MAT JOURNALS

Journal of Digital Integrated Circuits in Electrical Devices
Volume 2 Issue 1

A study of different steganographic methods

Department of Electrical and Electronics Engineering, Dr. Vijay Shrivastav
Institute of Engineering And Technology,DeviAhilya,Indore,India
Email- Vishrivastavv@Gmail.Com*

Abstract

Audio Steganography is a technique used to transmit hidden records by means of editing an audio signal in an imperceptible manner. it is a way that ensures secured records transfer among parties generally in internet network [2]. here we gift a novel technique for resolving the troubles related to the substitution method of audio steganography. inside the first degree of protection, we use an progressed RSA encryption algorithm (RPrime RSA) to encrypt message, which could be very complex to interrupt. Within the next level, the encrypted message is to be encoded into audio statistics for this we use a more powerful GA (Genetic set of rules) based totally Least huge Bit) algorithm. a good way to boom the robustness against intentional attacks wherein the hackers constantly strive to reveal the hidden message in addition to some unintended attacks together with noise addition, the encrypted message bits are embedded into random LSB layers. right here in order to reduce distortion, GA operators are used. The fundamental concept at the back of this paper is maintained randomness in message bit insertion into audio statistics for hiding the records from hackers and to provide a terrific, efficient technique for hiding the facts from hackers and dispatched to the vacation spot in a safer manner [5].

Keywords: *Audio Steganography, LSB, GA, HAS, HVS, RSA.*

INTRODUCTION

Steganography is the art and science to cover statistics in a cowl media such as text, audio, picture, video, and so forth [7]. The term steganography in Greek actually approach, "protected Writing" [15]. Steganography is the primary a part of the short developing region of information hiding [14]. Steganography affords strategies for hiding the lifestyles of a secondary message within the presence of a number one message. The number one message is called the carrier signal or service message, the provider sign can be textual content, audio, photo, video, etc.; the secondary message is referred to as the payload sign or payload message [1]. The message is being hidden in this sort of manner that the existence of secondary message is unknown to the observer and the service signal is modified in animperceptible manner [13].

There are various extraordinary steganographic strategies for hiding the secret message. The essential requirement for a steganographic method is imperceptibility because of this that the name of the game messages must now not be discernible to the human eye. There are two different requirements, one is to maximize the embedding capability, and the alternative is safety [8].

Amongst different Steganography sorts, one technique is the use of audio documents as stego-media. In a laptop-based totally audio steganography system, virtual sound is used for hiding secret message. by using barely changing the binary series of a sound record the secret message is embedded into the audio signal [3]. in the beyond few years, numerous algorithms have been offered for the embedding and extraction of message in audio sequences. all of the evolved

algorithms take benefit of the perceptual homes of the human auditory machine (HAS) in order to upload a message into a number sign in a perceptually transparent way. Hiding extra facts into audio sequences isa extra tedious task than that of snap shots [1], as Human Auditory gadget (HAS) is greater sensitive than Human visual device (HVS).The strategies proposed in this paper integrate the techniques of audio steganography and cryptography, so as to make the message extra secure. in this paper, cowl medium is an audio and the name of the game message used is textual content. In all application situations mentioned above, multimedia steganography

strategies ought to satisfy two primary necessities. the first requirement is perceptual transparency, i.e. cover object (item not containing any additional facts) and stego item (item containing mystery message) ought to be perceptually imperceptible. the second one constraint is excessive facts fee of the embedded statistics.

