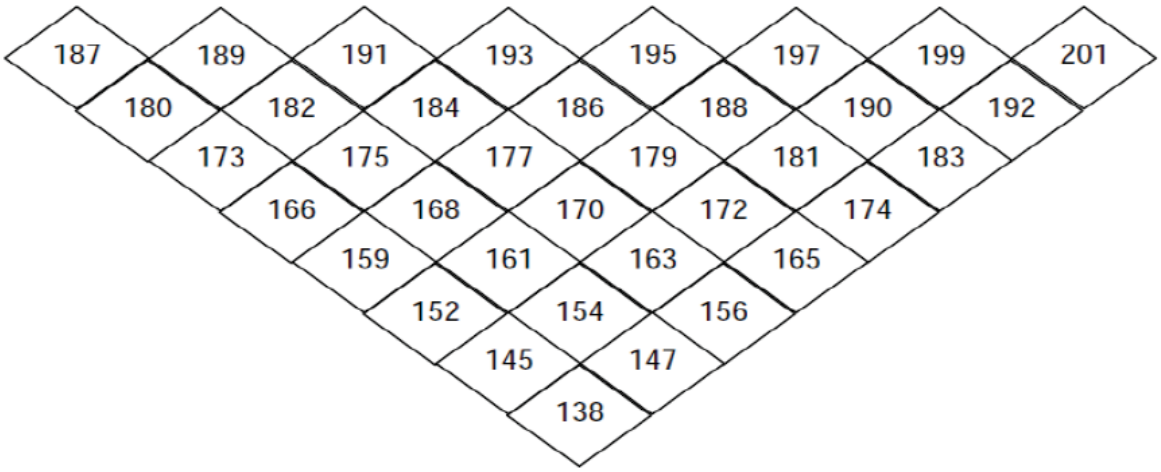
\

eISSN 1303-5150

Honey Structure:-



Honey Cipher Structure:-



In this Proposal, I have created the password,"Shanmukh2010", here h and 0 are repeated twice, the repeated characters in this password are omitted and follows the next characters [2]. Finally the filled password in this honey structure is "shanmuk201". This password is filled in the first level, and follows second level if not sufficient in the first level. After filling the password, remaining levels filled by the remaining characters. Finally fill the numeric's also to provide the security for home address. Whenever we create the structure, this structure specifies the all characters and numerics. Generate cipher text from hexadecimal representation, depending mapping from decimal values to hexadecimal values, because in this context

eISSN 1303-5150

hexadecimal contains special characters. These characters also like a scrabbled text.Honey cipher generating the plaintext and cipher text in same size via different conversations [5][9].

3. PROPOSED ARCHITECTURE:-

In this proposal honey cipher is basically provide security, but to provide more effectiveness for this, I would like to apply Cryptography technique for encryption and Steganography for hiding from sender side. Receiver move in reverse order of sender actions. Receivers extract the sender hidden data and decrypt the encrypted data and finally get original data from Honey cipher structure to honey structure. This proposal presents a novel method involving steganography and encryption thereby ensuring a relatively reliable communication without spoofing. The data is embedded in the LSB samples of frames. The unique key is applied to the stenographic signal for better secure transmission. The effect on the quality of the retrieved signal is minimal and there is zero percent of error in the bits extracted. Advancement of the current work can be done by hiding alphanumeric characters.

