Security for Digital Data using Combination of Audio Steganography and Cryptography

[1]Alisha Sikri,[2]Taruna, [3]Kirti Rana
M.tech Scholar, M.tech Scholar, Assistant Professor
, Department of Computer Science
Gateway Institute of Engineering & Technology Sonepat, Haryana, India
[1]alisha.sikri92@gmail.com,[2]taruna890@gmail.com,[3]rana.kirti11@gmail.com

***Abstract* - Steganography is the art and science of hiding that a communication is taken place. It embeds the secret file (text, audio or image) in other carrier file. Image steganography has widely developed. There are also many algorithm developed for it. Meanwhile, the interest in using audio data as cover object in steganography can be spelled out late emergence than image data. Audio information hiding has attracted more attentions recently. Spread spectrum (SS) technique has developed rapidly in this area due to the advantages of good robustness and immunity to noise attack. The spread-spectrum techniques for watermarking are very popular nowadays. Cryptography plays a major role in the field of network security. There are many encryption techniques available currently to secure the data. Cryptography can be defined as the art or science of altering information or change it to a chaotic state, so that the real information is hard to extract during transfer over any unsecured channel. Latest advancements in technology and new concepts like quantum cryptography have added a complete new dimension to data security. MATLAB R2013a has been used as an implementation platform using signal processing tool box.**

***Index Terms* - Cryptography, Steganography,Watermarking**

I.INTRODUCTION

Before the invention of steganography and cryptography, it was challenging to transfer secure information and, thus, to achieve secure communication environment. Some of the techniques employed in early days are writing with an invisible ink, drawing a standard painting with some small modifications, combining two images to create a new image, shaving the head of the messenger in the form of a message, tattooing the message on the scalp and so on[12].

Normally an application is developed by a person or a small group of people and used by many. Hackers are the people who tend to change the original application by modifying it or use the same application to make profits without giving credit to the owner. It is obvious that hackers are more in number compared to those who create. Hence, protecting an application should have the significant priority. Protection techniques have to be efficient, robust and unique to restrict malicious users. The development of technology has increased the scope of steganography and at the same time decreased its efficiency since the medium is relatively insecure. This lead to the development of the new but related technology called "Watermarking". Some of the applications of watermarking include ownership protection, proof for authentication, air traffic monitoring, medical applications etc [9,17]. Watermarking for audio signal has greater importance because the music industry is one of the leading businesses in the world
.

A.Applications of Watermarking

1. Ownership protection and proof of ownership: In ownership protection application, the watermark embedded contains a unique proof of ownership. The embedded information is robust and secure against attacks and can be demonstrated in a case of dispute of ownership. There can be the situations where some other person modifies the embedded watermark and claims that it is his own. In such cases the actual owner can use the watermark to show the actual proof of ownership [9, 8, 5].
2. Authentication and tampering detection: In this application additional secondary information is embedded in the host signal and can be used to check if the host signal is tampered. This situation is important because it is necessary to know about the tampering caused to the media signal. The tampering is sometime a cause of forging of the watermark which has to be avoided.
3. Finger printing: Additional data embedded by a watermark in the fingerprinting applications are used to trace the originator or recipients of a particular copy of a multimedia file. The usage of an audio file can be recorded by a fingerprinting system. When a file is accessed by a user, a watermark, or called fingerprint in this case, is embedded into the file thus creating a mark on the audio. The usage history can be traced by extracting all the watermarks that were embedded into the file.
4. Broadcast monitoring: Watermarking is used in code identification information for an active broadcast monitoring. No separate broadcast channel is required as the data is embedded in the host signal itself which is one of the main advantages of the technique [5].
5. Copy control and access control: A watermark detector is usually integrated in a recording or playback system, like in the DVD copy control algorithm [10] or during the development of Secure Digital Music Initiative (SDMI. The copy control and access control policy detects the watermark and it enforces the operation of particular hardware or software in the recording set [8].

