Audio Data Security and Feature Extraction over Cloud

Sayyada Fahmeeda
Asst. Professor
P.D.A College of Engineering
Gulbarga, Karnataka, India

Amreen Tabassum
PG Scholar
P.D.A College of Engineering
Gulbarga, Karnataka, India

ABSTRACT
The demand for on-demand services of multimedia; most individuals, companies, and governments use cloud services to maintain confidentiality from intruder from being hacked as every day huge data was embedded in a digital media or distributed over the internet. For this reason, the user require to secure their data and encryption method is the one that provides security to your information and most security system uses this technique which is widely used in the database areas such as internet banking, audio communication channel, phone recordings, music companies, military conversations etc. A Cryptographic encryption method is certainly the best option for maintaining the security to our audio files. As the audio is encrypted it does not make sense to recognize the audio for that reason audio feature extraction method is used for classification purpose. Audio classification involves extracting representative features and feeding them into the classifier. The proposed method provides security to audio files using spread spectrum technique and LSB steganography for easy search of these files by extracting audio features using K-NN classifier.

Keywords
Cryptography, Steganography, Feature Extraction, Audio Classification, Cloud Security.

1. INTRODUCTION
In a modern world with the use of cloud storage systems and computing has increased to a great extent, many critical problems have started to raise heads like Security of personal data being important as the hacker can easily hack so that encryption of multimedia is important. Currently, the exchange of data among users is rapidly grown so that the user requires securing their data systems to maintain the confidentiality of the data from attackers. Secret Information is a very important resource for any organization or individual person. Audio or sound medium is found to be used in many applications for providing security, voice commands, voice synthesis and entertainment. And before the invention of steganography and cryptography, it was challenging to transfer secure information and, thus to achieve secure communication environment. In digital media, Cryptography is a means of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it.

Steganography is in the form of digital security where digital data is hidden inside another digital media. Basically, Steganography is a process of introducing recoverable systematic calculated noise into a media, however irrespective of the quality of an algorithm no steganography technique is untraceable. Audio steganography can be applied to many audio formats as are, wave, mp3, mp4 etc. In this process first, the secret data is encrypted and then hide it in an original data. The stego medium is obtained by the addition of cover medium; here the cover medium is typically an audio file. In a computer based audio Steganographic system, secret messages are embedded in digital signals. In Audio Steganography, the perception of the Human auditory system (HAS) is used to hide information in the audio because it perceives over a wider power range. Embedding secret messages in digital sound is usually a difficult process than embedding data in other media due to its perception. Here, Steganography is often mixed with cryptography.

Cryptography and steganography achieve the same goal of data confidentiality via different means. The main difference between steganography and cryptography is that cryptography concentrates on keeping the contents of a message secret while steganography concentrates on keeping the existence of a message secret.

Audio feature extraction consists of extracting relevant features from a sound, and by using these features we can identify which audio we are searching for. Feature extraction involves the analysis of the input of the audio signal. All audio features are extracted by breaking the input signal into a succession of analysis windows or frames, each of around 10-40-ms length, and computing one feature value for each of the windows. One approach is to take the values of all features for a given analysis window to form the feature vector for the classification decision.

In this work, we propose a strong digital technique by combining cryptography with steganography for protecting audio files. We also embed features extracted from the audio into new audio as metadata for enabling easy search of these files via K-NN classifier.

2. RELATED WORK
Latest advancements in cryptography have added a completely new dimension to data security using encryption algorithm [1] the authors proposed a method for audio cryptography can be combined with audio steganography to provide security to the audio and also the image hidden in the audio. In [2], the researchers propose a secure method for artificially adding reverberation effects to an audio secret over the cloud with (K, N) Shamir's Secret Sharing (SSS) as the cryptosystem for audio recording, reproduction, editing, and enhancement. Their method implements convolution reverb and can be applied to any reverb impulse response and an audio secret in the encrypted domain(ED) over the cloud. Authors in [3] propose a Bio cryptography scheme for auditory signals to extract the secret key from the iris feature, and are utilized to encrypt and decrypt the audio feature. Here AES algorithm is used for encryption and decryption.

