Journal Homepage: - www.journalijar.com
INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)
Article DOI: 10.21474/IJAR01/1737
DOI URL: http://dx.doi.org/10.21474/IJAR01/1737

RESEARCH ARTICLE

Implementation of Audio Watermarking algorithm based on embedding strategy in high frequency sub-band with binary sequence using DWT-FFT

Shelke Sheetal V.[1], Mangal Patil[2] and J.S.Chitode[3]
1. P.G. student (Electronics Engg.) from Bharati Vidyapeeth Deemed University College of Engineering, Pune.
2. Assistant Professor (Electronics Engg.), Bharati Vidyapeeth Deemed University College of Engineering, Pune.
3. Professor, Bharati Vidyapeeth Deemed University College of Engineering, Pune.

Manuscript Info

Manuscript History

Received: 12 July 2016
Final Accepted: 22 August 2016
Published: September 2016

Key words:-
Audio watermarking, Discrete Wavelet Transforms, Fast Fourier Transform.

Abstract

This paper deals with the new method based on Discrete Wavelet Transforms (DWT) and Fast Fourier Transform (FFT) to secure audio communication. The separation of HF band and LF band of original audio signal is obtained using DWT. Additionally FFT is applied to HF subband and the digital watermark is embedded into magnitude spectrum of FFT. The experimental evaluation of the proposed algorithm is done using Signal to Noise Ratio (SNR), Bit Error Rate (BER) and Normalized Correlation (NC) which involves robustness and imperceptibility. This method offers promising result against different attacks such as volume scaling, resampling, requantization, low pass filtering, echo addition, additive white gaussian noise (AWGN), etc.

Introduction:-

Now a day multimedia contents are available in digital form. A major problem faced while accessing the data is unauthorized copying. To protect original data from unauthorized copying many techniques are available [1]. Digital watermarking is one of technique to protect the digital data. Digital watermarking is used to embed the data into source content which can be text, audio, image or video. But audio watermarking is a challenge for content authentication and protection [2].
The proposed paper is implemented using DWT-FFT in which a watermark is used to hide data which prevents unauthorized copying.
The algorithm consists of following component:
1. The watermark
2. The watermark embedder
3. The watermark extraction

In first step, by using secrete key watermark length can be decided. The PN sequence is generated which has a number of bits same as the watermark length [3]. The generated PN sequence is inserted into the least significant bit (LSB) of original audio signal [4]. By applying secrete key in extraction procedure, original PN sequence is obtained which is known as watermark.
The remaining paper is organized as follows. Section II gives the basic idea about watermarking scheme. The embedding and extraction method are demonstrated in section III. Performance evaluation is described in section IV followed by conclusion of the work.

Corresponding Author:- Shelke Sheetal V
Address:- M-Tech.(Electronics Engg.) from Bharati Vidyapeeth Deemed University College of Engineering, Pune.

Basics of Watermarking Scheme:-

The basic idea of watermarking is to embed a watermark signal into the original audio signal. The watermark can be recovered from original signal later on by using watermark key [5]. If more watermarked data are available for recovery, then it is more robust [6]. Watermark systems use one or more secure keys to ensure security against detection watermark. The embedding process of watermarking scheme is shown in Figure 1.

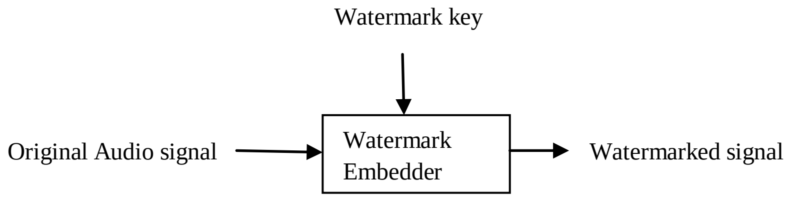

Figure 1: Watermark Embedding Process

The input to this method is the watermark, the original audio signal, and a watermark key. The host audio signal may be uncompressed or compressed depending on application. The watermark can be of any nature, such as a number, a text, an image or an audio signal [7]. The watermark key is used to protect the watermark. The watermarking techniques are usually referred to as secret watermarking techniques.

The extraction process of watermarking is depicted in Figure 2. In which the watermark signal, the watermark key, and the original watermark are used as inputs for the system [8]. The original watermark is retrieved by using secrete key.