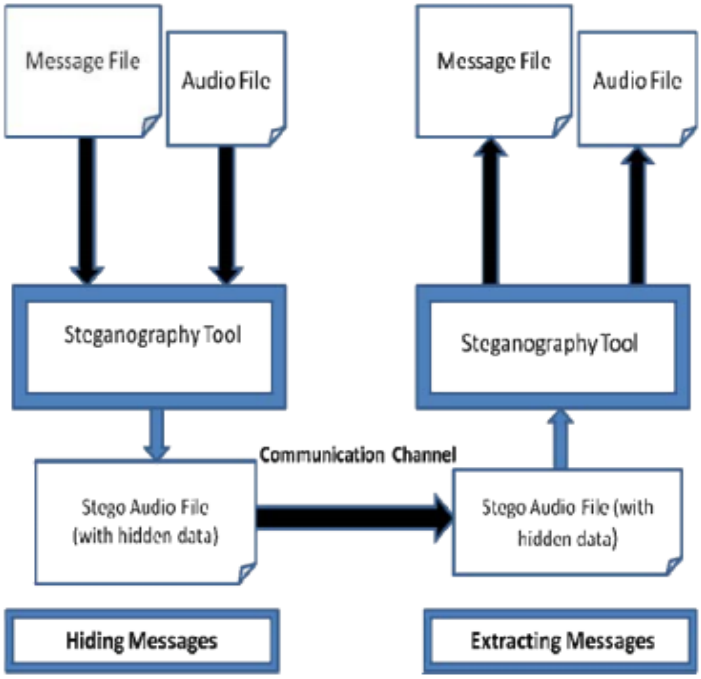

Fig1: *Audio Steganography Manner*

all the stego-applications, except requiringa high bit price of the embedded facts, have need of algorithms that hit upon and decode hidden bits without get right of entry to to the original multimedia collection [6]. in this paper we take a textual content file as a textual content message, the use of RPrime RSA encryption algorithm encrypt the textual content message and shop the encrypted text message into another record "encrypt.txt". Now examine the audio .wav report byte clever, and convert the encrypted text document into byte. Then applying proposed LSB set of rules, embed message bits to the audio bit steam in random positions (to boom the robustness) to get the stego-audio, right here Genetic algorithm operators are used to decrease the bit stage deviation happened between host audio and stego-audio. Now to get the original messageobserve opposite LSB approach and RPrime RSA decryption method on stego-audio.

RELATED WORK

unique strategies are already used to cover message intoaudio document, i.e., in Audio Steganography. to begin with, simpleLSB, then modified LSB method had been used [2]. some of theauthors tried to growth the LSB layer to increase therobustness against assault. It always increases the distortionin host audio.in this paper we initially encrypt the message the use of uneven algorithm (RPrime RSA) after which encryptedmessage bits are inserted at random better LSB layerfunction of the host audio. This allows in growing therobustness.

METHODOLOGY

in this paper, first, we encrypt text message the usage of RPrime RSA encryption set of rules. and then applying proposedLSB algorithm, embed message bits to the audio bit move(sixteen bit pattern) in random and better LSB layer positions(boom the robustness) to get a group of chromosomes.

Now Genetic algorithm operators are used to get the followinggeneration chromosomes. subsequent choose the nice chromosomein step with the high-quality health value. fitness cost is a fee ofLSB role for which we get a chromosome with theminimal deviation evaluating to the authentic host audiosample. here better LSB layer is given better preference incase of layer choice. we have authentic audio pattern andplacing message bit in extraordinary LSB layer positions we getsome new samples. now and again it is able to show up that for morethan one LSB layer we get the same difference amongunique audio pattern and new audio samples. In this situation,we will pick the higher LSB layer [2].

on this paper, an wise algorithm is used to embed themessage bits within the deeper layers of samples and regulate differentbits to lower the mistake and if alteration is not possible forany sample it will ignore them, which facilitates in attainingbetter capacity which refers to the quantity of recordsthat a data hiding scheme can correctly embed withoutintroducing perceptual distortion in the marked media androbustness which measures the potential of embedded data orwatermark to resist against intentional and accidentalattacks [9].

GENETIC algorithm approach

Within the genetic algorithms, the parameters are represented by usingan encoded binary string, called the "chromosome". And theelements within the binary strings, or the "genes", are adjusted toreduce or maximize the health price. The health functiongenerates the fitness value of chromosomes, which iscomposed of more than one variables to be optimized by GAoperators and also facilitates in calculating mistakes [10].

There are 4 main steps on this set of rules:-

a. Alteration

step one is alteration. The alteration step inside the geneticset of rules refines the coolest solution from the contemporarytechnology to provide the following generation of candidatesolutions. in this step, the message bits are changed with thetarget bits of samples. goal bits are those bits which might bepositioned at the layer that we want to adjust. this is done with the aid of asimple substitution that does not want adjustability of end resultbe measured [4].

b. modification

This step is the most critical and important part ofset of rules. All effects and achievements that we count on aredepending in this step. in this level two unique efficientand wise algorithms may be used with the intention to try andlower the amount of error and enhance the transparency. Transparency evaluates the audible distortion because of signadjustments like message embedding

or attacking. one in all them is a easy and ordinary approach, but in thing ofperspicacity may be more green to regulate the bits ofsamples better.