Authors in [4],[5],[6],[7] proposed, schemes for embedding image/text in a cover audio file using steganography systems and used the LSB method for embedding a secret message in carrier audio file…In [4] Emphasize will be in the proposed scheme of image hiding in audio and its comparison with a simple least significant bit insertion method for data hiding in

audio. In [5], a random key generator is employed to two purposes. First to encrypt the hidden message, and to generate random jumping in the wave file to give more robustness to the steganography system. In [6] researchers, use steganography technique where the first message will be encrypted using the RSA algorithm then it will be hidden in a cover audio file using LSB technique. Hiding results show no noise in the stego-wave file after embedding process, also no difference in size is observed between the original wave audio file and stego-wave file.In [7] messages is first encrypted using the vigenere square encryption algorithm and then ASCII conversion of data takes place. After those characters in information or data are embedded into deep layers through modified LSB method. After that audio transposition encryption is used for audio.

Authors in 2015[8] and 2016[9] discussed cryptography based secure steganography technique, [8] where firstly encrypt the data using the DES algorithm then embed this encrypted text into an audio file by using LSB modification. The resulting analysis shows that the system is more robust than the existing method and transparency is also maximized. But in [9] messages is encrypted using a newly developed symmetric key lookup XOR cryptographic algorithm and thereafter the encrypted message is embedded inside an image file using LSB. This combinational methodology satisfies requirements such as capacity, security, and robustness for secure data transmission over the network better than DES because it provides a strong encryption scheme with minimized cipher text using a one-to-one mapping.

In [10], the authors present an audio feature extraction scheme which is represented by the scales of the basis vector. In this approach, a set of basis vectors is constructed to extract pitch, timbre and residual inharmonic components from the spectrum and the experiment result shows the effectiveness of the proposed feature which is evaluated on 13 category audio effect classification tasks.

3. PROPOSED WORK

This system uses spread spectrum encryption with XOR operation for audio cryptography and Modified Least Significant Bit(LSB) algorithm for Steganography. The system uses the same key for steganography and cryptography.

3.1 Audio cryptography

In general, the spread spectrum technique, enhance the bandwidth of the message signal. With spread spectrum technique, the addition of real number can flip a basic frequency that is determined by a global variable call encryption depth. The encryption process begins with preprocessing segmentation of voice data. The systems consist of two main processes encryption and decryption.

3.1.1 Encryption process: the encryption process begins with a reading of the original WAV file using WAV reader. The audio processing data is completed by inserting the key to separate the audio data to be encrypted.

3.1.1.1 Codeword Generation: The key entered by the user is not used as it is for encryption. The key is converted to the codeword. The codeword generator takes the key from the user. Performs an operation on it and generates the codeword. The generated CODEWORD is given to the encryption module.

3.1.1.2 Encryption: This module converts the audio data into un-meaningful binary data. This is achieved with the help of CODEWORD. The encryption module performs a XOR operation between original audio data and the CODEWORD generated as shown in the figure1 below.

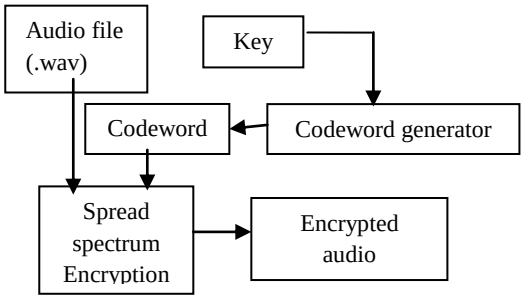

Fig 1: Encryption Process

3.1.2 Decryption Process: Decryption process is a reverse of the encryption process. This process commences with reading encrypted WAV files using the same key of an encrypted process.

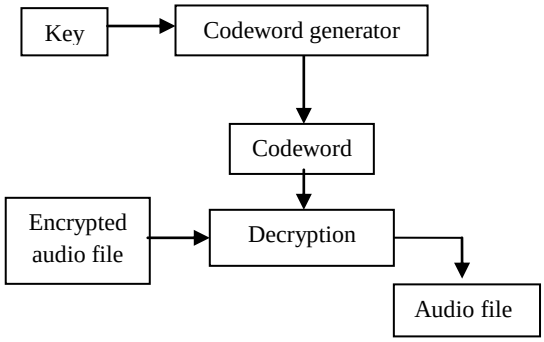

Fig 2: Decryption Process

For Decryption process also the user needs to enter the key. Again key entered by the user is not used as it is for decryption. The key is transformed into the codeword. The codeword generator takes the key from the user, performs an operation on it and finally decryption process is carried out. The diagram for audio decryption is shown in figure2.

3.2 Audio steganography

We are suggesting a system that can be built by considering steganography and cryptography approach. The proposed system will accept the information as an input (text file).

This information (text file) will be encrypted by an approach of cryptography i.e. AES algorithm. Once the encryption is done, then the data can be made ready to hide behind an audio file format (.wav file) by applying steganography approach. This way it will be a safe option to send this audio file (.wav) over the network without worrying for the hidden information. This way sender may feel quality trust on his data sharing aspect.