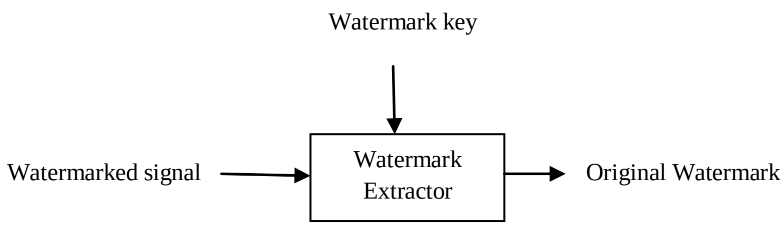

Figure 2: Watermark Extraction Process

The proposed scheme:-

In this section, we present watermark embedding and retrieval process in detail. Two transforms namely DWT and FFT are employed [9]. Watermarking scheme can be divided into two main categories: The spatial domain and transform domain. Spatial domain has low frequency hiding capacity. Watermark is embedded in spatial domain. It is a direct method which has less computational cost, high capacity and more perceptual quality. There are some advantages of spatial domain but, it is less suitable for authentication application. In the transform domain desired watermark gets embedded into frequency coefficients [10]. This domain has less perceptual quality but it is more robust so it is widely used in copyright protection.

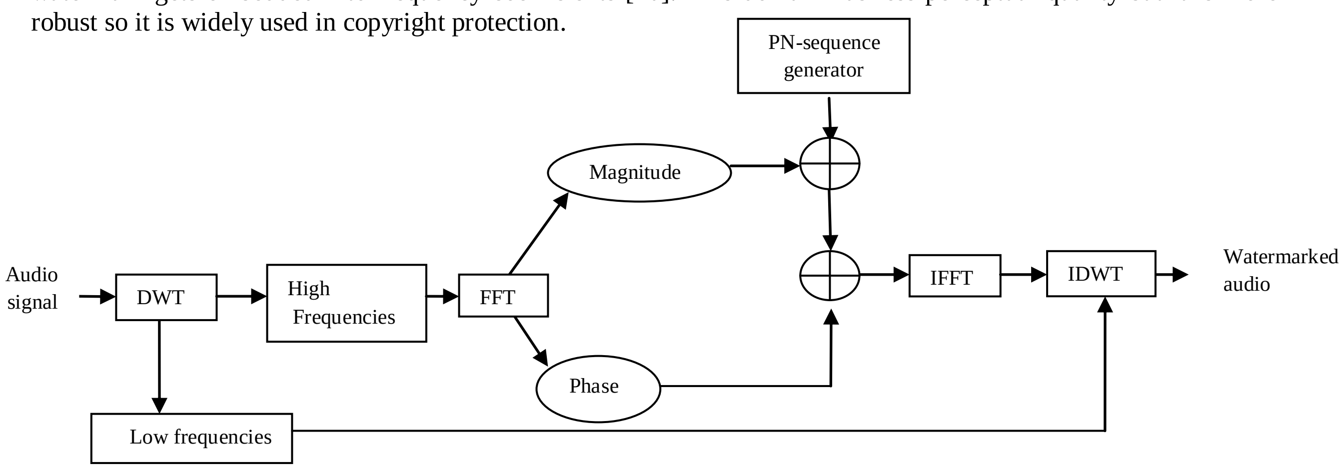

Figure 3: Block diagram showing the general steps to embed the PN sequence into an audio signal

A. Watermark Embedding Process:-

Figure 3 shows the steps performed to embed watermark in audio signal [11]. The embedding process is described in following steps:

1. Separate out the high frequency subband and low frequency subband from original signal by using DWT (Discrete Wavelet Transforms).
2. The High frequency subband is now segmented into frames.
3. Apply FFT (Fast Fourier Transform) to the each frame.
4. Calculate the magnitude and phase spectrum of each frame using Fast Fourier Transform (FFT).
5. Find LSB of each frame from magnitude spectrum.
6. Embed watermark i.e. PN sequence into LSB of each frame which ensures that watermark is located into LSB of each frame.
7. Take an inverse FFT of the complex spectrum to calculate the watermarked frame.
8. Apply the inverse DWT.
9. Add the low frequency subband to received signal.
10. Finally concatenate all watermarked frames to obtain the watermarked audio signal.