6. Information carrier: The blind watermarking technique can be used in this sort of applications. These applications can transfer a lot of information and the robustness of the algorithm is traded with the size of content [12].
7. Medical applications: Watermarking can be used to write the unique name of the patient on the X-ray reports or MRI scan reports. This application is important because it is highly advisable to have the patients name entered on reports, and reduces the misplacements of reports which are very important during treatment [5].
8. Airline traffic monitoring: Watermarking is used in air traffic monitoring. The pilot communicates with a ground monitoring system through voice at a particular frequency. However, it can be easily trapped and attacked, and is one of the causes of miss communication. To avoid such problems, the flight number is embedded into the voice communication between the ground operator and the flight pilot. As the flight numbers are unique the tracking of flights will become more secure and easy [1].

B. AUDIO WATERMARKING TECHNIQUES

Features of Human Auditory System (HAS)

Note that audio watermarking is more challenging than an image watermarking technique due to wider dynamic range of the HAS in comparison with **human visual system** (HVS). Human ear can perceive the power range greater than 109: 1 and range frequencies of 103:1 [8]. In addition, human ear can hear the low ambient Gaussian noise in the order of 70dB [8]. However, there are some useful features such as the louder sounds mask the corresponding slow sounds. This feature can be used to embed additional information like a watermark. Further, HAS is insensitive to a constant relative phase shift in a stationary audio signal, and, some spectral distortions are interpreted as natural, perceptually non-annoying ones. Two properties of the HAS dominantly used in watermarking algorithms are frequency (simultaneous) masking and temporal masking [16].
1. Frequency masking: Frequency (simultaneous) masking is a frequency domain phenomenon where low levels signal (the maskee) can be made inaudible (masked) by a simultaneously appearing stronger signal (the masker), if the masker and maskee are close enough to each other in frequency [16]. A masking threshold can be found and is the level below which the audio signal is not audible. Thus, frequency domain is a good region to check for the possible areas that have imperceptibility.
2. Temporal masking: In addition to frequency masking, two phenomena of the HAS in the time domain also play an important role in human auditory perception. Those are pre-masking and post-masking in time [16]. However, considering the scope of analysis in frequency masking over temporal masking, prior is chosen for this thesis. Temporal masking is used in application where the robustness is not of primary concentration.

Requirements of the Efficient Watermark Technique

According to IFPI (**International Federation of the Phonographic Industry**) [4], audio watermarking algorithms should meet certain requirements. The most significant requirements are perceptibility, reliability, capacity, and speed performance [16].
1. Perceptibility: One of the important features of the watermarking technique is that the watermarked signal should not lose the quality of the original signal. The signal to noise ratio (SNR) of the watermarked signal to the original signal should be maintained greater than 20dB [4]. In addition, the technique should make the modified signal not perceivable by human ear.
2. Reliability: Reliability covers the features like the robustness of the signal against the malicious attacks and signal processing techniques. The watermark should be made in a way that they provide high robustness against attacks. In addition, the watermark detection rate should be high under any types of attacks in the situations of proving ownership. Some of the other attacks summarized by **Secure Digital Music Initiative** (SDMI), an online forum for digital music copyright protection, are digital-to-analog and analog-to-digital conversions, noise addition, band-pass filtering, time-scale modification, echo addition, and sample rate conversion [14].
3. Capacity: The efficient watermarking technique should be able to carry more information but should not degrade the quality of the audio signal. It is also important to know if the watermark is completely distributed over the host signal because, it is possible that near the extraction process a part of the signal is only available. Hence, capacity is also a primary concern in the real time situations [4].
4. Speed: Speed of embedding is one of the criteria for efficient watermarking technique. The speed of embedding of watermark is important in real time applications where the embedding is done on continuous signals such as, speech of an official or conversation between airplane pilot and ground control staff. Some of the possible applications where speed is a constraint are audio streaming and airline traffic monitoring. Both embedding and extraction process need to be made as fast as possible with greater efficiency [4].
5. Asymmetry: If for the entire set of cover objects the watermark remains same; then, extracting for one file will cause damage watermark of all the files. Thus, asymmetry is also a noticeable concern. It is recommended to have unique watermarks to different files to help make the technique more useful [4].