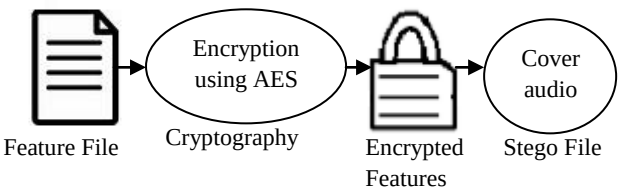

Fig 3: audio feature in cover audio.

Here AES uses 128-bit block encryption. 128-bit encryption is a data/file encryption technique that uses a 128-bit key to encrypt and decrypt data or files. It is one of the most secure encryption methods used in most modern encryption algorithms and technologies. 128-bit encryption is considered to be logically unbreakable. And finally, the data can be hidden in a wave file using LSB method.

3.2.1 Least significant bit (LSB): This system uses the least significant bits in every sample of the encrypted audio file to hide a sequence of bytes containing the secret data. LSB coding is the simple way to hide information in a digital audio file by replacing the least significant bits of each sample with a secret message. The least significant bit (LSB) is the bit position in a binary integer giving unit value similar to unit value in decimals. The LSB is also referred to as the right-most bit.

3.2.2 Extraction Of feature file: The function of this module is to extract the text data from a wave file. This module uses a reverse LSB algorithm to fetch out the text bits from a Wave file (Stego File). The extraction is based on the mode in which the data is hidden.

3.3 Audio searching and classification

This is the major part of our project. Audio classification system analyzes the input audio signal and creates a tag that describes the signal at the output. The tag here is the feature values of each input audio which are unique to each and every audio. Obviously, for searching, we need to extract the characteristics features of audios like spectral density, pitch and so on… An audio signal classification system should be able to categorize different audio input formats. Particularly, detecting the audio type of a signal a sample audio is given that matches with the other audio features present in the cloud.

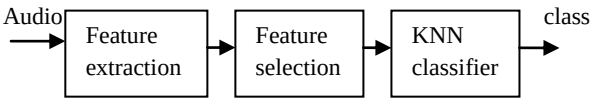

Fig 4: audio classification system.

Once the features are matched K- Nearest neighbor classifier is used for classification of audios. K-nearest neighbors (KNN) is a simple algorithm that stores all available cases and classifies new cases based on a similarity measure. Using KNN algorithm we can identify and categorize the common or nearest audio feature in MATLAB. In *k-NN classification*, the output is a class membership. An object is classified by a majority vote of its neighbors, with the object being assigned to the class most common among its *k* nearest neighbors. The neighbors are taken from a set of objects (database feature values) for which the class (for *k*-NN classification) or the object property value is known. This can be thought of as the training set for the algorithm, though no explicit training step is required.

4. RESULT AND DISCUSSION

The original Wave file before hiding the text content and the Wave file after hiding the text content (stego file) is having the same size. The secret text file was hidden in Cover Wave file using LSB method. The text file generated after de-stegano process and having the same size as that of an original text file before hiding. The Cover wave file with different sample rates was used for testing purpose. But they were no any adverse effects due to change in sample rate. An increase in sample rate further increases the capacity of hiding secret data. The original text can be securely and properly extracted from the stego file.

Table 1: Test result of steganography process.

Class	Cover media size	Secret message (input)	Encrypted message size	Stego file size
Animal	79 KB	enc.xls	10 KB	79 KB
Hindi	79 KB	enc.xls	10 KB	79 KB
Kannada	79 KB	enc.xls	10 KB	79 KB
Music	79 KB	enc.xls	10 KB	79 KB
vehicle	79 KB	enc.xls	10 KB	79 KB

The result of data hiding and data extraction process is shown is table 1 and table 2.

Table 2. Test result De-steganography process.

Class	Stego file (input)	Stego file size	Recover text file after un-hiding	Recover text file size
Animal	Stego1.wav	79 KB	feature.xls	22 KB
Hindi	Stego1.wav	79 KB	feature.xls	22 KB
Kannada	Stego1.wav	79 KB	feature.xls	22 KB
Music	Stego1.wav	79 KB	feature.xls	22 KB
Vehicle	Stego1.wav	79 KB	feature.xls	22 KB

As shown in table 3 and figure5 –Signal to noise ratio and mean square error changes for different audio class even if the audio file size is same.

Table 3: MSE & PSNR values for different audio class Audio file of size: 80Kb.