B. Watermark Extraction Process:-

In watermark extraction process, the detection process is described in following steps:

1. Take watermarked audio signal as input.
2. Give the secret key.
3. Perform DWT to watermarked audio signal to obtain high frequency subband.
4. Apply Fast Fourier Transform to HF subband.
5. Obtain LSB of each frame from the magnitude spectrum having same frequency in selected range.
6. Extract watermark i.e. PN sequence by using secret key.

Performance evaluation:-

It is almost impossible to achieve robustness against attacks so, as a practical point of view host file will successfully retrieve once the attack is applied [12]. The proposed watermarking algorithm is evaluated using two measures, namely subjective evaluation and objective evaluation.

A. Subjective Evaluation:-

Table 1 shows Mean Opinion Score which is considered as subjective evaluation measure [13]. The results for MOS between host audio and watermarked audio for the proposed scheme are shown in Table 2. This subjective evaluation is very time consuming because it is directly based on human listening tests [14]. The result of this subjective evaluation differs from person to person. To obtain more accurate results, objective evaluation is preferred [15]. The obtained MOS values are averaged considering 10 listeners and tabulated in Table 2.

Table 1: Mean Opinion Scale

Grade	**Description**	**Quality**
5	Imperceptible	Excellent
4	Perceptible	Good
3	Slightly annoying	Fair
2	Annoying	Poor
1	Very Annoying	Bad

Table 2: Experimented Values of Subjective Measures

Audio Sample	**Average MOS**
Classical	4.7
Pop	4.8
Flute	4.9
Rock	4.8
Speech	4.7
Jazz	4.7
Instrumental	4.8

B. Objective Evaluation:-

To evaluate the performance of the proposed scheme, objective metrics such as payload and BER are used. The BER and payload are described as follows [16].

B.1. Bit Error rate (BER):-

BER is used to evaluate the watermark detection accuracy after signal processing operation.

$$\text{BER (W, W')} = \frac{\sum_{i=1}^{M}\sum_{j=1}^{M} W(i,j) \oplus W'(i,j)}{M \times M} \quad (1)$$

W denotes original watermark and W' denotes extracted watermark.

$\oplus$ Denotes exclusive OR (XOR) operator.

B.2 Payload:-

The data payload refers to the number of bits that can be embedded into the audio signal within a unit of time and is measured in the unit of bps (bit per second) [17]. Suppose the length of host audio signal is L seconds, and the watermarked data is of size M bits. Then, the data payload is defined as follows:

$$\text{Data Payload} = \frac{Watermarked\ \ data}{Length\ of\ host\ audio}\ \text{bps.} \quad (2)$$

Results and discussion:-

For the experimental observations, we use .wav classical, pop, jazz, rock, flute, speech and instrumental audio samples (. sec). The watermark is embedded in the left and right channels. The length of PN sequence is decided by the secrete key. The digital watermark is generated using PN sequence generator which is given as follows: 1000001000011000. Figure 4 shows the results of payload v/s audio samples. From figure it is observed that 60.8 bps payload is obtained for flute samples while 34.8 bps is obtained for classical samples.

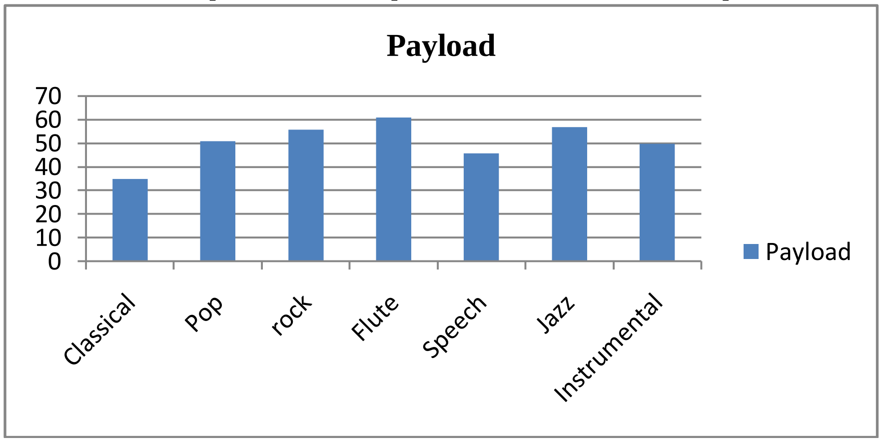

Figure 4. Payload for different audio files

The bit error rate for various types of audio samples is calculated and compared against various attacks such as additive noise, volume scaling, low pass filtering, re-sampling, re-quantization, echo addition and time stretching [18]. It is analyzed from the Figure 5, Figure 6 and Figure 7 that, proposed method provides minimum BER values for pop samples against various attacks, except time stretching attack. The evaluated results shows that time stretching attack provide maximum BER values for all types of audio.