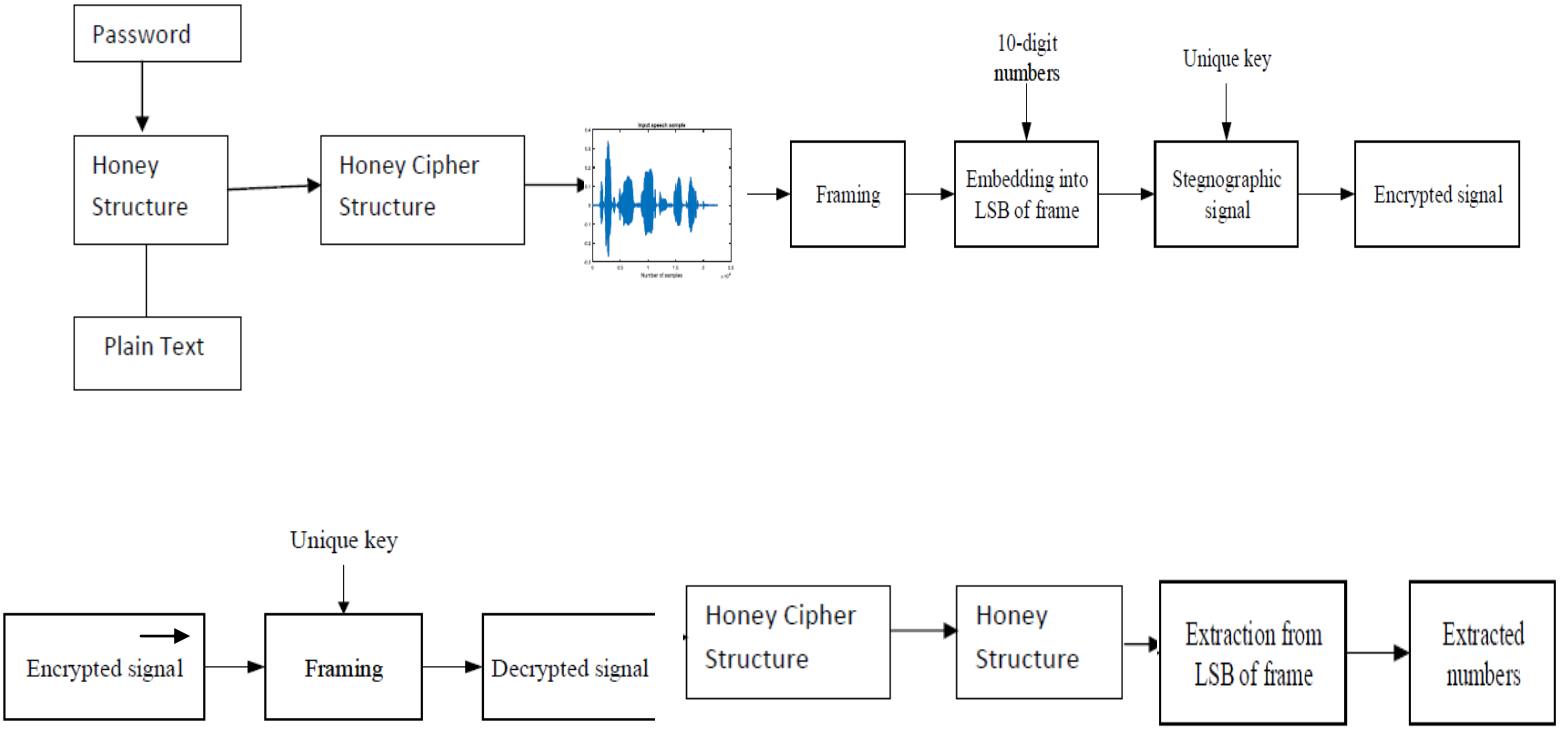


Fig-1: Proposed Block diagram for honey cipher Structured Steganography and Encryption

eISSN 1303-5150

The proposed method, the speech signal is sampled at 8 kHz with the frame length of 160 samples. In the LSB of each frame information is hidden. The unique key which is known to authorized users is used for encryption of the stenographic signal. It empowers for a more secure communication, in the case of external unauthorized tampering, there will be a variance between the sequence numbers sent and received. Signal is protected from spoofing due to the scrambling algorithm utilized. The proposed block diagram is as shown in the fig. 1. Proposed Process for hiding and encrypting there are four steps are required to implement.

4. IMPLEMENTATION:

A. Proposed procedure for encryption at sender side.

Step 1:**Honey Ciphering:** It is used toconvert the readable message into unreadable form, which is called Honey cipher form using ASCII Characters.

Step 2: **Framing:** It is a process of dividing speech signal into N number of frames with the length of 160 samples per frame. Frames of the speech signal are shown in the fig.2.

Step 3: **Embedding:** A set of N integers with length of 10 digits which are varying from 0 to 9. The generated numbers are divided by 1000 to ensure that the amplitude of the signal after later step of encryption remains in the desired range. The obtained floating-point numbers are concealed in the 10 samples of LSB of each frame. The number of LSB samples can be chosen according to the bits in need of hiding, here 10 is chosen as we are embedding a 10-digit number.

Step 4: **Encryption:** Foremost aspect of the encryption lies in generation of unique key, several logics can be applied, an insight into cryptography would guide in development of key with compound logic ensuring it's not cracked in case of interception.

B. Proposed procedure for decryption at receiver side

Step 1:**Deciphering:** receiver receives honey cipher text and it is decipher using reverting honey cipher to honey structure.

Step 2: **Framing**: Received encrypted signal divided into N number of frames of equal size similar to the process in encryption, as framing is the necessary stage in processing a signal.

Step 3: **Decryption:** the framed signal is decrypted by applying the unique key generated previously in encryption process which is known to authorize users alone. Frames of the decrypted speech signal are shown in fig.5.

