Genetic Algorithm Based Audio Steganography

Akshay Tharmia#1, Niketan Kudtarkar#2, Nishant Mishra#3, SarthakBhingarde #4,Prof.Rohini Patil#5
#Computer Department, Terna Engineering College Navi Mumbai, India

Abstract: *Data encryption is suitable method to protect data, whereas steganography is the process of hiding secret information inside some carrier. In the proposed method encrypting message with ECC key using AES and GA based LSB Algorithm to encode the encrypted message into audio data. It gives a high level of authentication, security and resistance against extraction by attacker.*

Keywords: *Genetic algorithm, ECC, Message encryption*

I. INTRODUCTION

Steganography,meaning concealing of sensitive information with the help of non-covert data is one of the best method for hiding data. In audio steganography, we use digital audio files to bury data in them. This audio is then transmitted. Implementation of this technique is done by slight alteration of the binary sequence of the audio file and the algorithm used for this purpose is called “Genetic Algorithm”. The name is so because it depicts the process of genetic evolution in humans

Steganography is the art and science of hiding information such that its presence cannot be detected[1]. The secret information is hidden in some carrier file and then transmitted. The carrier file can be an image, Audio file, text file, video file, etc.

On the basis of cover file used for embedding, the steganography techniques are divided into different categories. The focus will be on using audio as cover file in this paper.

II. METHODOLOGY

In order to secure and avoid detection of message and communication, active attack can be further controlled by methods of steganography In previous system they tried to hide message in audio file in LSB, initially simple LSB& then modified LSB used but the LSB layers were increased which decreased robustness. In proposed system we use Genetic algorithm to embed data in audio which increases the robustness of data and sound to noise ratio of genetic algorithm is same as LSB.For encryption we are using Elliptic curve cryptography (ECC) which uses same concept of trap door as RSA algorithm but generates smaller keys as compared to RSA.Following paragraph describes the comparison of previous system and proposed system.

RSA vs ECC

The security level which is givenby RSA, can be provided even by smaller keys of ECC.

For example, the 1024bit security strength of a RSA couldbe offered by 163 bit security strength of ECC [3]

Symmetric-key	**E C C**	**R S A / D L P**
6 4 b i t	1 2 8 b i t	7 0 0 b i t
8 0 b i t	1 6 0 b i t	1 0 2 4 b i t
1 2 8 b i t	2 5 6 b i t	2048-3072 bit

III. ECC(Elliptic key Cryptography)

Our goal is to calculate k*P=Q, where P and Q are points (set B) on an elliptic curve: y2= x3 +ax +b. Operation '*' denotes the series of Point doubling and Point adding.

A. Point adding

For given two points P(xp,yp),Q(xq,yq) (P≠±Q) in the set B, the group operator will allow us to calculate a third point R(xr,yr), also in the set B, such that P + Q = R. Not difficult to find the coordinates of point R:xr= s2 –xp - xqwhere s2 =2xp + xq +xr – xp As

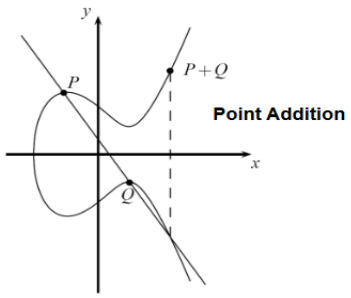

Fig 1: Point Addition

2.Point doubling

For given point P(xp,yp) in the set B, the group operator will allow us to calculate a third point R(xr,yr), also in the set B, such that P + P = 2P= R. xr = s2 -2xp where s= (3xp 2−a)/2yp and yr=yp+s(xr–xp)

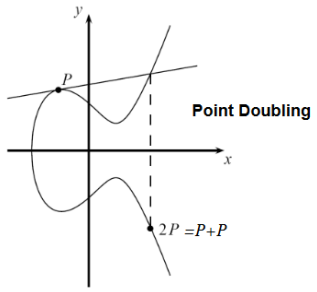

Fig 2: Point Doubling

point R belongs to the straight line (PQ) then s= (yr−yp)/(xr−xp) and we find: yr = yp +s(xr –xp)

3. Point multiplication

One of the most vital operations for all applications of elliptic curves is scalar multiplication. In this project we will use approach for computing k*P was introduced by Montgomery

Algorithm: Binary method

INPUT:

An integer k>0 and a point P.
OUTPUT:
Q=k*P
1. Set k←(kl-1…k1k0)2
2. Set P1←P, P2=2P.
3. for I from l-2 downto 0 do
If ki=1
then Set P1←P1 +P2, P2←2P.
Else Set P2←P2+P1, P1←2P1.
4. RETURN (Q=P1)
Q is the KEY

