Audio Steganography using RSA Algorithm

Harshal Chhadwa, Glynes D'souza, Swaradi Godane, Pooja Sharma

Abstract: A significant amount of research is done to improve the effectiveness in data hiding. Audio steganography is an art of hiding secret information inside an audio file, such that the representation of audio file won't be altered. Steganography is one of the safest ways of secret data transmissions in today's digital world. In this paper, large embedding capacity steganography method is proposed using LSB substitution. Alongside, the power and security of the RSA cryptosystem is based on the fact that the factoring problem is "hard." The public and private keys are related mathematically, but the parameters are chosen so that calculating the private key from the public key is either impossible or prohibitively expensive. Thus two level security and robustness is achieved. The original and stega-audio signals show resemblance hence there is minimum chance of detecting the secret message hidden in the stega-audio. MATLAB is used for proposed algorithm and proposed results have been shown.

Keywords: Cryptography; Steganography; LSB; RSA; Stega-Audio

I. INTRODUCTION

Information security plays a vital role during internet communication in today's era of technology and it is one of the most challenging issues now a days. This information is not secure and it can be easily intercepted and misused by an eavesdropper. This threat of accessing secret information by unintended receiver is an existing concern for data communication experts. This information transfer must be hidden and secured. Reversible data hiding is one of the technique of data hiding, which is lossless i.e. we will be able retrieve the entire original cover information with very less distortion from the marked data after extraction of entire hidden data [1]. To secure this information, and overcome the threat of intruder, Steganography and Cryptography are widely used. Audio steganography is a technique which uses audio as a cover-object to hide the original message.

Steganography is the art and science of passing hidden messages in such a way that only sender and the intended receiver can detect the existence of the hidden message. Historical examples of Steganography consist of Text hidden on wax-covered tablets, Null ciphers, and tattoo of a message on the head of a messenger. Cryptography defines as the art and science of transforming data into a sequence of bits that appears as random and meaningless to a side observer or attacker. It comes from Greek words crypto (secret) and graphy (writing or drawing). Steganography also comes from the Greek words steganos (covered) and graphy (writing or drawing) and can be defined as the hiding of information by embedding messages within other, seemingly harmless messages, graphics or sounds [2]. When used standalone steganography and cryptography techniques are vulnerable to attacks. Attacks on steganography and cryptography lead to detection and destruction of the secret data. Steganography attacks focuses on detecting the changes in the cover that has been used to send the secret message while, cryptography attacks focuses on breaking down the secret message. Security breaches can be overcome when the advantages of both these techniques are combined together. Steganography algorithms applied on cryptography techniques results into a robust system. The objective of using two techniques in combination in the proposed system is such that benefits of the two techniques can be combined and a more secure and robust system can be built [3].

For literature survey different papers and related work have been studied [4-11]. The use of Cryptography along with Steganography is mostly neglected by most of the researchers so we have decided to develop a technique that integrated both Cryptography with Steganography.

II. PROBLEM STATEMENT

The use of internet has increased tremendously and a lot of information is shared on it. If this information is not secured, it can be easily intercepted and misused by the attacker. So to secure this information many robust algorithms are used. One way this can be done, is by using Cryptography and Steganography. The principle of Cryptography is to manipulate the information so that unintended receiver will not be able to understand the message, however the principle of Steganography is to mask the very presence of communication; i.e. it hides the existence of the message. Both of these techniques are widely used to prevent non-deliberated receiver's attacks from unauthorized access. The main purpose of this paper is to provide multilayer robust security by integrating Cryptography along with Steganography.

III. PROPOSED SYSTEM

This section gives a brief about the proposed system. It shows the working of our system. It is broadly divided into three sub-sections – Firstly the message is encrypted using cryptographic algorithm, here we have used RSA algorithm for the same. Then this encrypted message is concealed into an audio file using steganography algorithms, here LSB substitution algorithm is used. Lastly steganalysis is performed i.e. hidden message is extracted from the stega-audio and then decrypted into original message. Fig. 1 depicts the flowchart for our proposed system.