The applied attacks are represented as follows:

1. A1, A2, A3 and A4: volume scaling with scaling factor 0.8, 0.9, 1.1 and 1.4 respectively.
2. A5: Additive Noise.
3. A6: Low Pass Filtering.
4. A7: High Pass Filtering.
5. A8: Resampling.
6. A9, A10 and A11: Requantization with 8 bit, 16 bit and 32bit respectively.
7. A12: Time Stretching.

8. A13: Echo Addition.
9. A14: White Gaussian Noise.
10. A15 and A16: MP3 compression with 64 kbps and 128 kbps respectively.

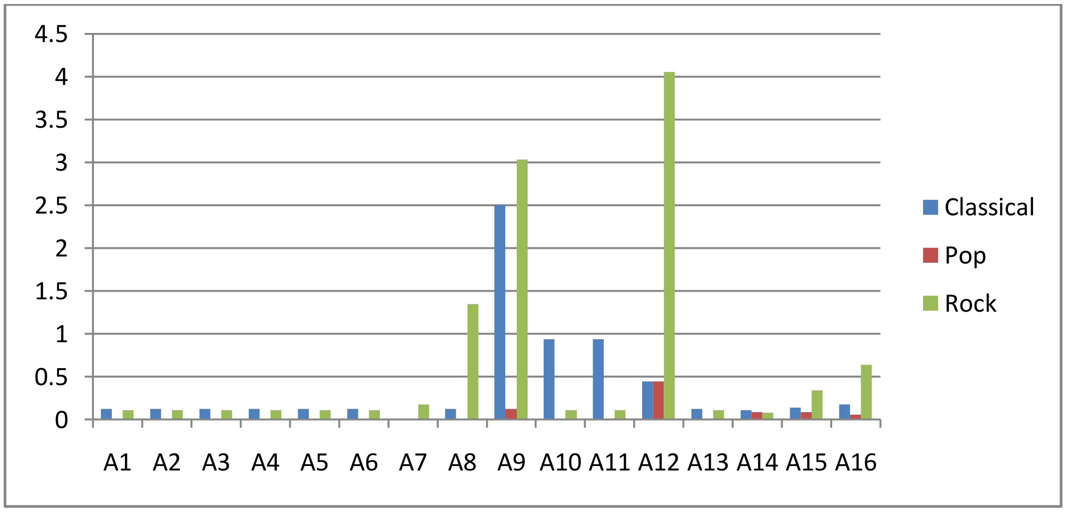

Figure 6: BER results for classical, pop and rock

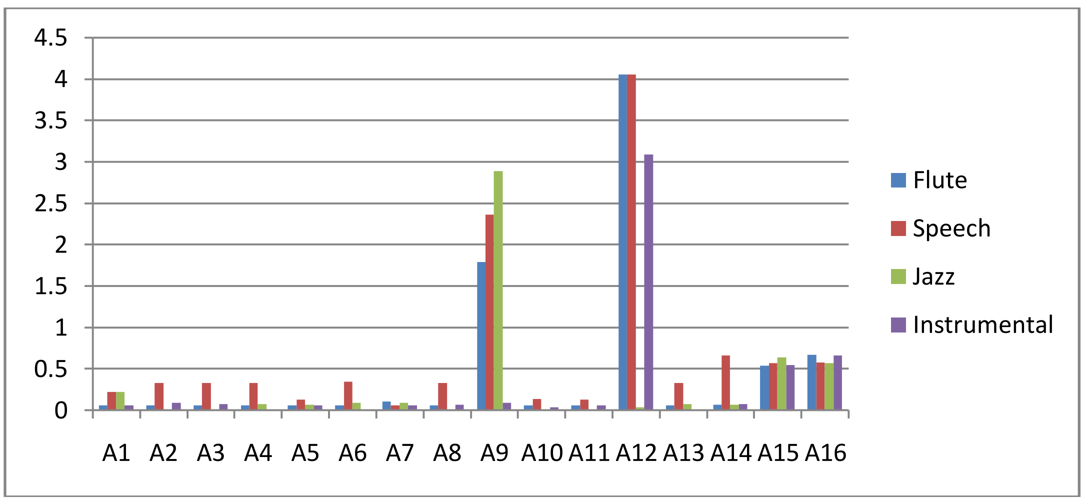

Figure 7. BER results for flute, speech, Jazz and instrumental

Original watermark and extracted watermark are shown in following tables. Different type of audio files such as classical, flute, rock, pop, speech, jazz and instrumental are played with various attacks. PN sequence is used as watermark which is hidden into the audio files in the embedding procedure. Watermark extraction has done by using watermark extraction procedure [19].

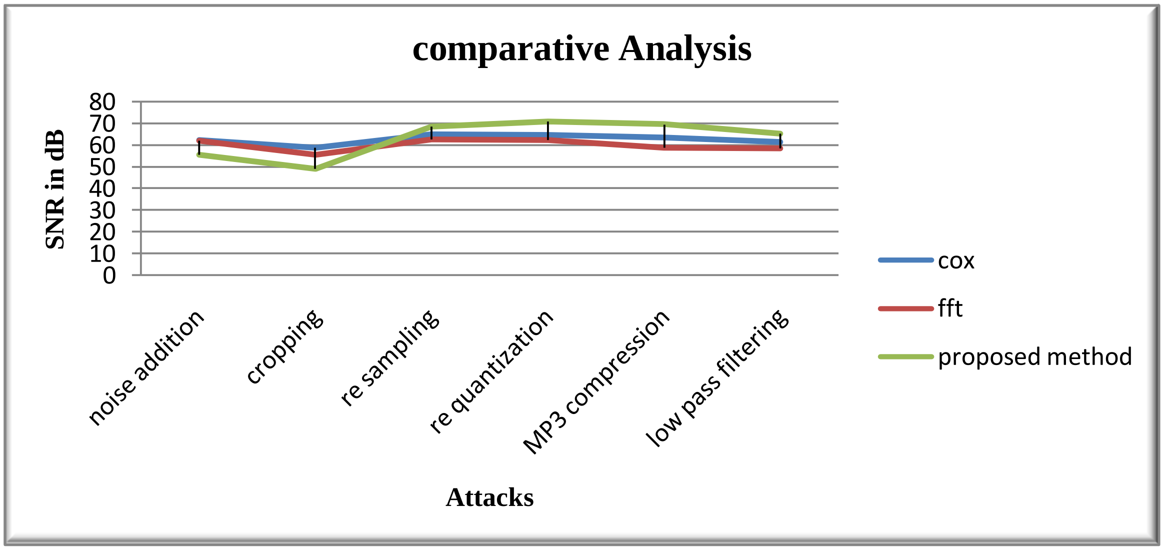

Figure 8. Comparative Analysis

Figure 8 shows the comparative analysis made with earlier methods considered SNR as a performance metrics. The proposed method provides about 55 dB SNR for noise addition attack which is less than other two methods. Whereas the proposed method provides better SNR results as compared to other two methods for different attacks such as re-sampling, re-quantization, MP3 compression and low pass filtering.

Conclusion:-

A new facet in robust audio watermarking is proposed and analyzed in this paper using DWT-FFT. Without disturbing quality of audio signal, good authenticity is achieved. Robustness of this technique is evaluated against various attacks such as echo addition, time stretching, etc and the results indicate that this technique provides better results than other existing methods. The proposed algorithm use DWT and FFT for audio watermarking process. We proved by simulation result that this algorithm is robust against different attacks such as volume scaling, requantization, resampling, low pass filter. Evaluated results shows that proposed method provides improved SNR [More than 20dB] which is standardized by International Federation of Phonographic Industry [IFPI].

