Journal of Engineering Sciences
Vol 11, Issue 6,June/2020
ISSN NO:0377-9254

Audio Steganography Based on LSB Encryption and Chaos Encryption

Mohammed Ishaq Hussain[1], Syed Abubakar Siddiq[2], Prof Rafath Samrin[3]
UG Scholar, Dept of IT, ISL Engineering college, Bandlaguda, Hyderabad, Telangana[1,2]
HOD, Dept of IT, ISL Engineering college, Bandlaguda, Hyderabad, Telangana[3]

Abstract:

An enhancement of data protection system for secret communication using reserve room in encrypted audios based on texture analysis with lifting wavelet is proposed here. The wavelet will decompose the audio into four frequency sub bands namely LL, LH, HL and HH. These coefficients are then utilized in the encoder for removing the redundancies. The Selective embedding is utilized in this method to determine host signal samples suitable for data hiding. This approach uses the Least Significant Bits (LSB) insertion to hide data within encrypted audio data. The binary representation of the hidden data is used to overwrite the LSB of each byte within the encrypted audio randomly .The hidden data will be used to enable the receiver to reconstruct the same secret transformation table after extracting it and hence the original audio can be reproduced by the inverse of the transformation and encryption processes. We proposed the encrypting user's data using RC7 Algorithm with a Secret Key, Which is embedded in a Audio using LSB based audio steganography techniques. The simulation results indicate that the framework can be successfully utilized in Audio data hiding applications.

Key words: LSB, wavelet, encryption

INTRODUCTION:

All modern steganography algorithms for digital audios are content adaptive in the sense that they restrict the embedding modifications to complex regions of the cover which are difficult to model for the steganalyst. The probabilities with which the individual cover elements are modified (the selection channel) are determined jointly by the size of the embedded payload and content complexity. The most accurate detection of content-adaptive steganography is currently achieved with detectors built as classifiers trained on cover and stego features that incorporate the knowledge of the selection channel. While selection-channel-aware features have been proposed for detection of spatial domain steganography, an equivalent for the JPEG domain does not exist. Since modern steganography algorithms for Audio are currently best detected with features formed by histograms of noise residuals split by their JPEG phase, we use such feature sets as a starting point in this paper and extend their design to incorporate the knowledge of the selection channel. This is achieved by accumulating in the histograms a quantity that bounds the expected absolute distortion of the residual. The proposed features can be computed efficiently and provide a substantial detection gain across all tested algorithms especially for small payloads.

METHODOLOGY:

Currently, three main methods are being used to protect data: cryptography, watermarking, and steganography. Cryptography involves scrambling secret information to make it unreadable to eavesdroppers . Cryptography not only turns plaintext into ciphertext, but also exposes the importance of secret information, thus arousing the curiosity of attackers. Steganography and watermarking are two important branches of information hiding and they embed data transparently into carrier objects. Watermarking establishes the identity of information to prevent unauthorized use. It embeds the information into digital file in such a way that its removal is hardly possible. The main difference between steganography and watermarking is that watermarking does not necessarily hide the fact that information is transmitted secretly from a third party. Steganography emphasizes the imperceptibility and undetectability of information and requires a considerable capacity for communication efficiency.

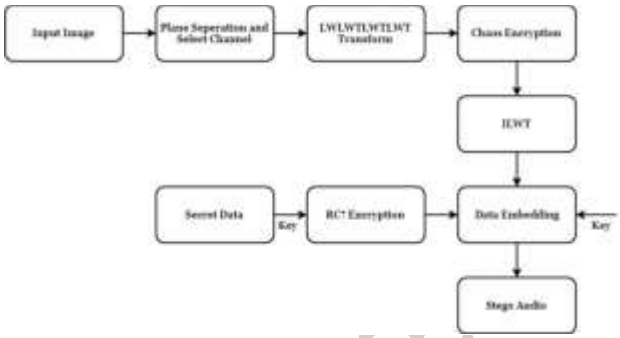
The object to be protected by digital watermarking is the carrier object, and the main performance required by digital watermarking is robustness .

There are many carriers of steganography, including audio, audio, video, text and other multimedia files. At present, there are many researches on audio steganography. Compared with audio, audio steganography is less studied. Since human auditory system (HVS) is more sensitive than human visual system (HAS), the change of audio signal is more likely to cause human sensory perception, which also puts forward higher requirements for audio steganography technology. Human auditory system is the second largest source of information acquisition after visual system. At the same time, audio, as a kind of multimedia, has the characteristics of wide frequency range and high redundancy. Voice chat in instant messaging and the popularity of VOIP also lead audio to more application fields. Therefore, the study of audio steganography technology has important significance and broad application prospects.

PROPOSED METHOD:

The Audio Steganography technique is based on,Lifting Wavelet Transform (LWT) and Least Significant Bits (LSBs) substitution. In order to increase the security level a simple encryption with chaotic key has been proposed. The proposed system has a high sensitivity in choosing keys because a small change in CKG causes a new secret key for transmitting. Speech steganography algorithm that based on (LWT) can satisfy full recovery for the embedded secret messages in the receiver side. The lifting scheme of DWT is an algorithm to implement wavelet transforms in an efficient way. It is also a wonderful method to create so-called second-generation wavelets. The lifting wavelet transform is a multi-resolution representation that means the signal divided to two parts the first called approximation sub-band and second part named detail sub-band these parts are obtained by applying corresponding wavelet filters (high-pass filter, low-pass filter). Generally lifting scheme consists of three steps, Splitting, production, and update with the Chaos crypto system and RC7 Encryption for secret data.

