IJCER International Journal of Computer & Electronics Research

# Data Based Text Encrypting in Audio

**Bommala Suneel Kumar[1], S.Satyanarayana[2]**
[1]M.Tech Student, Dept of CSE, Raghu Engineering College, Visakhapathnam, A.P, India
[1]Associate Professor & HOD, Dept of CSE, Raghu Engineering College, Visakhapathnam, A.P, India

***Abstract*–Nowadays data authentication plays a major for the secrete transmission of the data respectively. Here in this data oriented authentication involves encryption followed by the respective decryption. Where in the encryption process takes place in the transmitter end while decryption takes place or handled at the receiver end respectively. Here an algorithm is designed based on the above strategy where complete privacy is maintained by the system. This one of the data hiding technique. Some of the data hiding techniques include cryptography, Stenography and watermarking. Therefore there is a slight variation between all these techniques in their implementation. Here the protection is also follows where we can hide text in text, Speech in the song which is related to the audio based scenario, Text in the song, Image in the image and text in the image respectively. Here the main aim of the projects is to hide the data in the form of text I the signal respectively. Here in this present methodology we are going to implement the method by the name of RSA respectively. Where the experimental analysis show that this particular method is used for the accurate hiding of the data takes place that is in the form of security based scenario.**

***Keywords:* Hiding Information, Data Hiding, Bits of High Priority, Bits of Low Priority, Audio Authentication, Data Transfer, Encryption.**

## 1. INTRODUCTION

Every day the technology is rapidly growing in the society. Therefore security plays a primary concern in each and every aspect of the system respectively[2]. There are many existing techniques which is based on the hiding principle and for this implementation there are a number of algorithms supported to it. Even though there are a large number of methodologies the hackers are easily hacking the data very easily. Therefore in the present situation hiding of the data plays a major role and mainly hiding is nothing but invisible respectively. Among all these data hiding techniques there is a simple rule that is encryption followed by the decryption respectively[1].

Therefore the normal and old data hiding technique is based on stegnography. Where the complete hiding of the data takes place respectively. Where it is implemented in the images followed by the stream of the frames of sequences in the form of video consequences respectively.Then after cryptography came into the implementation. Here in this particular based approach data manipulation takes place that the original data is converted into the manipulated form where the complete security is maintained. Now the latest technique is implemented by overcoming the drawbacks of cryptography followed by stegnography is watermarking[3]. It is one of the advanced technique where the protection is given to the data in such a fashion that parent data is visible apart from the child is hidden inside there is no doubt regarding the encryption oriented strategy. Here encryption takes place at the place of the transmitter and applied at the time of transmission. And the decryption is applied at the receiver where the decoding or the extraction of the original data takes place.

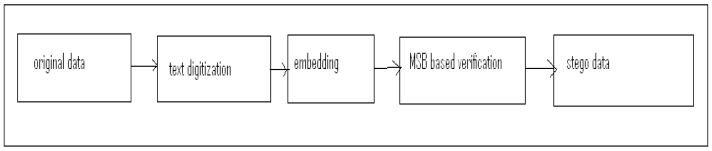

Fig 1: The data embedding process

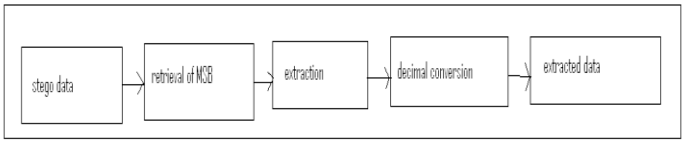

Fig 2: The data extraction process

## 2. METHODOLOGY

Here in this present scenario we are going to use a well defined technique and it is designed in such a fashion that the complete security has to be provided to the system. Here the data hiding is based on the combination of cryptography in order with that of the stegnography respectively[4][5].

Here the main intention of the system is to provide security for the message based on the text based scenario respectively. Therefore the text can be hidden in the text itself, The text can also be hidden in the image also and the new strategy with well known defined parameters in such a fashion where the message in the form of text is hidden in the data bits of the audio signal respectively[6].