Revised Version Manuscript Received on April 27, 2018.

Harshal Chhadwa, Department of Computer Engineering, Xavier Institute of Engineering, Mumbai (Maharashtra), India. E-mail: harshalc1996@gmail.com

Glynes D'souza, Department of Computer Engineering, Xavier Institute of Engineering, Mumbai (Maharashtra), India. E-mail: glynes.dsouza@gmail.com

Swaradi Godane, Department of Computer Engineering, Xavier Institute of Engineering, Mumbai (Maharashtra), India. E-mail: swaradigodane@gmail.com

Pooja Sharma, Department of Computer Engineering, Xavier Institute of Engineering, Mumbai (Maharashtra), India. E-mail: sharmapooja1203@gmail.com

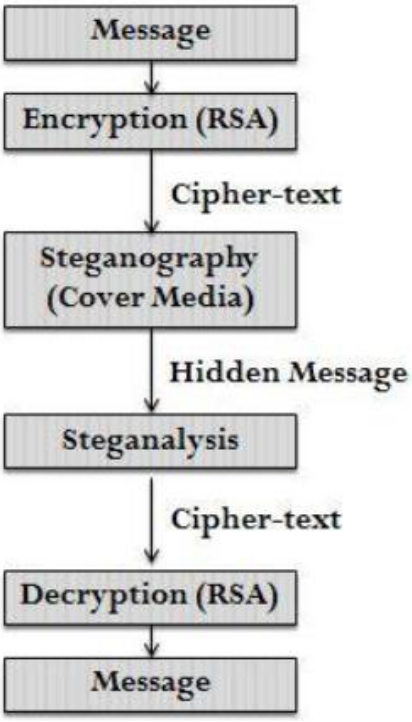

Fig. 1 Flowchart of Proposed System

A. Terminologies

1) Encryption: Process of converting plain text (message) into unreadable form i.e. cipher-text.

2) Cover-Media: It is the carrier medium to hide the message.

3) Steganalysis: Process of extracting hidden message from the cover-media.

4) Decryption: Process of converting cipher text to plain text (message).

B. Working

Step1: Message (Secret-data) is given as input to the proposed system.

Step2: This message is Encrypted using RSA algorithm and cipher-text is formed.

Step3: Cipher-text is embedded into cover media using LSB Substitution technique forming a stega-audio.

Step4: Steganalysis is performed on stega-audio to get the encrypted message.

Step5: The message is than Decrypted to get back the original message.

IV. ALGORITHMIC VIEW

Different methods are already used to hide message into audio file, i.e., in Audio Steganography. Initially, simple LSB, then modified LSB method were used [11]. Some of the authors tried to increase the LSB layer to increase the robustness against attack. It always increases the distortion in host audio. In this paper we initially encrypt the message using RSA algorithm and then encrypted message bits are inserted at random higher LSB layer position of the host audio. This helps in increasing the robustness. There are four main steps in this algorithm:-

A. Alteration

The first step is alteration. In this step, the message bits are replaced with the target bits of samples. Target bits are those bits which are placed at the layer that we want to alter. This is done by a simple substitution that does not need adjustability of result be measured [12].

B. Modification

This step is the most important and essential part of algorithm. All results and achievements that we expect are depending on this step. In this stage the algorithm used will try to decrease the amount of error and improve the transparency. Transparency evaluates the audible distortion due to signal modifications like message embedding or attacking. One of them is a simple and ordinary technique, but in aspect of perspicacity will be more efficient to modify the bits of samples better. Since transparency is simply the difference between original sample and modified sample, hence by using a more intelligent algorithm, more bits and samples are modified and adjusted as compared to the previous algorithms. If the used algorithm is able to decrease the difference of them, transparency will be improved.

C. Verification

In fact this stage is quality controller. What the algorithm could do has been done, and now the outcome must be verified. Here the difference between original sample and new sample is now checked.

