Novel Algorithm for Audio Based Steganography using variable key

Anju[1], Sudhir Rathi[2]
[1]*M.Tech Scholar,Sobhasaria Grop of Institution, Sikar ,Rajasthan*
[2]*Assistant Professor, Sobhasaria Grop of Institution, Sikar ,Rajasthan*

***Abstract*- Data Transfer is the basis of any of the communication process. And the possibility is always there that the data can be captured by the intruders.**
In the processed work, we are dealing with the audio message transfer in this to securely transfer the text message we have embedded or hide the text message within the audio message using the key and the key will be required to extract the required message.

INTRODUCTION

Security has dependably been a vital part of human. We are encompassed by a universe of secure communication, where individuals of different types are transmitting data such as credit card number to an online store than and as cunning as a terrorist plot to hijackers. The strategies that make secure communication practicable are not new. There has dependably been a need of securing the messages that are sensitive in nature. Such messages if presented to a few intruders may represent a risk to country's security or organization's basic choices. Therefore, such data must be secured at any expense and to fill the need to encrypt or hide the data. Cryptography (derived from Greek work 'kryptos' meaning hidden and 'graphein' meaning to write) [1] is utilized to encode the content to make it understandable. Cryptography may draw the suspicion of the intruder or third party towards the content that is in encoded. Steganography is the craftsmanship and exploration of composing concealed messages in such a way that nobody, aside from the sender end expected beneficiary, suspects the presence of the message, a type of security without knowledge of its presence. The word Steganography is of Greek origin and means "concealed writing" from the Greek words steganos meaning "covered or protected", and graphein meaning "to write" [2]. Steganography can be categorized based on the kind of media it utilizes to hide the data.

Text Steganography: It conceals the text behind some other text file. It is toughest type of steganography as the repetitive measure of text to hide the secret message is rare in text files.

Image Steganography: This type hides text or an image inside another text. It is the most frequently used strategy due to the restriction of the Human Eye.

Audio Steganography: Audio Steganography is a method used to transmit hidden data by adjusting a sound sign in an undetectable way. It is the science of concealing some secret text or audio data in a host message [3]. The host message before applying steganography and stego message after steganography have the same attributes..

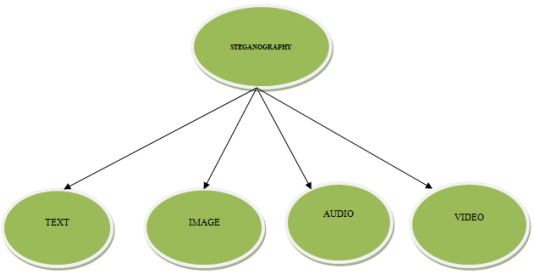

Figure 1 - Types of Steganography

Video Steganography: Video Steganography is the procedure of concealing some secret data inside a video. The expansion of this data to the video is not conspicuous by the human eye as the change of a pixel color is negligible.

II. AUDIO STEGNOGRAPHY

In audio steganography secret data is embedded in cover audio which consists of carrier (audio file), message and password. A basic model of audio

steganography is shown in Fig. 2.In this section, some important techniques of audio steganography are discussed in brief.

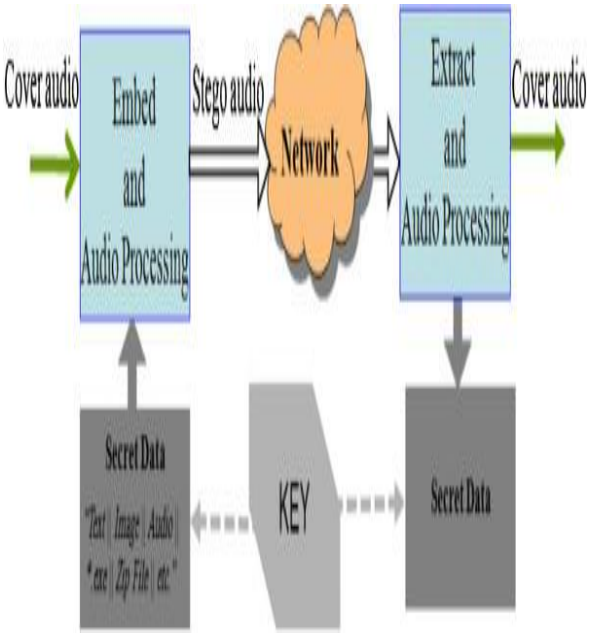

Figure 2 Audio steganography model

LSB Coding

A very basic methodology is the LSB (Least Significant Bit) algorithm, in this technique we replace the least significant bit(right-most bit) in some bytes of the cover file to hide a sequence of bytes containing the hidden data. This technique is usually an effective technique in cases where the LSB substitution doesn't cause significant quality degradation.