Class	Signal to noise ratio in db	MSE in db
Animal	33.95	2488.62
Hindi	37.71	5894.92
Kannada	29.23	837.8
Music	31.77	1505.4
Vehicle	32.95	1975.33

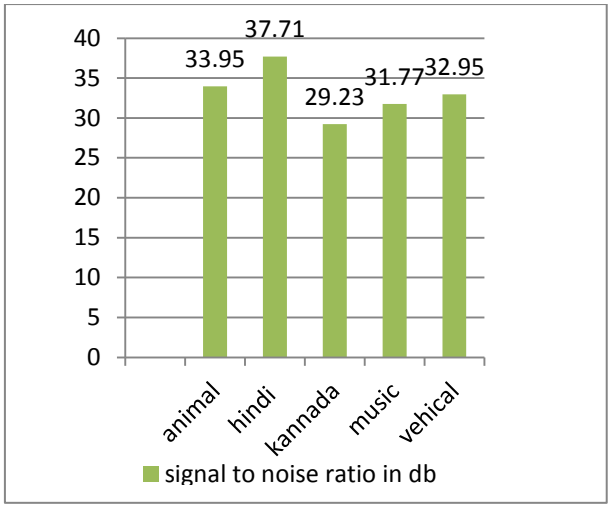

Fig 5: signal to noise ratio in db.

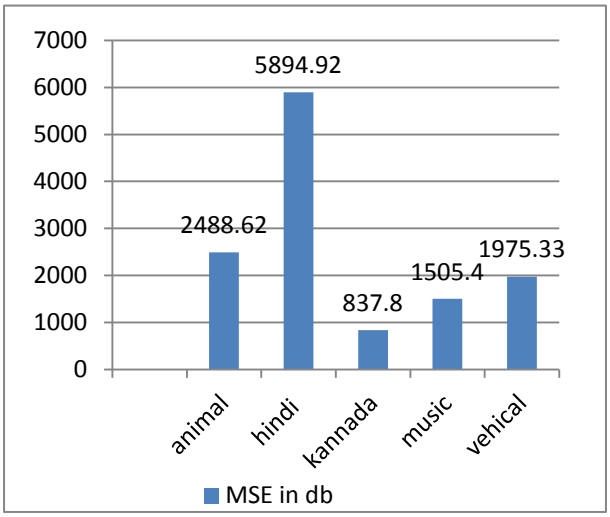

Fig 6: mean square error in db.

Table 4: Showing Ciphertext capacity to Plain text

	Plaintext in samples	Plaintext length	Ciphertext length		Time taken	
			DES	XOR	DES	XOR
1	8000	4	16	16	1.9510	0.7142
2	16000	5	16	16	0.9328	0.7336
3	24000	5	15	7	0.7803	0.6969
4	32000	5	16	16	0.8078	0.7203
5	40000	5	16	11	0.8113	0.7076

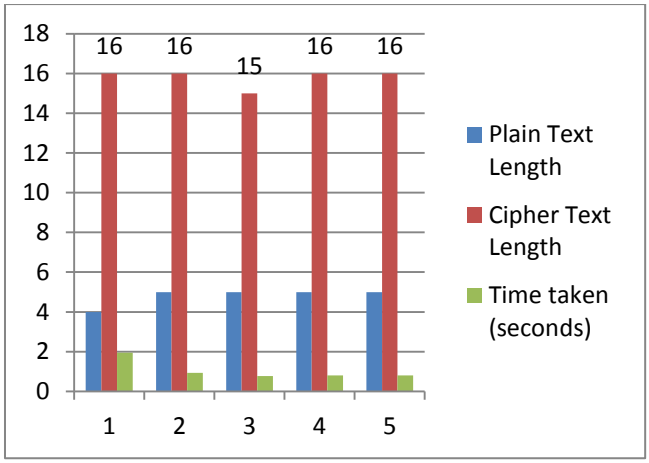

Fig 7: Time taken by DES algorithm for encryption.