IV. MESSAGE ENCRYPTION

Advanced Encryption Standard (AES):

AES is an iterative rather than Feistel cipher. It is based on 'substitution–permutation network'. It comprises, operations involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations).AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix −

A. Encryption Process

Following AES steps of encryption for a 128-bit block:

1. Derive the set of round keys from the cipher key.
2. Initialize the state array with the block data (plaintext).
3. Add the initial round key to the starting state array.
4. Perform nine rounds of state manipulation.
5. Perform the tenth and final round of state manipulation.
6. Copy the final state array out as the encrypted data

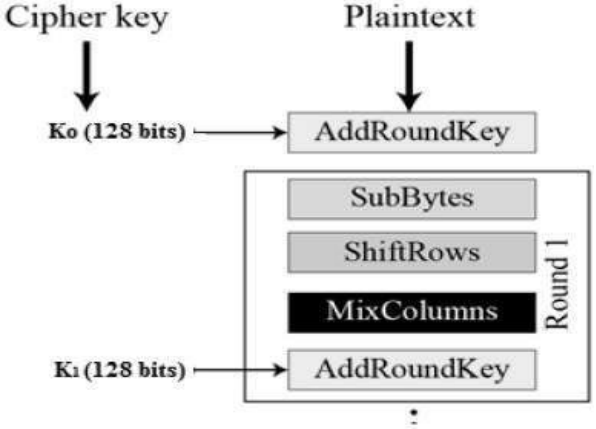

Fig 3: Advanced Encryption Standard

B. Decryption Process

The process of decryption of an AES ciphertext is similar to the encryption process in the reverse order. Each round consists of the four processes conducted in the reverse order −

Add round key
Mix columns
Shift rows
Byte substitution

Since sub-processes in each round are in reverse manner, unlike for a Feistel Cipher, the encryption and decryption algorithms needs to be separately implemented, although they are very closely related.

V. GENETIC ALGORITHM

The genetic algorithm is a search heuristic that imitates the process of natural transformation. The chromosome in the GA is generally held in binary encoding. Each chromosome represents a candidate solution in the searching space. The GA often needs a fitness function to assign a count to each chromosome in prevailing population. The GA starts with initializing a population of individuals by guess. The individuals grow through iterations, called generations. In each generation, each individual is checked with the fitness function. Genetic operators

are used for individuals in the population to produce a next generation of individuals. The process is continued until some form of criterion is met

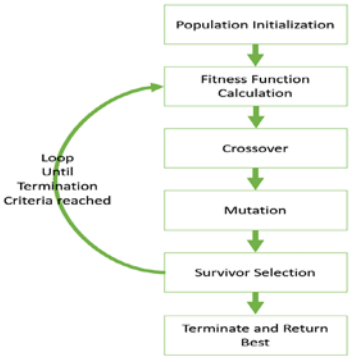

Fig 4: Genetic Algorithm phases

Algorithm:

GA()
initialize population
calculate fitness of population
while (termination criteria is reached) do
parent selection
crossover with probability pc
mutation with probability pm
decode and fitness calculation
survivor selection
find best
return best

Example:
Sample bits are: 00101111 = 47
Target layer is 5, and message bit is 1
Without adjusting: 00111111 = 63 (discrepency is 16)
After adjusting: 00110000 = 48 (discrepency will be 1 for 1bit embedding) Sample bits are: 00100111 = 39

VI. RESULT AND DISCUSSION

Sender encryptsthe message using the key provided by the receiver using ECC algorithm then embed the encrypted message in byte stream of audio using genetic function and converts embedded bytes to stego audio.

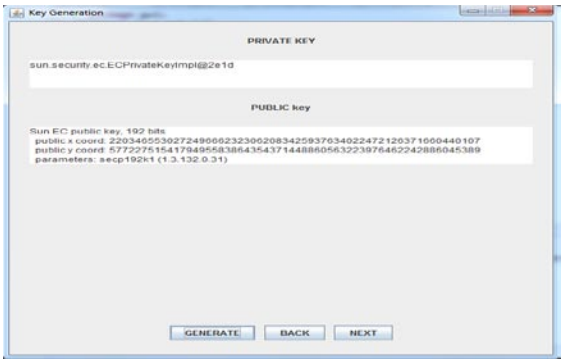

Fig 5:Key Generation Using ECC

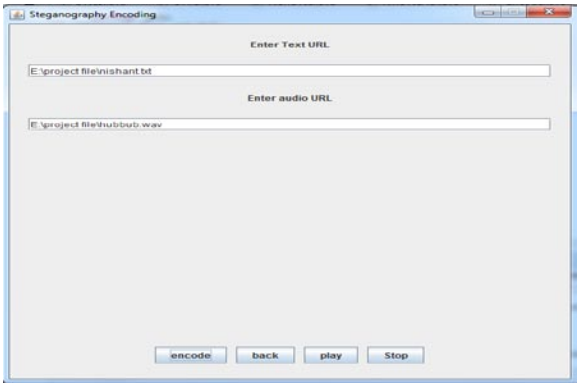

Fig 6:Audio and Text Selection

Receiver converts the received stego audio into byte stream then recovers the embedded encrypted message by applying reverse steganography operation and decrypting encrypted message using private key