WATERMARKING

Watermarking is a technique through which the secure information is carried without degrading the quality of the original signal. The technique consists of two blocks:

(i) Embedding block
(ii) Extraction block

The system has an **embedded key** as in case of a steganography. The key is used to increase security, which does not allow any unauthorized users to manipulate or extract data. The embedded object is known as **watermark**, the watermark embedding medium is termed as the **original signal** or **cover object** and the modified object is termed as **embedded signal or watermarked data [12]**.

The embedding block, shown in Figure 1.1 consists of watermark, original signal (or cover object), and watermarking key as the inputs (creates the embedded signal or watermarked data). Whereas, the inputs for the extraction block is embedded object, key and sometimes watermark as illustrated in Fig 1.2[12].

The watermarking technique that does not use the watermark during extraction process is termed as "**blind watermarking**." blind watermarking is superior over other watermarking involving watermark for extraction as watermarked signal and key are sufficient to find the embedded secret information [5].

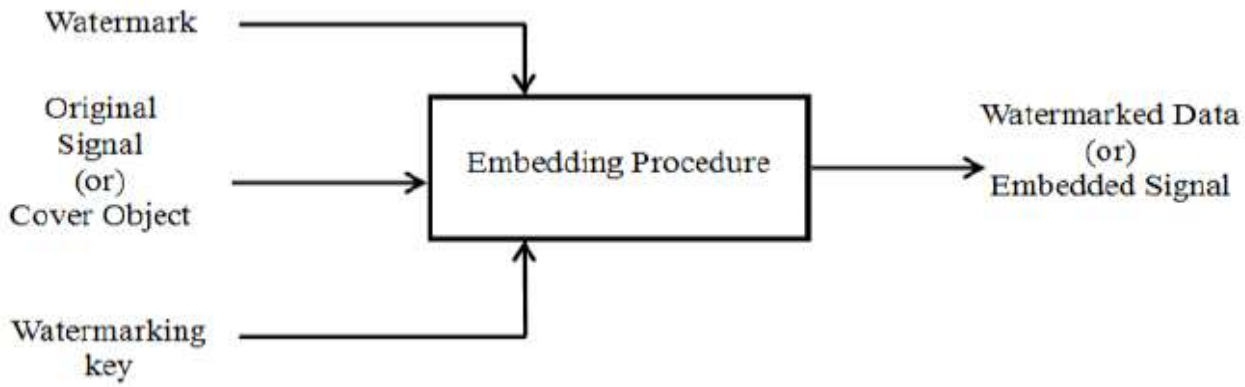

Figure 1.1 Digital watermarking embedding

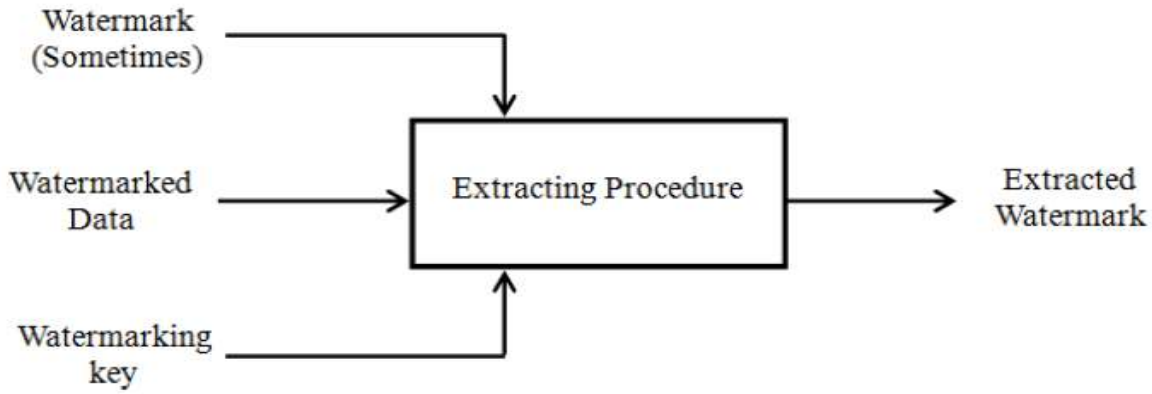

Figure 1.2 Digital watermarking extraction

II. LITERATURE SURVEY

Rashid Ansari et. al.[1] proposed a novel perception-based data hiding technique for digital audio is proposed. It exploits lower sensitivity of human auditory system (HAS) to phase distortion in audio compared with magnitude distortion. Audio is decomposed into subband signals some of which are selected for embedding data with a controlled alteration of phase using suitable all pass digital filters. The proposed scheme is robust to standard data manipulations yielding less than 2% error probability against compression, re-sampling, re-quantization, random chopping and noise addition.

Mark Sterling et. al. [2] describes an application of spread spectrum techniques in audio data hiding for watermarking and steganography. The method is self-synchronizing, cover dependent, and operates in the time domain. The Author use a special class of frequency-hop signal know as a Welch-Costas Array. Welch-Costas Arrays have the properties of range and Doppler resolution. This allows us to recover embedded data with a matched filter.