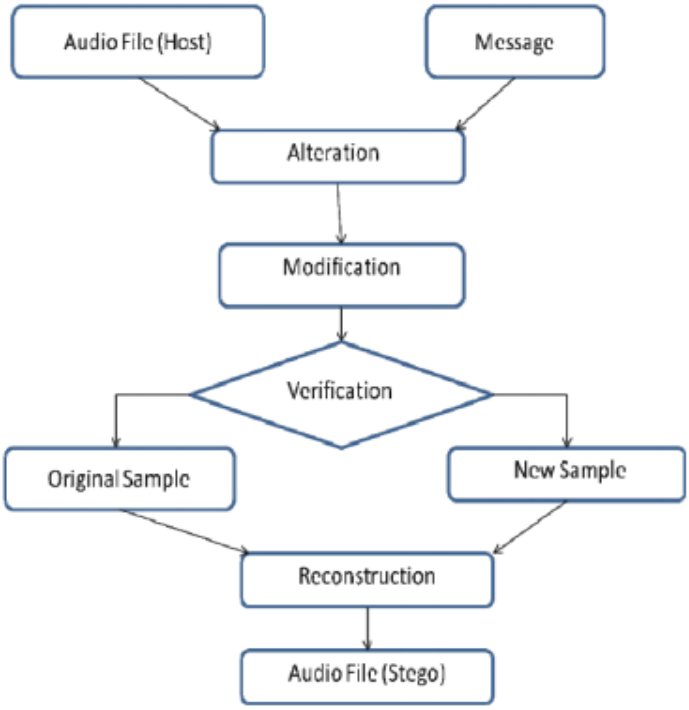

Fig2: *Genetic method Diagram*

c. Verification

In truth this level is first-class controller. What the algorithm could do has been accomplished, and now the final results should be validated. If the distinction between unique sample and new sample is suitable and reasonable, the brand new pattern may be time-honored; in any other case it is going to be rejected and original samplewill be utilized in reconstructing the brand new audio file as opposed to that [4].

d. Reconstruction

The closing step is the creation of new audio record (stego file).that is finished pattern with the aid of sample. There are states at the enter of this step. both changed pattern is input or theoriginal pattern that is the identical with host audio record. it iswhy we can say that the set of rules does now not adjust all samples or predictable samples. meaning relying at the status of samples (environment) and the selection of wise algorithm; which sample can be used and modified is determined [12].

5. expected final results

Proposed Audio Steganography set of rules will be used for five audio sequences from exclusive music styles (classical,pop, jazz, techno, rock). All music pieces might be watermarked the use of the proposed and GA based LSB watermarking set of rules.

The hackers will now not be able to discriminate the 2 audioclips (unique audio sequence and watermarked audio sign). effects of subjective checks will show that if the proposed set of rules is used for embedding then the perceptual satisfactory of watermarked audio will be higher in contrast to standard LSB embedding approach. this could verify that the defined algorithm has succeeded in growing the depth of the embedding layer and also in randomizing the bit layer without affecting

the perceptualtransparency of the watermarked audio signal.
consequently, there could be a extensive improvement in robustness in opposition to signal processing manipulation, because the hidden bits can be embedded better LSB layers deeper than within the standard LSB method.

ADVANTAGES OF OUR METHOD

- The used set of rules succeeds in now not handiest increasing the intensity of the embedding layer however also layer is chosen randomly without affecting the perceptual transparency of the stego audio sign.
- considering the fact that optimization is completed the use of Genetic algorithmoperators, there's message bit embedding that reasons minimum embedding distortion of the host audio.
- there may be a two-manner robustness (to recognize the actual role of the message bit) are there, First, insertion positions are randomly selected, 2nd, LSB layer are most of the time is high layer.
- Listening checks confirmed that during case of proposed technique the perceptual satisfactory of watermarked audio is better than in case of the standard LSB technique.
- for the reason that there's a substantial range of bits flipped in a number in bit layers and the adversary cannot perceive precisely which bit layer is used for the data hiding, for this reason the stegoanalysis of the proposed algorithm is more challenging.
- The proposed algorithm obtains significantly decrease bit errors charges compared to the same old algorithm.