Phase Coding

In phase coding technique we replace the phase of an initial audio segment with a reference phase that represents the secret information. The phase of remaining segments is adjusted in order to preserve the relative phase between segments. In terms of SNR (signal to noise ratio) , Phase coding is one of the most effective coding methods. As long as the modification of the phase is sufficiently small, an inaudible coding can be achieved.

Parity Coding

In this method we break a flag into separate examples and install each bit of the secret message from an equality bit. In the event that the equality bit of a chose area does not coordinate the secret bit to be encoded, the process transforms the LSB of one of the examples in the district. In this way, the sender has all the more a decision in encoding the secret bit.

Spread Spectrum

In this method sender endeavors to spread secret information across the frequency range of the sound flag utilizing a code which is free of the real flag. Accordingly, the last flag possesses a data transmission which is more than what is really required for transmission. This method is capable of contributing a better performance in some areas compared to LSB coding; phase coding, and parity coding techniques in that it offers a moderate data transmission rate and high level of robustness against removal techniques. The Spread Spectrum method has one main disadvantage that it can introduce noise into a sound file.

Echo Hiding

In this method we insert the secret information in a sound document by bringing a reverberate into the discrete signal. This method gives a high information transmission rate and better strength when looked at than different methods. Prior to the encoding process starts the first signal is separated into squares. Once the encoding process is done, the pieces are linked back together to make the last signal.

.

III. LITERATURE SURVEY

H. Liu, J. Liu, R. Hu, X. Yan and S. Wan[1] This paper proposes an adaptive audio steganography scheme based on wavelet packet energy which can be used to hide secret messages in digital audio. The major contribution of the proposed scheme is that the wavelet packet sub-bands of the host audio can be selected adaptively to embed the secret messages according to the masking effect of human auditory system (HAS) and weighted energy concentration . First, the host audio is divided into many segments which are then decomposed by wavelet packet to calculate the wavelet packet energy feature. Second, the covert data are embedded into each segment through adjusting the relationship among wavelet packet sub-bands by modifying or exchanging the coefficients of wavelet packet sub-bands. Finally, the experimental results and comparison with existing technique show that the proposed scheme has larger hiding capacity while maintaining imperceptibility and strong robustness.

J. S. Lamba, K. Sachdeva, V. Sinha and N. Singh[2] In this digital age, there has been a surge in the transmission of digital data. This data is not secure

and it can be easily intercepted and misused by an eavesdropper. To secure this data, steganography is used. 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 audio. If the existence of a message is unknown, it makes it harder to decrypt that message. Audio steganography is the field of steganography which hides the secret message in another medium. The secret message is embedded in a host message called cover audio. This cover audio is sent to the receiver who has a key to extract the hidden audio from the cover audio. The cover audio acts as a blanket to hide the message and the key acts as an extra layer of security. Audio steganography takes the advantage of the limitations and functioning of the human auditory system. This paper introduces and explains a way to improve the security by using differential pulse code modulation (DPCM).

A. Devi and K. B. ShivaKumar [3] Point of care testing (POCT) in patients with ischemic heart disease is impelled by the time critical need for quick, specific and accurate results for initiation of therapy instantly. The driving force behind POCT using ECG signals is to provide test immediately and conveniently to cardiac patients. This will intensify the probability of patient, physician and care team receiving the results faster, which facilitate immediate clinical management decisions to be taken. In wireless communication the biomedical data may be susceptible to potential attacks leading to following security challenges. To safeguard the privacy and integrity of biomedical data. To make sure that only authorized people can have the access to secret information. This paper proposes a five level wavelet decomposition based steganography technique applied to ECG signals along with RSA encryption and scrambling matrix based encoding technique to protect confidential information related to patient hidden inside ECG signals. To assess the efficiency of the proposed algorithm on the patient ECG signal, the two distortion measurement metrics like percentage RMSE difference (PRD) and PSNR(peak signal to noise ratio) have been compared with existing algorithm results and energy of watermarked ECG signal is compared with original ECG for Coiflet, Bioorthogonal and symlet wavelets. It is found that the proposed algorithm provides very high security protection for information related to patient and as well as with very less distortion of ECG signal, so that it remains diagnosable even after retrieval of patient related secret information.