XUE-MIN RU et. al. [3] present a steganalytic method that can reliably detect messages hidden in WAV files using the steganographic tool Steghide. The key element of the method is mining the correlation between wavelet coefficients in a short-duration (about 20ms) in each subband. This is done by performing a four-level 1-D wavelet decomposition of the audio signals, using a linear predictor for the magnitude of wavelet subband coefficients to extract significant statistics features, and employing support vector machines to detect the existence of hidden messages.

Anand Gupta et. al. [4] presents that Steganography is the science of writing hidden messages in such a way that no one apart from the sender and intended recipient even realizes if there is any hidden message. Most of the research done before in this area is focused on images, audios, and videos but a less amount of work has been done on MS Word documents which are identified with certain shortcomings. One of the major shortcoming in the previous method being large number of degenerations which were produced to embed a message, making it susceptible to active warden attack.

Cairong Li et. al. [5] proposed that Audio steganalysis has attracted more attentions recently. DSSS steganalysis is one of the most challenging research fields. In this paper, a novel algorithm to detect DSSS steganography in audio signal is proposed. Firstly, it takes DWT transform of special segment of audio and takes the detail sub-band coefficients, and then uses GMM to model the coefficients. Secondly, in order to monitor the effect of DSSS hiding, The Author calculate the GMM PDF (possibility density function) as to measure the difference. Thirdly, considering the two variables composed of wavelet coefficients and GMM PDF, the multivariate skewness and kurtosis were taken as features. Lastly, the SVM classifier is utilized for classification.

Zhiping Zhang et. al. [6] designs an audio covert communication system based on spread spectrum (SS) data hiding technology. Considering the characteristics of covert communication, some methods were proposed to solve the key problems in the system. Firstly, the system employed M-array SS coding combining with return-to-zero base band code to embed hiding data. In addition, the sender embedded the base band clock in audio signal for synchronization. Furthermore, Reed Solomon (RS) channel coding was applied in the system for error correction. This system was tested through an audio line and a FM audio broadcast platform as communication channels. Experiment results showed that the data error rates were 0.024% via audio line and 0.288% via FM audio when the hiding data rate was 7.8 bytes/s.