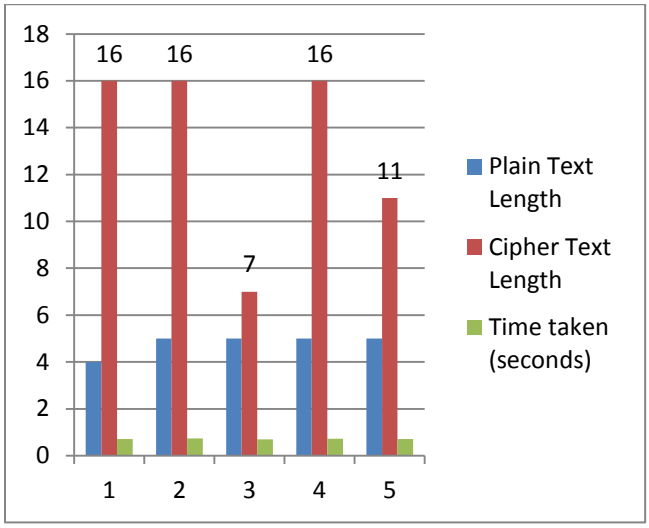

Fig 8: Time taken by XOR method for encryption.

The time complexity of the encryption algorithm was analyzed and its value was established both for its Worse and Best cases. Thereafter the performance evaluation was carried out using the cipher text capacity of the system compared to the ciphertext capacity of Data Encryption Standard (DES) against ex-or as shown in Table 4 and Figure 7 and 8 respectively.

Experiments were carried out on algorithms, the well-known Data Encryption Standard (DES) and the developed XOR using the same plain text to show how they fair with respect to the capacity of ciphertext produced after encryption. The experiments were repeated five (5) times with different plaintext size and its corresponding ciphertext on the same machine. The results are shown in Table 4.

5. CONCLUSION AND FUTURE SCOPE

The target of this paper is to implement three techniques like steganography, cryptography for secure transmission of audio data and audio classification for searching of the data by calculating the feature vector values as an input. In this paper, spread spectrum with XOR method used for cryptographic encryption and LSB technique is for steganography and K-NN classifier is used for identification and classification of the audios.

The result of this work can be used to provide security for audio files, searching for the files and is recommended for organizations, departments, companies where information security is required. Further research on this work can be carried out for other stego objects such as video files were the searching process is done for video files. The result shows that the proposed system offers almost homogeneous MSE and PSNR irrespective of the type of the audio and accuracy of the audio classification is 98%.

The system can further be improved by improving the audio encryption techniques as spread spectrum is considered to be extremely elementary audio encryption method such complicated audio encryption technique may also bring with it the challenges with relating to time and computation complexities must be overcome by using appropriate optimization technique such as linear programming and quadric programming.

6. REFERENCES

[1] Alisha sikri, taruna, kirti rana,"security of digital data using combination of audio steganography and cryptography". International Journal of Engineering Development and Research © 2016 IJEDR | Volume 4, Issue 2 | ISSN: 2321-9939.

[2] M. abukari y, pradeep k. atrey, namunu c.maddage,"secure audio reverberation over cloud". 10th annual symposium on information assurance(asia '15), June 2-3,2015, albany, ny Fröhlich, B. and Plate, J. 2000. The cubic mouse: a new device for three-dimensional input. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems

[3] Sruthi B. Asok, P. Karthigaikumar, Sandhya R, Naveen Jarold K, N.M Siva Mangai, "a secure cryptographic scheme for audio signals"International conference on Communication and Signal Processing, April 3-5, 2013, India. 978-1-4673-4866-9/13/$31.00 © 2013 IEEE

[4] Pradeep Kumar Singh and R.K.Aggrawal," Enhancement of LSB based Steganography for Hiding Image in Audio", (IJCSE) International Journal on Computer Science and Engineering, ISSN : 0975-3397, Vol. 02, No. 05, 2010, 1652-1658

[5] Inas Jawad Kadhim " A New Audio Steganography System Based on Auto-Key Generator", Al-Khwarizmi Engineering Journal, Vol. 8, No. 1, PP 27 - 36 (2012)

[6] Harshita kapadia, Harawane sneha Haribau, Harsha patil " audio steganography and security using cryptography", IJCSN, volume 4, issue 2, April 2015

[7] Nisha kundu, Dr. Amadeep kaur, "A secure Approach to audio steganography" international journal of engineering trends and technology (IJETT), vol 44, No. 1, February 2017

[8] Surubhi bhansal and puneet Sharma "cascaded cryptography and audio styeganography" international journal of engineering, applied and management sciences paradigms, Vol 26, Issue 01, July 2015

[9] William W.F, Osofisan A.O, Asanbe M.O, " A lookup XOR cryptography for high capacity least significant bit steganography" IJAIS, Vol 10- No. 7, March 2016.

[10] Xueyuan Zhang, Zhuosheng Su, Pei Lin, Qianhua He, Jichen Yang, "An Audio Feature Extraction Scheme Based on Spectral Decomposition". 978-1-4799-3903-9/14/$31.00 © 2014 IEEE.