BLOCK DIAGRAM:



In every system of steganogrpahy we can take the two major blocks based on the performance work. Those are embedding and extracting. Here we are giving some cryptography systems

CRYPTOGRAPHY

Symmetric Key Algorithms :

In this algorithm, the same key is used by transmitter and the receiver to encrypt and decrypt the message respectively.

RC4

RC4 is a symmetric key stream cipher developed by Ron Rivest. It is well known for its simplicity and speed in its software. It uses variable key length typically between 40 and 2048 bits. Here the data stream is XORed with the generated key sequence.

AES

AES also known as Rjindael's algorithm. AES is a symmetric block cipher designed by Vincent Rijmen and Joan Daemen published in 1998. The variable key length are 128, 192 and 256 bits. Two types of hashing algorithms can be used namely SHA1 (Secure hashing Algorithm 1) Digest Size: 160 bits, Block Sizes: 512 bits, Rounds: 80 and MD5 (Message Digest 5) Digest Size: 128 bits, Block Sizes: 512 bits, Rounds: 4

3DES

The triple data encryption algorithm (TDEA) is a Symmetric key block cipher. It applies DES (Data

Encryption Standard) three times to each data block. It uses a Key bundle that consists of 3 keys K1, K2, AND K3 each 0f 56 bits. DES is ubiquitous, easy to implement in both hardware and software. Asymmetric Key Algorithm: In this algorithm the sender and the user use different keys to encrypt and decrypt. The asymmetric key we used here is RSA.

RSA

RSA is a public-key cryptosystems, asymmetric key algorithm. RSA is developed by Ron Rivest, Adi Shamir, and Leonard Adleman in 1977. Here sender and receiver use different keys to encrypt and decrypt.

STEGANOGRAPHY PROCESS

For steganography also we have different types of techniques like

A. Audio steganography

Here an audio is the cover object and information is hidden based on pixel intensities[5]. It make use of different terminologies like cover-audio which is used as carrier for undisclosed information, confidential information to be hidden into audios, stego-audio (message plus cover audio), stego-key for extracting the message.

B. Audio steganography

Here audio file is used as cover object and digital audio formats like WAVE, MPEG etc are used for hiding information [6]. It is one of the effective method to protect the privacy.

C. Video steganography

Here video file is used as cover object and it make use of Mp4, MPEG or other video formats. The embedding of secret information to the video is not visible to human eye [7]. Due to availability of large number of frames secret data can be easily disguised inside a video. Embedding capacity of video is more than the digital audio.

D. Network steganography

In this type, TCP, UDP, IP etc like network protocols are used as a cover object. It uses modification of a single network protocol.

E. Text steganography

Here text is used as cover object. It is classified into three categories: Format based methods, Random and Statistical generation, Linguistic methods.

The key algorithms used for encryption and decryption are AES, RC4, 3DES and RSA. Secret message is encrypted using one of these algorithms. For the proposed work, performance is measured with the AES algorithm. As shown in figure 2, encoded text is the result of outer layer which is to be embedded into the cover that results in StegoAudio. Audio Steganography forms the inner layer of the proposed module where Least Significant Bit (LSB) and Reversible Data Hiding (RDH) Techniques are implemented. Schematic representation of the proposed research work is highlighted in figure 2. The proposed model provides 4 encryption options and 3 embedding options. The proposed algorithm first converts the secrete message into cipher using one of the mentioned algorithm and reversible data hiding takes place on respective cipher. Reverse procedure is applied at the receiver end.Method is applied for gray as well as color audios. The quality of audio is observed for existing algorithm and the proposed algorithm. Also performance is measured for LSB algorithm with AES encryption.

ADVANTAGES

High hiding Capacity & High Robustness
Less degradation in Image quality during hiding

APPLICATIONS
Research institute.
Medical information protection.
Defense application.

SOFTWARE REQUIREMENTS
MATLAB 7.14 and above versions.
Image and Video Processing toolboxes

Result:

CONCLUSIONS

A new algorithm hiding technique is proposed in this paper using chaotic logistic map. This algorithm is simple, fast, and efficient and has high imperceptivity. The chaotic logistic map has been used in encrypting and embedding with DCT which increases the security and imperceptivity because the sensitivity of logistic map to initial condition leads to generate different sequence with different initial value. As seen in experimental results using DCT in embedding will not damage cover images which reflect by value of correlation that equal 1, it means high identical between the cover before and after embedding.

REFERENCES

[1] Reem Majid Mikhail , "Information Hiding Using Petri Nets and Wavelet Transform" theses, Iraq, University of Technology , 2007.

[2] NedaaFleah, " robots method to hide text file in sound wave file against the compression method mp3 " , Thesis ,Technology University, Bagdad 2005.

[3] Haider Ismael Shahadi& Razali Jidin& Wong Hung Way , " A Novel and High Capacity Audio Steganography Algorithm Based on Adaptive Data Embedding Positions" Electronic and Communication Engineering, Tenaga National University (UNITEN), Putrajaya , Malaysia ISSN: 2040- 7459; e-ISSN: 2040-7467 © Maxwell Scientific Organization, 2014.

[4] GEERT UYTTERHOEVEN& DIRK ROOSE &ADHEMAR BULTHEEL "Integer Wavelet Transforms using the Lifting Scheme", IEEE ,IMA CS ,OTE , p 6257-6253.

[5] Michel Misiti& Yves Misiti&Georges Oppenheim &Jean-Michel Poggi , "Wavelet Toolbox™ User's Guide", book , 2014.

[6]"Lifting Scheme of Wavelet Transform" 3TUhttp://shodhganga.inflibnet.ac.in/bitstream/10603/4341/7/07_chapter%203.pdfU0T3

[7] EmanHato Hashim , September 2013, "Speech Signal Encryption Using Chaotic Maps" thesis College of Science, Al Mustansiriyah University, Computer Science department.