Kaliappan Gopalan et. Al. [7] describes that Audio steganography using bit modification of time domain audio samples is a simple technique for multimedia data embedding with potential for large payload. Depending on the index of the bit used to modify the samples in accordance with the data to be hidden, the resulting stego audio signal may become perceptible and/or susceptible to incorrect retrieval of the hidden data. This paper presents some results of the tradeoff between the conflicting requirements of data robustness, payload and imperceptibility. Experimental results on both clean and noisy host audio signals indicate that while the payload can be as high as over 3000 bits/s – much higher rate than common audio data embedding techniques – noticeability of embedding is decreased and noise tolerance increased by using higher bit indices than the traditional least significant bit.

III. PROBLEM FORMULATION

It can be concluded from the above literature survey that existing methods such as DES, 3DES, RC2, RC4, RC6, RSA and BLOWFISH are much efficient methods for audio encryption. These techniques are applied on audio data, for securely transmitting audio data over the network. Total Data Encryption Standard (DES), total Advanced Encryption Standard (AES) and selective AES encryption techniques are applied on the quantized audio data. A comparison between these encryption techniques is discussed by calculating the time consumption as well as SNR values. Experimental results demonstrate that the time consumption for selective AES encryption on MP3 compression is less than total AES and DES encryption techniques on MP3 compression. So, the selective encryption technique is better than total DES and AES encryption techniques as it takes less time with degradation of signal that is inaudible to the unauthorized users, That the selective AES encryption technique is better than the other two encryption techniques. RSA is asymmetric encryption technique. RSA technique is used for the encryption and decryption on the lower frequency bands because all the frequency regions do not participate equally in the communication. After applying the encryption on different frequency bands, it is observed that, the encryption on the lower frequency band is more effective than the higher one. The technique is applied on phase values. Having all these above features, existing methods still have scope of improvements. There are some common problems in existing methods, which have been formulated to propose new method for audio encryption. These problems are as follows:

1. Existing methods do not combat with higher frequency band audio.
2. Existing methods need very large time encryption and decryption.
3. Encrypted audio file is not much secure from existing methods as it is very easy for intruder to break the algorithm.
4. Existing methods requires only single key for encryption and decryption which reduces the security level.

IV. PROPOSED WORK

Spread Spectrum Technique

These techniques are derived from the concepts used in spread spectrum communication [17]. The basic approach is that a narrow band signal is transmitted over the large bandwidth signal which makes them undetectable as the energy of the signal is overlapped. In the similar way the watermark is spread over multiple frequency bins so that the energy in any one bin is very small and certainly undetectable. In spread spectrum technique, the original signal is first transformed to another domain using domain transformation techniques [17]. The embedding technique can use any type of approach for example quantization. Zhou *et al.* proposed an algorithm embedding watermark in 0th DCT coefficient and 4th DCT coefficients which are obtained by applying DCT on the original signal.

Embedded signal will undergo some attacks, thus, noise is added to the signal. To extract the watermark the attacked signal is fed through extraction procedure. The extraction process involves taking the attacked signal and applying DCT, framing the obtained components. And they obtained frames are used to obtain the watermark. Care is taken to replicate the procedure used for embedding process.In the context of audio steganography, the basic spread spectrum (SS) method attempts to spread secret information across the audio signal's frequency spectrum as much as possible. This is analogous to a system using an implementation of the LSB coding that randomly spreads the message bits over the entire sound file. However, unlike LSB coding, the SS method spreads the

secret message over the sound file's frequency spectrum, using a code that is independent of the actual signal. As a result, the final signal occupies a bandwidth in excess of what is actually required for transmission.

Two versions of SS can be used in audio steganography: the direct-sequence and frequency-hopping schemes. In direct-sequence SS, the secret message is spread out by a constant called the chip rate and then modulated with a pseudorandom signal. It is then interleaved with the cover-signal. In frequency-hopping SS, the audio file's frequency spectrum is altered so that it hops rapidly between frequencies. The math theory behind SS is quite complicated and goes beyond the scope of this project. However, Katzenbeisser and Petitcolas write about a generic steganography system that uses direct-sequence SS in Information Hiding Techniques for Steganography and Digital Watermarking. The following procedural diagram illustrates the design of that system when applied to our specific topic of audio steganography.