Step 4: **Extraction phase**: the hidden sequence of numbers is extracted from LSB samples of each frame. The extracted numbers are compared with the initially

eISSN 1303-5150

generated numbers, the transmission is declared successful upon matching, and failure in other case. In the case of failure, there arises a suspicion of attack on the signal.

5. RESULTS AND DISCUSSION:

This Proposal describes about the conversation from ASCII values to Hexadecimal representation, these hexadecimal character symbols are consider as Scrambled text. a novel method involving steganography and encryption thereby ensuring a relatively reliable communication without spoofing. The data is embedded in the LSB samples of frames. The unique key is applied to the stenographic signal for better secure transmission. The effect on the quality of the retrieved signal is minimal and there is zero percent of error in the bits extracted. Advancement of the current work can be done by hiding alphanumeric characters.

Plain text: Honey Cipher

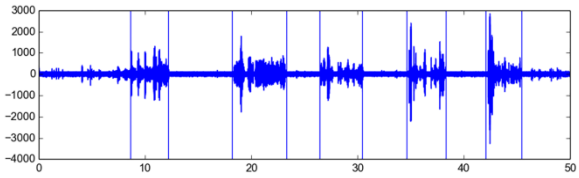
Honey Cipher Structure value: 189 188 179 190 159 186 175 183 189 190 61

Convert the Decimal value into and change the Least Significant bit, there after read the obtained decimal value.

Least Significant bit: 188 189 178 191 158 187 174 182 188 191 160

Cipher text: ╝╝▓┐ ╞╕« ╢ ╝┐ í

Senders Audio Clip:

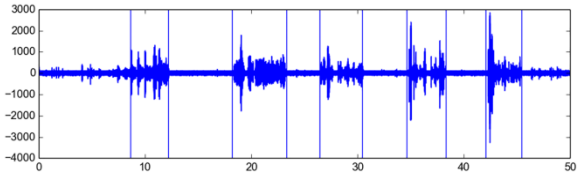


Sender Original Message: Honey Cipher

Receiver Received Message: ╝╝▓┐ ╞╕« ╢ ╝┐ í

Receiver has to decrypt the message in reverse order of the encryption procedure.

Receivers Audio Clip



eISSN 1303-5150

6. CONCLUSSION

This paper is present conversation from ASCII values to ASCII character symbols, these character symbols are knon as cipher text in this paper. Decryption is very easy to reconvert cipher text to plain text. But conversation is very intresting it may provide security, and there is a possibilty to capture and guess the cipher text to plain text by multiple pacticess. I thik other than ASCII, if this honey cipher strucutre is associated with any another algorithms in security, an opponent can not be guess the plain tect. If we create any secure table in database with more complicate and tuff guessing. So we can protect plaintexy from opponent and can transfer messages with confidential.

7. REFERENCES:

[1]. "Honey Cipher Structure" from International Journal Innovations in Engineering and Technology[IJIET], Special Issues NCRTEEFOSS-2016, ISSN:-2109-1059.

[2]. "Cryptography Symmetric Key Encryption Algorithms", from IJDCST @Jan-2016, Issue-V-4, I-1, SW-23 and ISSN-2320-7884 (Online),ISSN-2321-0257 (Print).

[3]. M. Rambabu, N Ramana, Dr.M. Sadanadam, "Enhanced Honey Cipher Structure with Multiple Cipher Structures", www.ijcrt.org, © 2017 IJCRT, Dec 2017| ISSN: 2320-2882.

[4]. Network Security Essentials by "William Stalling", Third Edition.

[5]. Security using Pyramidal Cipher Form from IJFTE Journals.

[6]. W.Ehrsam, etal., " A Cryptography Key Management Scheme for Implementing the Data Encryption Standard", IBM System Journal,VOL.7,PP.-125,2010.

[7]. J.Katz and Y.Lindell, Introduction to Modern Cryptography;,Chapman & all/CRC.2008.

[8]. T.Fukunga and J. Takahashi, "Practical fault attack on a Cryptographic LSI with ISO/IEC 18033-3 Block Ciphers", 2010.PP.84-92.

[9]. A.Barenghi,etal., " Low Voltage fault attacks to AES and RSA on general purpose processors", IACR Eprint archive, Vol.130,2010.

[10]. ASCII or EBCDIC, Translation Tables from Google Wikipedia.

[11].http://www.malighting.com, for conversation from ASCII Decimal Values to Character Symbols.

[12]. Data Hiding in Speech Signal Using Steganography and Encryption by Hanisha Chowdary N School of electronics and Engineering Vellore Institute of Technology Vellore, India.