References:-

1. Siwar Rekik, Driss Guerchi, Sid-Ahmed Selouani and Habib Hamam, “Speech steganography using wavelet and Fourier Transforms”, EURASIP Journal on Audio, Speech and music processing 2012.
2. B.Chen and G.W.Wornell, “Quantization index modulation: A class of provably good methods for digital watermarking and information embedding,” IEEE Trans. Inform. Theory, vol. 47 (4), pp. 1423–1443, 2001.
3. ZhengLiuandAkiraInoue, “Audio Watermarking Techniques Using Sinusoidal Patterns Based on Pseudorandom Sequence”, IEEE Transactions On Circuits And Systems For Video Technology,Vol.13,NO.8,pp.801-812,2003.
4. N.Cvejic and T.Seppänen, “Increasing robustness of LSB audio steganography by reduced distortion LSB coding,” Journal of University Computer Science, vol. 11(1), pp. 56-65, 2005.
5. T.Cedric, R.Adi, and I.Mcloughlin, “Data concealment in audio using a non- linear frequency distribution of PRBS coded data and frequency-domain LSB insertion,” IEEE Region 10 International Conference on Electrical and Electronic Technology, Kuala Lumpur, Malaysia, pp. 275-278, September 2000.
6. P.K.Dhar, M.L.Khan and J.M.Kim, “A New Audio Watermarking System using Discrete Fourier Transform for Copyright Protection,” International Journal of Computer Science and Network Security, vol.10 (6), June 2010.
7. Pranab Kumar Dhar, Jong-Myon Kim, “Digital Watermarking Scheme Based on Fast Fourier Transformation for Audio Copyright Protection” International Journal of Security and Its Applications Vol. 5 No. 2, April, 2011.
8. K.Fitz and L.Haken, “On the Use of Time-Frequency Reassignment in Additive Sound Modeling,” Journal of the AES, vol. 50, no. 11, pp. 879-893, Nov. 2002.

9. Ali Al-Haj, Ahmad Mohammad and Lama Bata, “DWT–Based Audio Watermarking”, the International Arab Journal of Information Technology, Vol. 8, No. 3, July 2011.
10. Y.Yoshitomi, T.Asada, Y.Kinugawa and M.Tabuse, "An Authentication Method for Digital Audio Using a Discrete Wavelet Transform," Journal of Information Security, Vol. 2 No. 2, pp. 59-68. doi: 10.4236/jis.2011.22006, 2011.
11. Harleen Kaur, Usvir Kaur, “Blind Audio Watermarking schemes: A Literature Review”, IRACST – Engineering Science and Technology: An International Journal (ESTIJ), ISSN: 2250-3498, Vol.3, No.2, April 2013.
12. J.Cooley and J. Tukey, “An algorithm for the machine calculation of the complex Fourier series,” Math. Comput., vol. 19, pp. 297-301, 1965.
13. B.P.Bogert, M.J.R.Healy and J.W.Tukey, “The Quefrency Alanysis of Time Series for Echoes: Cestrum, Pseudo-Auto covariance, Cross-cestrum and Shape Cracking,” in Proceedings of the Symposium on Time Series Analysis, by M. Rosenblatt, pp. 209-243, Wile N.Y. 1963.
14. J.Cooley and J.Tukey, “An algorithm for the machine calculation of the complex Fourier series,” Math. Comput., vol. 19, pp. 297-301, 1965.
15. S.Murata, Y.Yoshitomi and H. Ishii, "Audio Watermarking Using Wavelet Transform and Genetic Algorithm for Realizing High Tolerance to MP3 Compression," Journal of Information Security, Vol. 2 No. 3, pp. 99-112. doi: 10.4236/jis.2011.23010, 2011.
16. Komal Shedge, Mangal Patil, J.S.Chitode ,”A new facet in Robust Audio Watermarking in DWT-SVD Domain”, International Journal Of Engineering Research & Technology(IJERT),ISSN:2278-0181,Vol-3 Issue 5,May-2014.
17. Wei Li, Xiangyang Xue, and Peizhong Lu, “Localized Audio Watermarking Technique Robust Against Time-Scale Modification” IEEE transactions on multimedia, vol. 8, no. 1, February 2006.
18. I.J.Cox, J.Kilian, and T.Leighton, “T. Shammoon, Secure Spread Spectrum Watermarking for Multimedia,” IEEE Trans. Image Process, vol. 6(12), pp. 1673-1687, 1997.
19. P.Bassia and I.Pitas, “Robust audio watermarking in the time domain”, IEEE transactions onMultimedia,Vol.3,Issue:2,pp.232–241,2001.