CONCLUSION

in this paper, an smart set of rules is used in order to try and embed the message bits within the deeper layers of samples and regulate other bits to decrease the error and if alteration isn't feasible for any samples it will forget about them. To attain higher ability and robustness, the message bits are embedded into multiple, vague and deeper layers through the use ofthe proposed genetic set of rules [11]. by using using this method of records hiding the observer will now not be capable of suspect that the statistics is there at all. again, if a person knows that facts is in the audio, it is very difficult to extract the statistics from the host audio. the important thing concept of the algorithm is random and higher LSB layer bit embedding maintaining minimal embedding distortion of the host audio. Listening checks showed that described set of rules succeeds in growing the intensity of theembedding layer from lower to better random LSB layers without affecting the perceptual transparency of the stegoaudio sign. since the proposed algorithm obtains notably decrease bit mistakes prices in comparison to the trendy set of rules, consequently the improvement in robustness in presence of additive noise is obvious. Our paintings may be further prolonged to a new level in which possible use the proposed set of rules for hiding photograph.

REFERENCES

1. *Zamani, M., Manaf, A.A., Ahmad, R.B., Zeki, A.M., &Abdullah, S. (2009) A genetic-set of rules-based technique for audio steganography. world Academy of science, Engineering and era, fifty four.*
2. *Krishna Bhowal, AnindyaJyoti friend, Geetam S. Tomar, P. P. Sarkar, "Audio Steganography the usage of GA", IEEE complaints, 2010.*
3. *Krishna Bhowal, Debnath Bhattacharyya, AnindyaJyoti pal, Tai-Hoon Kim, "A GA based totally audio steganography with greater*

protection", Springer technology, enterprise Media, LLC 2011.

4. *MazdakZamani, HamedTaherdoost, Azizah A. Manaf, Rabiah B. Ahmad, and Akram M. Zeki, "sturdy Audio Steganography thru Genetic algorithm", IEEE, 2009.*
5. *Sridevi, R., Damodaram, A., &Narasimham, S. V. L. green technique of audio steganography with the aid of changed LSB set of rules and strong encryption key with stronger security. magazine of Theoretical and applied data era, 2005–2009 JATIT.*
6. *Cvejic N. and Seppänen T. "growing the potential ofLSB based totally audio steganography", Proc. fifth IEEEglobal Workshop on Multimedia signal Processing, St. Thomas, VI, December 2002, pp. 336-338.*
7. *ElhamGhasemi, JamshidShanbehzadeh, NimaFassihi,"excessive potential photo Steganography usingWaveletrework and Genetic algorithm", complaints of the global MultiConference of Engineers and pc Scientists Vol. 1, 2011.*
8. *Lee, Y. okay.,& Chen, L. H. (2000). high capability imagesteganographic model. In IEEE proceedings vision, photograph and signal processing (pp. 288–294).*
9. *palS.okay., Saxena P. k. and MuttoS.okay. "The destiny of Audio Steganography". Pacific Rim Workshop on digital Steganography, Japan, 2002.*
10. *C. S. Shieh, H. C. Huang, F. H. Wang and J. S. Pan, 'Genetic Watermarking based on remodel-areastrategies', sample popularity, vol. 37, no. three, pp.555-565, 2004.*
11. *eleven. MazdakZamani, AzizahBt Abdul Manaf, RabiahBtAhmad3, FarhangJaryani, HamedTaherdoost, SamanShojaeChaeikar, and HosseinRouhaniZeidanloo, "a unique method for Genetic Audio Watermarking", journal of information warranty and protection five, 2010,102-111.*
12. *MazdakZamani, AzizahBt Abdul Manaf, HosseinRouhaniZeidanloo and SamanShojaeChaeikar, "Genetic substitution-based totally audio steganography for high capability packages", Int. J. internet era and Secured Transactions, Vol. three, No. 1, 2011,ninety seven-one hundred ten.*
13. *Westfeld A. and Pitzmann A. "attacks on Steganographic structures". Lecture Notes in pc science, vol. 1768, Springer-Verlag, Berlin, pp. 61-seventy five, 2000.*
14. *Petitcolas, F. A. P., Anderson, R. J., & Kuhn, M. G.(1999). factshiding—a survey. court cases of IEEE, 87(7), 1062–1078.*
15. *Fridrich, J. et al. (2000) 'Steganalysis of LSB encodingin colour photos', court cases of the IEEE worldwide convention on Multimedia and Expo, IEEE Press, New York, pp.1279–1282.*