M. Rana and F. B. Kunwar [4]: As communication is being done by electronic means in open air generally, security of data is highly desirable. One such technique of doing this is steganography. The requirement of a system that ensures increasing capacity, robustness and security of embedded data there have been so many variants in existing steganography technique. Due to this diversity it needs some technique to optimize the existing traditional substitution technique. The audio file is chosen as cover file due to its practical availability and "Masking Effect".

B. Datta, P. Pal and S. K. Bandyopadhyay [5] In this paper a robust audio steganography method is introduced which involves multiple layers for embedding secret data. In LSB technique generally a single or multiple bits are embedded always in one or some particular bit positions. So it is easy to get that data by knowing those positions. The robustness increases in LSB approach by considering higher LSB layer but it reduces the perceptibility of audio. Here in this proposed work LSB embedding is used in multiple layers and also capacity is increased by embedding two bits at a time. Here always two different pairs 01 and 11 are embedded instead of four, made using two bits at a time at the same time increases robustness more. Without knowing the bitwise operation applied here for extraction it is not also very much easy to get the actual data. After embedding flag setting and bit adjustment is done for maintaining the perceptual transparency of stego audio. Here in this proposed work capacity is also increased by considering 6 bit binary instead of 7 or 8.

IV. PROPOSED SOLUTION

We have proposed a secured File sharing and the message transferring system in which the message communication is done only between the registered users.

The module of the systems are divided into the following parts,

Description:

1. Registration:
-To access the core system, user first need to register themselves by providing required details.
2. Login:
-After registration, user may login into the system.
3. Algorithm Selection:
-Here, user will select the algorithm such as DES (Data Encryption Standard), AES (Advance Encryption Standard) or LSB (Least Significant Bit) for encrypting data into image file.
4. Image Selection/Audio Selection
-Here, User selects an image/audio for sending a secret message. In some case where the encrypted image is sent then the step 5-6 are skipped and a new step of decryption of the image will be introduced.
5. Entering Text:
-Here, User enter/inputs the text that is to be hidden in the image.
6. Setting Password and Encrypting the Data:
-User sets a password and use the encryption technique to encrypt the data.
7. Sharing:
-After hiding the text with the encryption technique, user saves the image a then sends it to the other party i.e. Receiver.

Algorithm for the Image Encryption
The algorithm for the image encryption is as follows:
Step 1: Read Image file to be encrypted
Step 2: Check for the Image Extension and valid then load the image.
Step 3: Load the Key
Step 4: Convert the image file to binary
Step 5: Encrypt the using the key.
Step 6: Store the Encrypted Image on the Hard disk.

Algorithm of Decrypting Image
The algorithm of decrypting the image is as follows:
Step 1: Read Image file to be decrypted
Step 2: Check for the Image Extension and valid then load the image.
Step 3: Load the Key
Step 4: Convert the image file to binary
Step 5: Decrypt the using the key.
Step 6: Store the Decrypted Image on the Hard disk
Produce a secret key to encode and to unscramble the data. The DESCryptoServiceProvider depends on a symmetric encryption calculation. The symmetric encryption requires a key and an introduction vector (IV) to encode the data. To unscramble the data, you should have a similar key and a similar IV. You should likewise utilize a similar encryption calculation. You can produce the keys by utilizing both of the accompanying methods:

- Method 1 You can prompt the user for a password. Then, use the password as the key and the IV.
- Method 2 When you create a new instance of the symmetric cryptographic classes, a new key and IV are automatically created for the session.

Algorithm for Embedding Of Data
The algorithm for embedding of data is as follows:

1. Input the Audio File
2. Input the Text File or Text to be Hidden
3. Input the Key File Used for the Encryption Purpose (Same Key file will be used for Decryption purpose)
4. In the Embedded process first the chunk of wave stream of the audio files are obtained in order to count the number of samples required for embedding the data , if the samples obtained is not sufficient then the error message is generated. Then the source audio stream and destination audio stream are opened (destination audio is the new audio file which get created after the embedding process). Then the message and key are embedded bit by bit with the carrier audio.
5. Finally we can get the audio with hidden data

Algorithm for Extracting Of Data
The algorithm for extracting of data is as follows:

1. Input the Audio File
2. Input the Text File which will store the extracted data.
3. Input the Key File Used for the Decryption Purpose (Same Key file will be used for Encryption purpose)
4. First the carrier wave file is extracted for the provided audio file, the message is extracted from the audio file using the key file which is provided as input and then a new file stream is obtained in order to write the extracted data into the new destination file.
5. Finally this data converted into original secrete data