Whenever and whatever the system we are going to implement it compose of three parts such a encryption at the time of transmitter followed by the transmission to the desired destination and there at the destination the decryption of the data takes place in order to extract the particular hidden data respectively[7]. Here we are going to use the method in a combined fashion as cryptography followed by the stegnography respectively. Here initially the audio signal is taken into the database. Then the text to be hidden is taken into the sytem and converted to binary in the form of zeros and ones respectively. Then both are mingled together in a combine fashion here the least significant bits are taken into the consideration respectively[8].

Depending on the conditionality basis the data is hidden. In the above fashion encryption phenomena takes place at the transmitted side. At the receiver side complete reverse process takes place where the decryption oriented scenario is implemented. Here we finally conclude that stegnography is used for the data hiding purpose and the cryptography is used for the privacy based scenario. Where implemented for the security purpose. Here in our project the main aim of the system is to protect the message in the form of text by the help of the audio signal from the hackes or the unknown persons respectively.

## 3. RESULTS

A lot of analysis takes place and a huge comparison takes place between the several existing techniques followed by the proposed technique. And a lot of research takes place on the present system based on the different data sets of the message signal that is in the form of the text respectively. And also the audio in the form of the speech respectively. Upon comparison the present system is effective on comparison to the several other techniques because several existing techniques got used only one technique that is either the stegnography or a cryptography or even a water making. Here we are going to use it in a combine fashion where the security is somewhat plays a crucial role in protecting the data.

Here stegnography is used for hiding purpose and cryptography is used for the protection that is manipulation of the data from the third party members that is hackers respectively. If at all in the worst cases one can be detected but both of them detection is completely impossible.

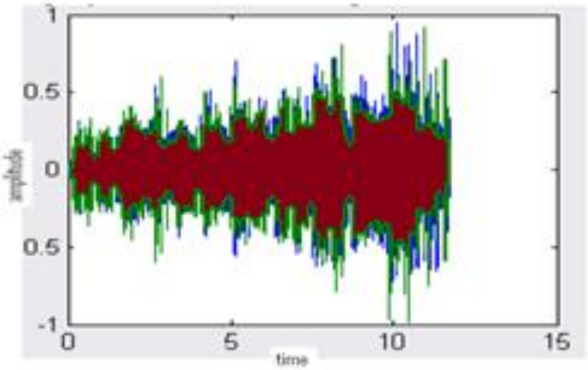

Fig 3: The representation of the signal based on audio with respect to both amplitude followed by time respectively

## 4. CONCLUSION

Here a latest technique is implemented and it is designed a particular framework in such a fashion where it is completely different from the several previous existing techniques respectively. Here in this present strategy there is a combination of both the techniques one will be working on the process on the least significant based bits oriented scenario and the other one is working in the most significant bit scenario. Here the main intention of the system is very clear that whatever the system is designed it must be highly secure and it must be in such a position that it must overcome the drawbacks of the several previous existing techniques respectively where the complete hidden data must be protected.

## REFERENCES

[1] M. M. Amin, M. Salleh, S. Ibrahim, M. R. Katmin and M. Z. I. Shamsuddin, "Information Hiding using Steganography", 4th National Conference on elecommuni cation Technology Proceedings, Shah Alam, Malaysi.

[2] Stefan Katzenbeisser, Fabien A. P. Petitcolas, "Information HidingTechniques for Steganography and Digital Watermarking". Boston,Artech House, pp. 43 – 82. 2000.

[3] Methods of Audio Steganography, Internet publication on www.Snotmonkey.com

[4] Mazdak Zamani, Azizah A. Manaf, Rabiah B. Ahmad, Akram M. Zeki, and Shahidan Abdullah,“A Genetic Algorithm Based Approach for Audio Steganography ”, World Academy of Science, E ngineering and Technology 54 2009.

[5] I. Cox, M. Miller, J. Bloo m, J. Fridrich, and T. Kalker. Digital Watermarking and Steganography. Morgan Kaufmann, 2 edition, 11 2007.

[6] I. Cox, J. Kilian, T. Leighton, and T. Shamoon. protected spread spectrum watermarking for images, audio and video. Image Processing, 1996. Proceedings., International seminar on, 3, 1996.

[7] F. Rosenblatt. The perceptron a probabilistic form for information storage and organization. Brain Psych. Revue,62:386.408, 1958.

[8] D. Rumelhart and J. McClelland. Parallel circulated processing: investigation in the microstructure of cognition, vol.1: foundations.MIT Press Cambridge, MA, USA, 1986.