D. Reconstruction

The last step is the creation of new audio file (stego file). This stego file will be created using the naming convention as filename_stego.wav and will be saved at the same location as that of the original audio.

V. RESULTS AND CONCLUSIONS

The following figure i.e. fig 2 is the GUI of the proposed system. From the fig 4 and fig 5 it can be seen that the waveforms of the audio do not change i.e. the waveform of the audio before embedding the data and after embedding the data are similar and the difference between the two signals is very less which is almost unnoticeable.

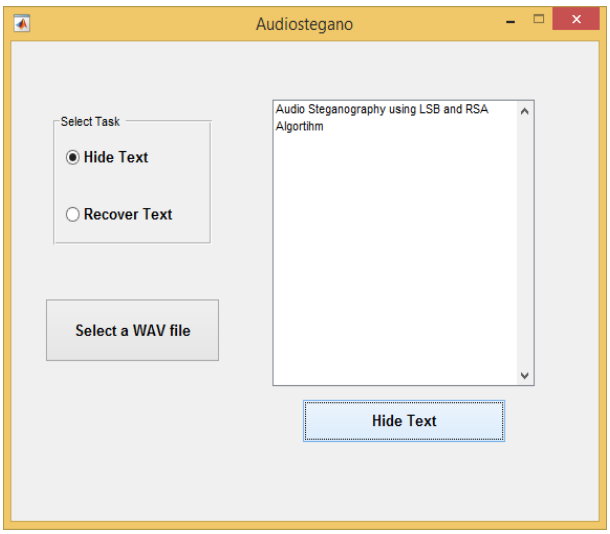

Fig. 2 GUI for the Proposed System

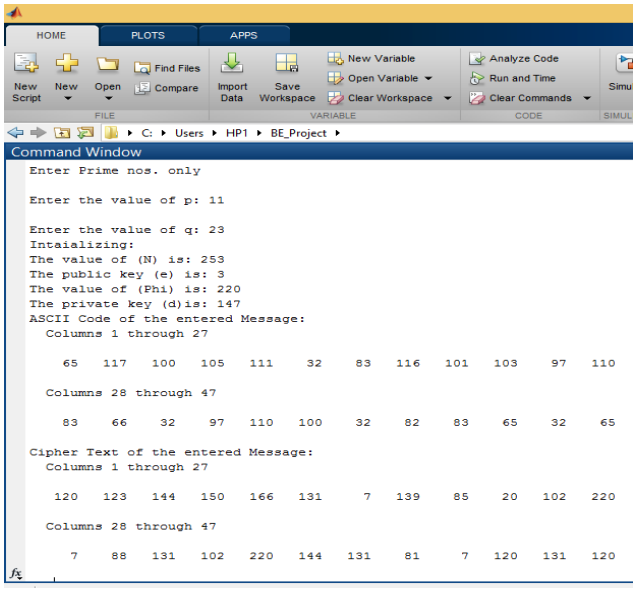

Fig. 3: Implementation of RSA Algorithm

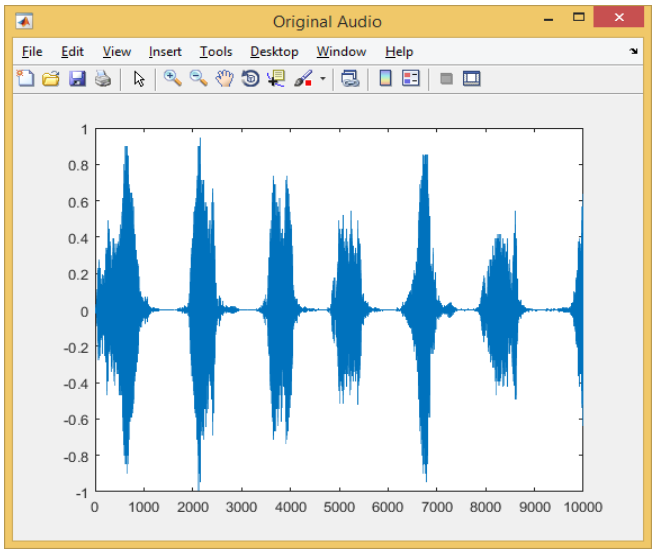

Fig. 4 Representation of Audio without Data

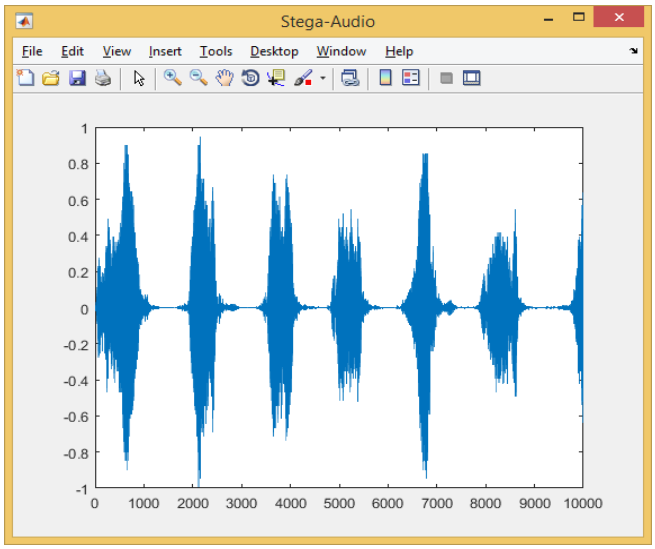

Fig. 5 Representation of Audio with Data

REFERENCES

1. Anitha Devi M.D, Dr K B ShivaKumar, "Novel Audio Steganography Technique for ECG Signals in Point of Care Systems(NASTPOCS)", 2016 IEEE International Conference on Cloud Computing in Emerging Markets.
2. Ankit Gambhir, Sibaram Khara, "Integrating RSA Cryptography & Audio Steganography", International Conference on Computing, Communication and Automation (ICCCA2016).
3. Nikita Lemos, Kavita Sonawane, Bidisha Roy, "Secure Data Transmission using Video", IEEE@2015.
4. Anitha Devi M.D, Dr K B ShivaKumar , "Novel Audio Steganography Technique for ECG Signals in Point of Care Systems(NASTPOCS)", 2016 IEEE International Conference on Cloud Computing in Emerging Markets.
