ISSN (Print) : 0974-6846
Indian Journal of Science and Technology, *VOL 8(34),DOI: 10.17485/ijst/2015/v8i34/69604, December 2015* ISSN (Online) : 0974-5645

Audio Steganography using QR Decomposition and Fast Fourier Transform

Ifra Bilal* **and Rajiv Kumar**

Department of Computer Science and Engineering, Sharda University, Greater Noida - 201306, Uttar Pradesh, India; liberal.ifra@gmail.com, rajivbec@gmail.com

Abstract

Large demand of internet services requires our data to be transmitted in a secure manner. Data can be transmitted secretly using three security methods: Steganography, cryptography and watermarking. Among these, steganography provides better confidentiality. It is the art and science of hiding information in ways that prevents the detection of the hidden message. We focus in this paper on audio steganography where the carrier to hold the secret image is a digital audio file. The novelty of this paper lies on the implementation of QR decomposition technique in audio steganography. To the best of our knowledge no QR technique has been implemented in audio steganography. The paper embeds the bits of the secret image in the lower diagonal elements of the carrier audio file using QR decomposition technique. Three different formats have been specified for input secret image: .jpg, .bmp, .png. The paper also embeds the secret image along the frequency distribution of the carrier audio using Fast Fourier Transform. Another contribution of this paper is comparison between Fast Fourier Transform and QR decomposition technique. The quality of the image is measured using PSNR. The result shows that QR decomposition technique is better than existing Fast Fourier Transform as the calculated PSNR is above 40 dB for all the input images. Further, the paper compares the results obtained from QR technique with other existing methods like SVD. It can be noted that the accuracy of the QR decomposition technique is more than the existing methods and has proven to be very efficient. The system can be used for covert communication or tamper proofing.

Keywords: Audio Signal, Confidentiality,Fast Fourier Transform, Steganography, QR Decomposition Technique

1. Introduction

With the large demand of internet services today, thousands of millions of people use internet for real communication and many life applications. People in one way or the other rely on internet services to transfer their confidential data. However, rapid use of internet application requires our data to be transmitted in a secure manner. Data can be transmitted secretly using three main methods of security: Cryptography, watermarking and steganography. Cryptography is where security engineering meets mathematics. It protects the secret information by encrypting it into an unreadable format (cipher text). Watermarking is about establishing the identity of information to prevent unauthorized use. It embeds the information into digital file in such a way that its removal is hardly possible. Typical application of digital watermarking is to identify the ownership of content by embedding the owner mark into it. It is mainly used for authentication, certification and conditional access. Steganography is the art and science of hiding information into a digital file in such a way that prevents the detection of the hidden message. