An effective audio watermarking approach with high data embedding

Hardeep Singh Saini, Dinesh Arora, Manisha Verma

Abstract**—*The watermarking has gained a large popularity among the research work that various authors are working in this direction to improve its performance and to enhance the security of the data. After having review to the traditional work done on audio watermarking, certain limitations related to the hidden image file were found in it. Thus, in this work, the author presents a novel audio watermarking technique. In this work the cover file is an audio file and the image are used to hide behind the signals of the audio. To enhance the security level of the image, the Run-length encoding (RLE) compression mechanism is applied to the image and signals before hiding the image. The RLE is preferred because it is a lossless data compression and encryption mechanism. It ensures the data security and considers the storage management as another major aspect. After applying RLE, the Least Significant Bit (LSB) mechanism is applied to hide the encrypted image behind the digital signals. After implementation, the performance of proposed work is evaluated in the terms of PSNR, BER, and MSE. The obtained results prove that the proposed work outperforms the traditional work.***

Keywords**—*Pseudo Noise, Least Significant Bit (LSB), Watermarking, Run-length encoding (RLE).***

I. INTRODUCTION

In an audio signal an audio watermark is embedded that is a unique electronic identifier and utilized to recognize ownership of the copyright [1]. It is identical to a watermark on a photograph. A procedure in which data is embedded into a signal such as picture, video or audio in a manner that is hard to eliminate is known as Watermarking [2]. After copying the signal, likewise, the data is carried in the copy. To enable copyright protection and ownership verification the watermarking has become gradually more significant [3].

The Spread Spectrum Audio Watermarking (SSW) is majorly secure mechanism of audio watermarking. On a huge bandwidth in SSW a narrow band signal is transferred in order that the signal energy represented in any signal frequency is unnoticeable. Consequently, the watermark is spread on several frequency bands in order that the energy in one band is unnoticeable. A fascinating characteristic of this watermarking procedure is that obliterating it requires noise of high amplitude to be added to all frequency bands. SSW is a powerful watermarking strategy because, to dispose of it, the attack must influence all conceivable frequency bands with adjustments of significant strength [4, 11]. In the information the visible defects are generated by this. Through utilizing a Pseudo Noise (PN) Sequence, the Spreading spectrum is accomplished. In the traditional SSW mechanisms, the receiver should know the PN sequence utilized at the transmitter and the position of the watermark in the watermarked signal for investigating hidden data. This is a high security characteristic, since any unapproved client who does not approach this data can't identify any hidden data. For discovery of hidden data from SSW the investigation of the PN sequence is the major factor. Through applying heuristic mechanisms like evolutionary paradigms, the PN sequence investigation is feasible, the huge computational expense of this operation prepares it unreasonable [5, 12]. In the utilization of evolutionary paradigms as an optimization tool because of the fitness function evaluation in which mostly the computational complexity is included which might be too hard to describe or be computationally very costly. The utilization of fitness granulation as an emerging fitness approximation mechanism is the current projected mechanism in rapidly recovering the PN sequence [6]. The costly fitness evaluation step is replaced with an approximate model through utilizing the fitness granulation mechanism known as Adaptive Fuzzy Fitness Granulation that is also named as AFFG. To extort the hidden information, the evolutionary paradigms are utilized, and the entire procedure is known as Evolutionary Hidden Information Detection, where the fitness approximation mechanisms are utilized as a tool to accelerate the procedure or not.

It is feasible to embed extra data in an audio track by using an audio watermarking mechanism. An audio book or a commercial is adapted to some extent in a defined way to attain this, the audio signal of a music recording [7, 14]. This adaptation is very minor, so the human ear can’t distinguish an audio dissimilarity. Sound watermarking innovation in this way manages a chance to create duplicates of a recording which are seen by listeners as indistinguishable to the real one however which may vary from each other based on the inserted data.

The software only which represents a perspective of the kind of implanting and inserting parameters is equipped for removing such extra information that were installed earlier. Without such programming or if wrong implanting parameters were chosen it is impossible to expect to get to these extra information [8]. This evades unapproved extraction of installed data and makes the method entirely flexible.

The Music Trace is used this feature in a targeted way. A unique set of embedding parameters are acquired by each Music Trace consumer. Therefore, only that consumer can extort the data that is embedded by him. It is not feasible to extort or access the embedded data of someone else.

Revised Manuscript Received on December 22, 2018.

Hardeep Singh Saini, Indo Global College of Engineering, Abhipur, Mohali-140109, India

Dinesh Arora, Chandigarh Engineering College, Landran, Mohali-140307, India

Manisha Verma, Indo Global College of Engineering, Abhipur, Mohali-140109, India

*Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication*

A couple of other factors assume a significant role to the inaudibility of the watermark and process security [9]. The First one is the data rate of the watermark which is a sign of the volume of the information that can be transferred in a specified interval of time. The Second one is the robustness of the watermark. After an intentional attack or after transmission and the inherent signal adaptations the robustness is a sign of reliability that watermark can be extorted. In case of Robustness the European Broadcasting Union investigates the Music Trace that is in turn used to implement the watermarking procedure [10]. Types of attack examined included analog transformation of the signal, digital sound coding, or repetitive filtering of the signal. This uncovered that the watermark can never again be extricated just when the superiority of the sound signal has been significantly corrupted because of the attack [15, 16].

The data rate and the robustness of the factors are equally reliant. The robustness of the watermark refuses as a result if more inaudible data is to be transferred in a specific time. Music Trace uses data containers which allow an acceptably high data rate and robustness to embed extra information [13]. A couple of most utilized information containers allow transmission of 48-bit extra information in 5 seconds among high robustness or 48-bit extra information in 2.7 seconds among a little lower robustness.

II. PROBLEM FORMULATION

As security is main concern in the today's scenario. While exchanging the information between the two-party's data security is must so that the data is not accessed by any unauthorized user. Audio watermarking is one the way if exchanging the data between the users. An audio watermarking is the process of embedded the text or image in the audio. In an audio signal an audio watermark is embedded that is a unique electronic identifier and utilized to recognize ownership of the copyright. A procedure in which data is embedded into a signal such as picture, video or audio in a manner that is hard to eliminate is known as Watermarking. There are various techniques of embedding image into the audio. Earlier the techniques like LSB, Echo-hiding were used for embedding data into the audio. In LSB the data that is to be send is embedded in the bits of the audio signal. The data is embedded into the real discrete audio signal through watermarking in Echo-Hiding through establishing a repeated edition of a real sample of the sound signal among some delay and decay rate to prepare it unnoticeable. But the main limitation of the traditional technique were that while the image was embedded into the audio, the whole image was send, including the portion, that was not requires, and as the results the data length increases and the chances of detection of information by unauthorized user also increases. Also more is the length of the data, more time is required to send the data.

So, there is need to propose a new method in which the data length is reduced. So that the security level of sending data will increase. As the new technique that is going to be proposed should be better than the traditional methods of embedding the data into the audio.

III. PROPOSED WORK

The data is embedded into the real discrete audio signal through watermarking in Echo-Hiding through establishing a repeated edition of a real sample of the sound signal among some delay and decay rate to prepare it unnoticeable. The problem that arises using the traditional methods of the audio watermarking was that the length of the data was more, due to which the audio watermarking can become less secure. So, in this a new method of the audio watermarking is proposed. In this before the data is hided into the audio signal the length of the data is reduced. The compression of the data before hiding it can increase the rate of sending the data. So, in these new methods the image is first compressed by using RLE encoding.and after that by using the LSB technique of audio watermarking the image is hided in the audio signal. The image that is hided in the signal is the watermarked image. The easy formation of the data compression is Run-Length encoding in this the runs of information are stored in the form of a single data value and count comparative to the actual run. The meaning of runs of data is the sequences where the similar information value exists in several consecutive data elements.

So, this proposed technique of the audio watermarking is efficient than the traditional techniques, as the length of the data is reduced.

The traditional methods of audio watermarking were not efficient as the data length was more the time consumed in sending the data also increases as decrease in the security of the system. So, a new method of audio watermarking is proposed, in which the data is compressed before hiding it into the signal. This method is efficient than the traditional methods of Audio watermarking. The methodology of the proposed technique is given below: -

Embedding of watermark

1) Initially select the audio signal in which the data is to be embedded for sending to the other authorized user form the source user.
2) A watermarked image is selected that is to be embedded in the audio signal for sending to the other authorized user form the source user.
3) In this step the size of the image is checked and if the size of the data is same as the audio file then goes to step 4. else go back to step 1
4) Now, Convert the selected watermarked image into the black/white form so that the data image is converted into the bits
5) Afterward in the next step the RLE encoding is applied on bits to compress the information, in which the sequences where the similar information value exists in several consecutive data elements are stored in the form of a single data value and count.
6) After this the data that is obtained after applying the Run-length encoding (RLE) encoding method is hided into the audio signal by using LSB technique of audio watermarking.

7) Finally, the data hiding audio file is obtained, after the file is obtained save the file. This file can be now being sent to the other user form the source user.

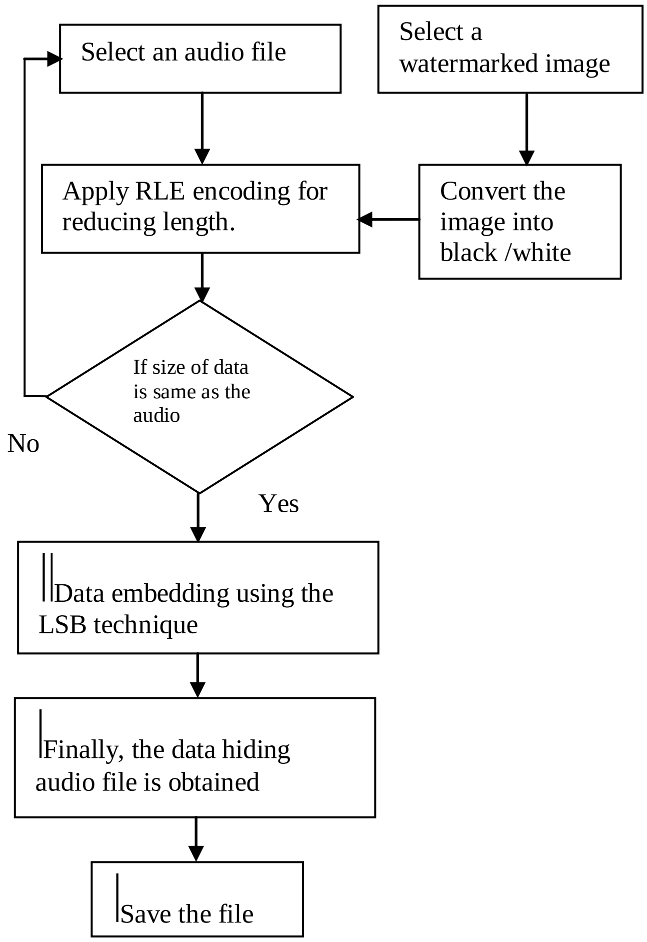

Select an audio file
Select a watermarked image
Apply RLE encoding for reducing length.
Convert the image into black /white
If size of data is same as the audio
No
Yes
Data embedding using the LSB technique
Finally, the data hiding audio file is obtained
Save the file

Figure 1 Flow chart of Embedding of Watermark

Extraction of watermark

After the encoding is done form the sender side, at the receiver end the decoding of the audio signal received is done to obtain the watermarked image Following are steps of decoding of the data: -

1) Select the audio file in which the data is hiding by the sender. So, to retrieve the information that is send by the user.
2) After the data hided audio signal. Next step is to extract the watermarked image from the audio signal.
3) After the image is extracted firm the audio signal, Next step is to apply the RLE decoding to obtain the information.
4) Finally, the extracted watermarked image is obtained from the audio signal.

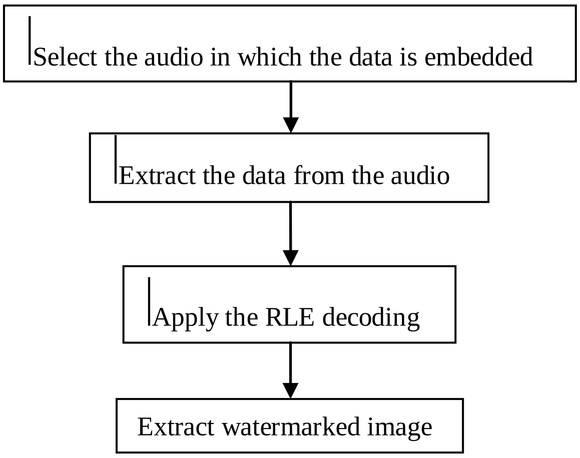

Select the audio in which the data is embedded
Extract the data from the audio
Apply the RLE decoding
Extract watermarked image

Figure 2 Flow chart of Extraction of Watermark

IV. RESULTS

This section defines the results that are obtained after implementing the proposed work in MATLAB. In this work, audio watermarking is done by applying RLE encryption technique. For this purpose, the graphical user interface is developed so that accessibility should become easy. The figure 3 shows the developed UI. Through user interface, the user can load the audio, process the audio and selected image, extract the data, evaluate the performance, and perform comparison. To start the processing of proposed work, first the user must click the on Load an audio with.wav format, by clicking this button the user will leads to the dataset where the audios are stored. From here, the user can select an audio for watermarking purpose.

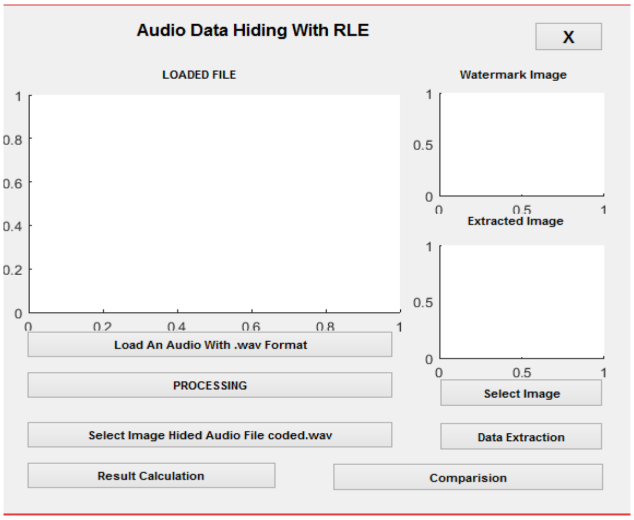


Figure 3 Proposed User interface for audio watermarking

Figure 4 shows the loaded audio file. After loading the audio file, next step is to select the image for hiding it behind the audio signals. The figure 5 delineates the message that is observed after hiding the image behind audio.

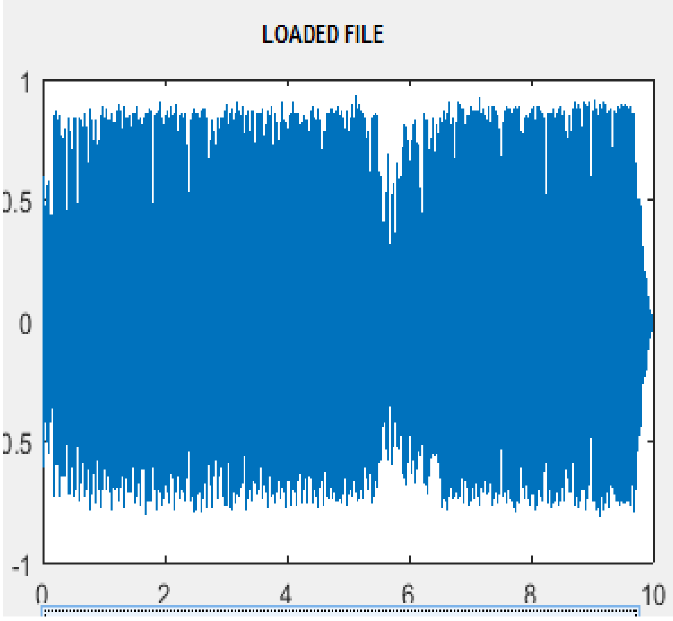
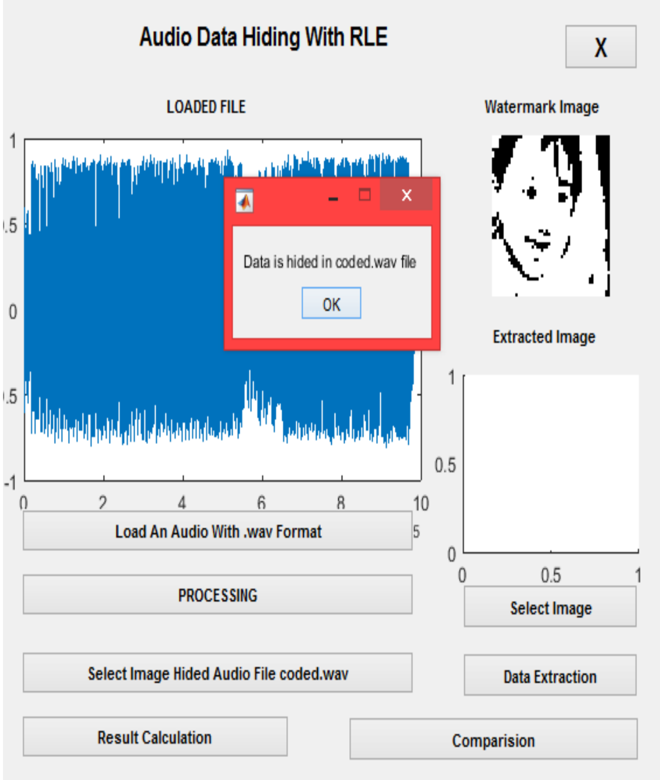


Figure 4 loaded audio file



Data is hided in coded.wav file

Figure 5 Data hiding

After hiding the image behind audio track, the next step is to extract the watermarked data. For this purpose, user must click the data extraction button. Then the extracted image will be displayed on the proposed interface as shown in figure 6.

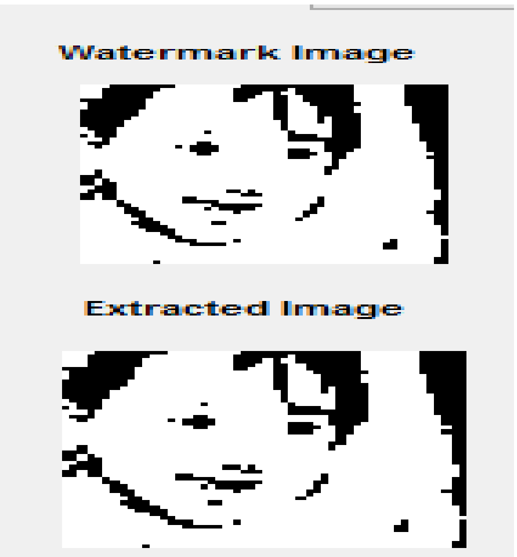


Figure 6 Extracted data in proposed work

Performance parameter in any field is used to measure the accuracy, efficiency, and proficiency of a technique. In the given proposed technique, performance parameters used are PSNR, MSE and BER. Each of them is explained as:

1. **PSNR (Peak Signal to Noise Ratio)** is a parameter used to evaluate the noise in the image or signal with respect to signal. It defines as a ratio between the maximum signal and the noise [17, 18]. Signal in the process is considered as an original data and noise is the error in the data. PSNR can be expressed as an equation in dB:

$$\text{PSNR} = 10.\, log_{10}\left(\frac{MAX_1^2}{MSE}\right)$$

$$= 20.log_{10}\left(\frac{MAX_1}{\sqrt{MSE}}\right)$$

$$= 20.log_{10}(MAX_1) - 10.log_{10}(MSE) \ldots\ldots\ldots\ldots\ldots\ldots\ (1)$$

In the above equation, Max is the maximum possible value of the image and MSE is the sum over all squared value differences which is divided by the size of an image.

2. **MSE (Mean Square Error)** is a parameter that defines the average error of an image. It is a difference between the estimator and the estimated value [17, 18]. It has used to estimate the quality of the proposed technique with respect to the traditional technique. Its value always is non-negative and closer to zero value is better.

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2 \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (2)$$

3. **BER (Bit Error Rate)** refers to the bitwise error rate in the signals. The formulation for BER is as follows.

$$BER = \frac{Number of\, Error\ obtained}{total\ number of\, transmitted\ bits} \ldots\ldots\ldots (3)$$

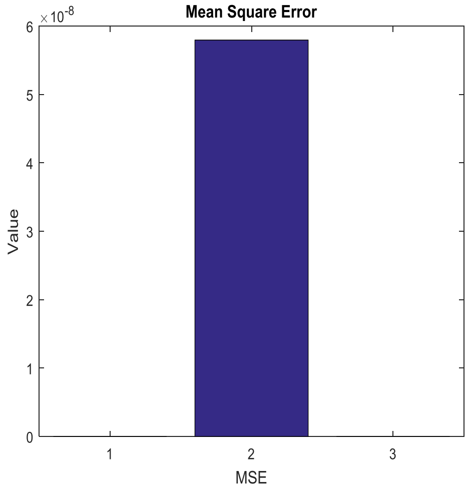


Figure 7 MSE analysis of proposed work

The graph in figure 7 represents the MSE of proposed work. It is evaluated for single case. Such 4 various cases are analyzed in proposed work and the MSE of proposed work is found to be quite effective. As per the observations from the graph given above, the MSE of proposed work is 5.7960e-08.

Similarly, the graph in figure 8 elucidates the BER of proposed work for single case. The system with lower BER is referred as the ideal once. Thus, it is mandatory top have the lower BER always. The graph proves that the BER of proposed work for single case is 0.0139.

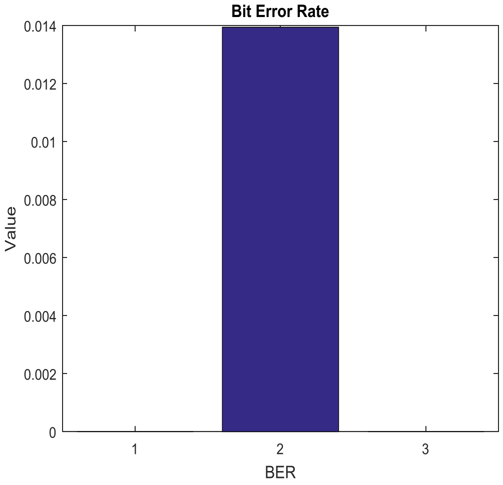


Figure 8 BER analysis of proposed work

The PSNR of proposed work is defined in figure 9. The PSNR is a performance metrics that is used to evaluate the peak signal to noise ratio in the obtained signals. This parameter defines the ratio of information with respect to the noise in the signals. The graph below proves that the PSNR of propose work is 71.7355.

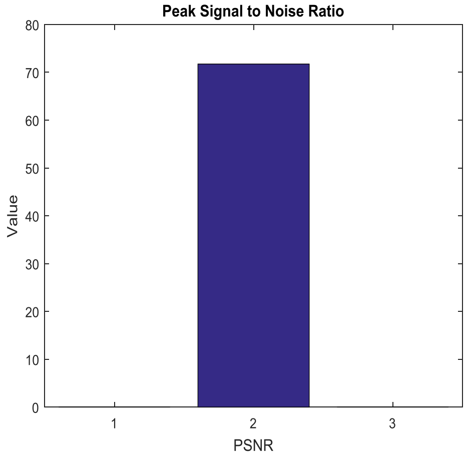


Figure 9 PSNR analysis of proposed work

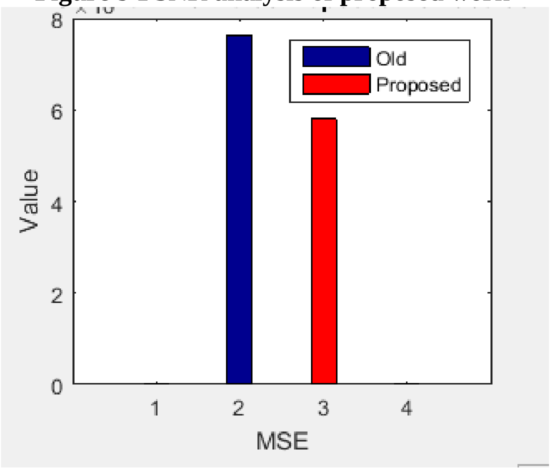


Figure 10 Comparison analysis of proposed and traditional work in terms of MSE

The graph in figure 10 defines the comparison analysis of proposed and traditional work in terms of mean square error. The MSE of traditional work is 7.624e-08 and for proposed work the MSE is 5.796e-08. The MSE of traditional work is higher in comparison to the proposed work.

The graph in figure 11 depicts the comparison analysis of the BER of proposed and traditional work. The bar in blue color shows the BER of old or traditional work and the bar in red depicts the BER of proposed work. The BER of proposed work is 0.013818 and for traditional work, it is 0.014049. Similarly, the graph in figure 12 shows the comparison analysis with respect to the PSNR. The PSNR of proposed wok is 72.3687 and the PSNR of old work is 71.1781. Therefore, it can be said that the PSNR of proposed work is higher than the traditional work and hence proves the proficiency of the proposed work.

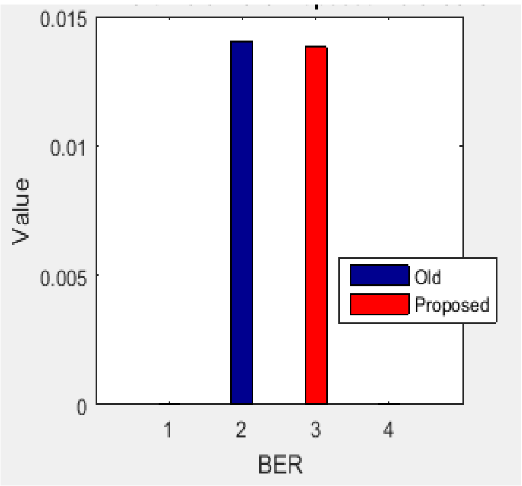


Figure 11 Comparison analysis of proposed and traditional work in terms of BER

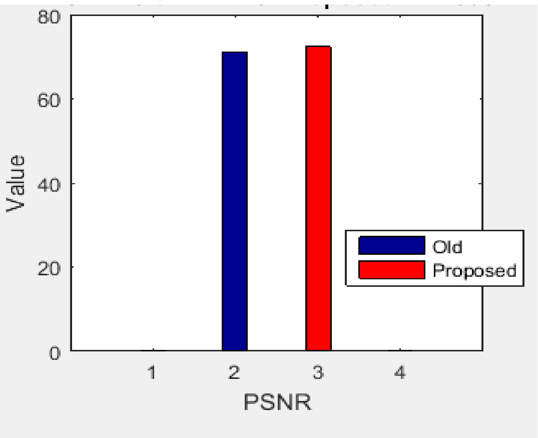


Figure 12 Comparison analysis of proposed and traditional work in terms of PSNR

V. CONCLUSION

The watermarking plays an important role to secure the data from unauthorized users. This study represents the concept of digital watermarking that has been gained a lot of attraction from all most each domain where the confidentiality and security of the information is major concern. Many research works have been conducted in this field and still some of these are under process. After analyzing the traditional work, the author concluded that the major focus was on image watermarking thus, in this work, the author developed the audio watermarking mechanism by using the image as a watermark. The performance of proposed work is evaluated in the terms of BER, PSNR and MSE. After evaluating the performance of the proposed work, the overall performance of the proposed work is found to be quite efficient than the traditional work.