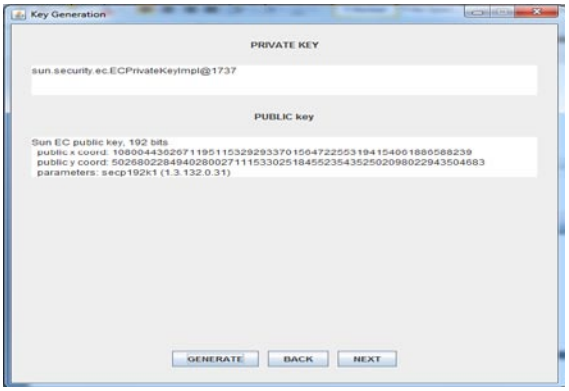

Fig7: Key Generation Using ECC at Receiver Side

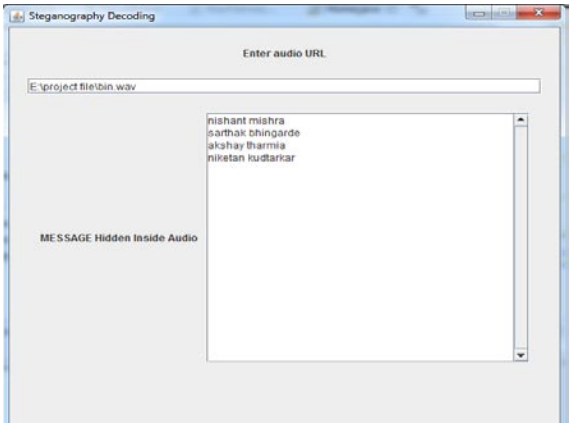

Fig 8: Decoded Message from Stego Audio

VII. CONCLUSION

In earlier systems image steganography was used to hide the data but that proved to be quite inefficient as it can store less amount of data in it. For this purpose audio steganography was developed to hide and send data inside an audio file. This was implemented using LSB technique which also proved to be inefficient as it was easy to detect presence of data inside the audio and extract data from it. To overcome these problems genetic algorithm is used to hide data in the audio file. Genetic algorithm increases robustness and has similar sound to noise ratio as that of LSB. This technique helps to tackle the security issues related to transfer of vital data. Further development of this technique will enable us to use other audio data formats for transfer of vital data

VIII. REFERENCE

[1] Rohit Tanwar, Sunil Kumar, Narender Gautam, Ravinder Gautam," A Spatial Domain Steganography Technique Based on Optimal Solution Using Genetic

[2] IEEE :-Robust audio steganography along with genetic algorithm by: Mazdak Zamani, Hamed Taherdoost, Azizah A. Manaf, Rabiah B. Ahmad , Akram M. Zeki

[3]National Security Agency. "*The Case for Elliptic Curve Cryptography,"www.nsa.gov/business/programs/elliptic_curve.shtml. 2009*

[4] 2011 7th International Workshop on Systems, Signal Processing and their Application(WOSSPA)By moncef Amara and Amar Siad

[5] mazadak Zamani et.al,"A Secure Audio Steganography approach"

[6] Mazdak Zamani et.al , "A Secure Audio Steganography Approach", International Conference for Internet Technology and Secured Transactions 2009.

[7] Bankar Priyanka ., Katariya Vrushabh R, Patil Komal K, "Audio Steganography using LSB'', International Journal of Electronics, Communication and Soft Computing Science and Engineering, March 2012, pp 90-92

[8] Ajay.B.Gadicha, "Audio wave Steganography", International Journal of Soft Computing and Engineering (IJSCE), Vol. 1, pp. 174-177, Nov. 2011

[9]Nedeljko, C. and S. Tapio, 2002. Increasing robustness of LSB audio steganography by reduced distortion LSB coding. Proceeding of the 5th IEEE International Workshop on Multimedia Signal Processing. St. Thomas, pp: 336-338.

[10] Samir, K.B., B. Debnath, G. Debashis, M. Swarnendu and D. Poulami, 2008. A tutorial review on steganography. Proceeding of the International Conference on Contemporary Computing (IC3-2008). Noida, India, August 7-9, pp: 105-114.