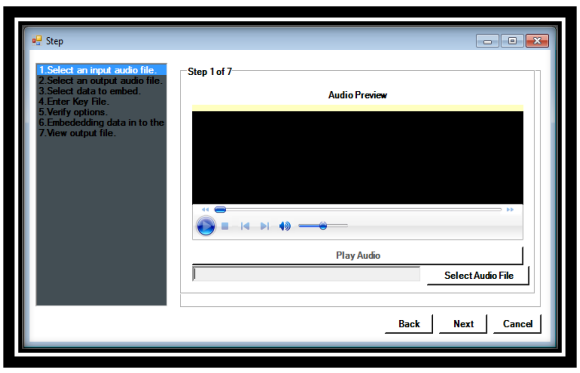

Fig 3. Proposed Implementation

V. CONCLUSION

In this data is embedded with the image and sent over the network where its integrity is verified by the comparison of hash value of the original data or image. The audio stegronography is also implemented, where the audio message can securely carry the text. The proposed work provides secure secret communication among sender and receiver, it ensures that embedded data remains inviolate & recoverable, watermarks the image with excellent visual quality without causing a noticeable loss of quality. It is useful for copyright ownership assertion purposes. The data which is hidden cannot be easily removed and resist common image manipulation techniques.

REFERENCES

[1] H. Liu, J. Liu, R. Hu, X. Yan and S. Wan, "Adaptive Audio Steganography Scheme Based on Wavelet Packet Energy," 2017 ieee 3rd international conference on big data security on cloud (bigdatasecurity), ieee international conference on high performance and smart computing (hpsc), and ieee international conference on intelligent data and security (ids), Beijing, 2017, pp. 26-31.

[2] J. S. Lamba, K. Sachdeva, V. Sinha and N. Singh, "Differential pulse code modulation in audio steganography," 2016 International Conference on Electrical, Electronics, Communication, Computer and Optimization Techniques (ICEECCOT), Mysuru, 2016, pp. 131-135.

[3] A. Devi and 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 (CCEM), Bangalore, 2016, pp. 101-106.

[4] M. Rana and F. B. Kunwar, "A temporal domain audio steganography technique using genetic algorithm," 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, 2016, pp. 3141-3146.

[5] B. Datta, P. Pal and S. K. Bandyopadhyay, "Robust multi layer audio steganography," 2015 Annual IEEE India Conference (INDICON), New Delhi, 2015, pp. 1-6.

[6] M. Tayel, A. Gamal and H. Shawky, "A proposed implementation method of an audio steganography technique," 2016 18th International Conference on Advanced Communication Technology (ICACT), Pyeongchang, 2016, pp. 180-184.

[7] Fabian Monrose, Michael K. Reiter, Qi Li , Susanne Wetzel, "Cryptographic Key Generation from Voice", In Proceedings of the 2001 IEEE Symposium on Security and Privacy, May 2001.

[8] Neha Rani and Jyoti Chaudhary, "Text Steganography Techniques: A Review", International Journal of Engineering Trends and Technology (IJETT) – Volume 4 Issue 7- july 2013

[9] Swati Gupta and Deepti Gupta, "Text - Steganography: Review Study & Comparative Analysis", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 2 (5), 2011

[10] ChintanDhanani and Krunal Panchal, "Steganography using web documents as a carrier: A Survey", International Journal of Engineering Development and Research (IJEDR), ISSN: 2321-9939, 2013

[11] S. Low, N.Maxemchuk, J.Brassil, L. O'Gorman, 1995. "Document marking and identification using both line and word shifting", Proceedings of the 14th Annual Joint Conference of the IEEE Computer and Communications Societies, INFOCOM 95.

[12] M.S.Durairajan1, Dr. R. Saravanan , "Biometrics Based Key Generation using Diffie Hellman Key

Exchange for Enhanced Security Mechanism", International Journal of Chem Tech Research CODEN .

[13] Mohit Sharma,"Secure Message Transfer using ImageSteganography",Imperial Journal of Interdisciplinary Research (IJIR) 2016.

[14] Mrs. Kalavathi.Alla, Dr. R. Siva Ram Prasad, "A Novel hindi Text Steganography using Letter Diacritics and its compound words",2008.

[15] Anderson, R.J. &Petitcolas, F.A.P., "On the limits of steganography", IEEE Journal of selected Areas in Communications, May 1998.