REFERENCES

[1] Vinita Gupta and Atul Barve (2014), “A Review on Image Watermarking and It’s Techniques” International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 4, Issue 1, pp.92-97

[2] Shraddha S. Katarina (2012) “Digital Watermarking: Review” International Journal of Engineering and Innovative Technology (IJEIT), Vol. 1, Issue 2, pp 145- 153

[3] Manjit Thapa, Sandeep Kumar Stood, Meenakshi Sharma (2011), “Digital Image Watermarking Technique Based on Different” (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 2, No. 4, pp 14- 19

[4] Darko Kirov ski, H.S. Malvar (2003), “Spread-Spectrum Watermarking of Audio Signals”, “IEEE transactions on signal processing, Vol. 51, NO. 4, pp1020- 1033. Doi. 10.1109/TSP.2003.809384

[5] Komal V. Genkan and Pallavi K. Patil (2012), “Overview of Audio Watermarking Techniques” International Journal of Emerging Technology and Advanced Engineering Website, Vol. 2, Issue 2, pp 67- 70,

[6] Ali Al-Haj, Ahmad Mohammad and Lama Bata (2011), “DWT–Based Audio Watermarking”, The International Arab Journal of Information Technology, Vol. 8, No. 3, pp 326-333

[7] Won-gyum Kim and Jong Chan Lee and Won Don Lee (1999), “An audio watermarking scheme robust to mpeg audio compression”, Published in NSIP.

[8] Kais Khaled and Abdel-Ouahab Boudraa (2013), “Audio Watermarking via EMD”, IEEE transactions on audio, speech, and language processing, Vol. 21, No. 3, pp 75-80. Doi.10.1109/TASL.2012.2227733

[9] Shinichi Murata, Yasunari Yoshitomi, Hiroaki Ishii (2011), “Audio Watermarking Using Wavelet Transform and Genetic Algorithm for Realizing High Tolerance to MP3 Compression”, Journal of Information Security(**JIS),** Vol.2 No.3, pp. 99-112

[10] Mitchell D. Swanson, Bin Zhu, Ahmed H Tewfik, Laurence Boney (1998) “Robust audio watermarking using perceptual masking”, ELSEVIER Signal Processing, 66, pp 337—355 https://doi.org/10.1016/S0165-1684(98)00014-0.

[11] Yenta Said Can, Fatih Alagoz, and Melih Evren Burus (2014), “A Novel Spread Spectrum Digital Audio Watermarking Technique” Journal of Advances in Computer Networks, Vol. 2, No. 1, pp 6-9

[12] Shervin Shokri, Mahamod Ismail, Nasharuddin Zainal, Abdollah Shokri (2013), “BER Performance of Audio Watermarking Using Spread Spectrum Technique” 4th International Conference on Electrical Engineering and Informatics (ICEEI), Vol. 11, pp 107–113. Doi. https://doi.org/10.1016/j.protcy.2013.12.168

[13] Premia Demarks and Robert Markiewicz (2014), “Robust Audio Watermarks in Frequency Domain”, Journal of telecommunication and information technology, pp 12-21

[14] Ranjeet Yadav, Sachin Yadav, Jyotsna Singh (2010), “Audio Watermarking Based on PCM Technique”, International Journal of Computer Applications, Vol. 8, No.2, pp 24-28.

[15] Harbinder Singh, Haya Fatima, Samreeti Sharma, Dinesh Arora (2017), “A novel approach for IR target localization based on IR and visible image fusion”, 4th International Conference on Signal Processing, Computing and Control (ISPCC), pp.235-240, IEEE.

[16] Arshdeep Kaur, Harbinder Singh, Dinesh Arora (2017). “An efficient approach for image denoising based on edge-aware bilateral filter”, 4th International Conference on Signal Processing, Computing and Control (ISPCC), pp.56-61, IEEE.

[17] Ramandeep Kaur, Jagriti Bhatia, Hardeep Singh Saini and Rajesh Kumar (2014), “Multilevel Technique to Improve PSNR and MSE in Audio Steganography”, International Journal of Computer Applications (IJCA), ISSN: 0975-8887, Vol.103, No.5, pp.1-4. doi.10.5120/18067-9008

[18] Ramandeep Kaur, Abhishek Thakur, Hardeep Singh Saini, Rajesh Kumar (2014), “Enhanced steganographic method preserving base quality of information using LSB, Parity and spread spectrum technique”, 5th IEEE International Conference on Advanced Computing & Communication Technologies (ACCT- 2015), at Rohtak, Haryana, India, pp.148-152. doi.10.1109/ACCT.2015.139