V. RESULTS

The proposed method would not only provide highly secure audio but also efficient for audio file having higher frequency band. MATLAB R2013a has been used as an implementation platform using signal processing tool box. Six audio files 'audio 0.wav', 'audio 1.wav', 'audio 2.wav', 'audio 3.wav', 'audio 4.wav' and 'audio 5.wav'. The size of files are 32KB, 151KB,404KB,497KB, 647KB and 1360KB respectively. Audio is first encrypted using advanced random permutation method and then decrypted using reverse process. Figure 1 is the snapshot of original input audio waveform and encrypted audio waveform for 'audio 0.wav'. It is clearly seen from figure 1 that original signal is converted into a high frequency noise signal. It would be impossible for intruder to reconvert encrypted signal into original signal. Figure 2 is the snapshot of waveform of encrypted audio and decrypted audio. Figure 3 is the snapshot of waveform of original audio and decrypted audio. Both waveforms are looking almost similar. To prove these analytical results we have given some output parameters i.e. MSE, PSNR, normalized correlation value, entropy of original signal, entropy of encrypted signal and entropy of decrypted signal. The values of these signal is given in table 1.

Table 1 comparison of different parameters for different file

File name	MSE	PSNR	NC	Entropy of original audio file	Entropy of encrypted audio file	Entropy of decrypted audio file
Audio 0	5.2445e-11	102.7351	1.0000	2.0392	4.3394	2.0392
Audio 1	5.3218e-13	113.4271	1.0000	2.6555	4.3174	2.6555
Audio 2	2.7508e-11	105.5349	1.0000	3.6904	4.2555	3.6904
Audio 3	4.6920e-10	93.2186	1.0000	3.9514	4.1553	3.9530
Audio 4	2.9723e-10	92.6796	1.0000	3.0281	3.9390	3.0281
Audio 5	1.0054e-10	98.3980	1.0000	4.2722	4.2882	4.2722

VI. CONCLUSION

It can be concluded from this paper that there are many encryption techniques available currently to secure the data. Latest advancements in technology and new concepts like quantum cryptography have added a complete new dimension to data security. The strength of this cryptographic technique comes from the fact that no one can read (or steal) the information without altering its content. This alteration alerts the communicators about the possibility of a hacker and thus promising a highly secure data transfer. In this research work, we have discussed various cryptographic algorithms (encryption standards), encryption techniques for audio data and some of encryption standards that have been used for encryption on audio data which are used for Network security purpose. With the help of these algorithms, one can generate its own algorithm by making modifications into existing algorithms to make audio data more secure. A new encryption algorithm for audio files is propose and presented in this research work. This new algorithm performs encryption using a advance random procedure. Statistical analysis using MSE, PSNR, correlation, and entropy showed that the algorithm is not vulnerable to statistical attacks. In addition, the huge number of possible keys makes a brute-force attack on the algorithm impossible. Our experiments show that the effectiveness of the proposal. It is a fast and simple solution, yet it can provide sufficient security for audio files. In future, the proposed method for audio cryptography can be combined with audio steganography. The combined method will not only provide security to the audio but also to the image hided in audio.

VII. REFERENCES

[1]. Rashid Ansari, Hafiz Malik, Ashfaq Khokhar," Data-Hiding in Audio Using Frequency-Selective Phase Alteration**".**0-7803-8484-9/04/$20.00, 4004 IEEE, V-389, ICASSP 2004.