5. A. Arora, M. P. Singh, P. Thakral, N Jarwal, " Image Steganography using Enhanced LSB Substitution technique", 2016 Fourth International Conference on Parallel, Distributed and Grid Computing (PDGC).
6. Japtej Singh Lamba, Karan Sachdeva, Vishal Sinha, Neetu Singh, "Differential Pulse Code Modulation in Audio Steganography", 2016 International Conference on Electrical, Electronics, Communication, Computer and Optimization Techniques (ICEECCOT).
7. Kamred Udham Singh, "LSB Audio Steganography approach", International Journal of Emerging Technology and Advanced Engineering ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 4, Issue 4, April 2014.
8. RSA Encryption – Keeping the internet secure [AMS Grad Blog] Available: https://blogs.ams.org/mathgradblog/2014/03/30/rsa/
9. Mohsen Bazyar, RubitaSudirman, "A New Method to Increase the Capacity of Audio Steganography Based on the LSB Algorithm," University Teknologi Malaysia, 81310 UTM Johor Bahru, Malaysia.
10. Jayaram P, Ranganatha H R, Anupama H S, "INFORMATION HIDING USING AUDIO STEGANOGRAPHY – A SURVEY," The International Journal of Multimedia & Its Applications (IJMA) Vol.3, No.3, August 2011.
11. Krishna Bhowal, Anindya Jyoti Pal, Geetam S. Tomar, P. P. Sarkar, "Audio Steganography using GA", IEEE Proceedings,2010.
12. Mazdak Zamani, Hamed Taherdoost, Azizah A. Manaf, Rabiah B. Ahmad, and Akram M. Zeki, "Robust Audio Steganography via Genetic Algorithm", IEEE, 2009.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.