[2]. Mark Sterling, Edward L. Titlebaum, Xiaoxiao Dong, Mark F. Bocko, "An Adaptive Spread Spectrum Data Hiding Technique For Digital Audio". 0-7803-8874-7/05/$20.00 ©2005 IEEE, V – 685, ICASSP 2005.
[3]. Xue-Min RU , Hong-Juan Zhang , Xiao Huang, "Steganalysis of Audio: Attacking The Steghide". Proceedings of the Fourth International Conference on Machine Learning and Cybernetics, Guangzhou, 18-21 August 2005.
[4]. Anand Gupta, Deepak Kumar Barr, Deepali Sharma , "Mitigating the Degenerations in Microsoft Word Documents : An Improved Steganographic Method". 978-1-4244-3314-809$25.00 2009 IEEE.
[5]. Cairong Li, Wei Zeng, Haojun Ai, Ruimin Hu , "Steganalysis of Spread Spectrum Hiding Based on DWT and GMM". 2009 International Conference on Networks Security, Wireless Communications and Trusted Computing.
[6]. Zhiping Zhang Xihong Wu ," An Audio Covert Communication System for Anolog Channels". 2010 International Conference on Electrical and Control Engineering".
[7]. Kaliappan Gopalan, "Audio Steganography using Bit Modification – A Tradeoff on Perceptibility and Data Robustness for Large Payload Audio Embedding". 978-1-4244-7116-4/10/$26.00 ©2010 IEEE.
[8]. Dmitriy E. Skopin, Ibrahim M. M. El-Emary, Rashad J. Rasras, Ruba S. Diab, "Advanced Algorithms in Audio Steganography for Hiding Human Speech Signal". 978-1-4244-5848-6/10/$26.00 ©2010 IEEE.
[9]. Marcus Nutzinger, Christian Fabian, Marion Marschalek, "Secure Hybrid Spread Spectrum System for Steganography in Auditive Media". 2010 sixth International conference on Intelligent Information Hiding and Multimedia Signal Processing.
[10].Rizky M. Nugraha, "Implementation of Direct Sequence Spread Spectrum Steganography on Audio Data". 2011 International Conference on Electrical Engineering and Informatics 17-19 July 2011, Bandung, Indonesia.
[11]. Sarosh K. Dastoor , "Comparative Analysis of Steganographic Algorithms intacting the information in the Speech Signal for enhancing the Message Security in next Generation Mobile devices" . 978-1-4673-0126-8/11/$26.00_c 2011 IEEE.
[12]. Bo Liu, Erci Xu, Jin Wang, Ziling Wei, Liyang Xu, Baokang Zhao, Jinshu Su , "Thwarting Audio Steganography Attacks in Cloud Storage Systems". 2011 International Conference on Cloud and Service Computing.
[13]. Muhammad Asad, Junaid Gilani, Adnan Khalid, "An Enhanced Least Significant Bit Modification Technique for Audio Steganography". 978-1-61284-941-6/111$26.00 ©2011 IEEE.
[14]. Saswati Ghosh, Debashis De, Debdatta Kandar, "A Double Layered Additive Space Sequenced Audio Steganography Technique for Mobile Network". 2012 International Conference on Radar, Communication and Computing (ICRCC),SKP Engineering College, Tiruvannamalai, TN., India. 21 - 22 December, 2012. pp.29-33.
[15]. Pooja P. Balgurgi, Prof. Sonal K. Jagtap, "Intelligent Processing : An Approach of Audio Steganography".2012 International Conference on Communication, Information & Computing Technology (ICCICT), Oct. 19-20, Mumbai, India.
[16]. Ming Li,, Michel K. Kulhandjian, Dimitris A. Pados, *E*, Stella N. Batalama and Michael J. Medley, "Extracting Spread-Spectrum Hidden Data From Digital Media", IEEE Transactions On Information Forensics And Security, VOL. 8, NO. 7, JULY 2013.
[17]. Parul Shah, Pranali Choudhari and Suresh Sivaraman, "Adaptive Wavelet Packet Based Audio Steganography using Data History". 2008 IEEE Region 10 Colloquium and the Third ICIIS, Kharagpur, INDIA December 8-10. 286.


IJEDR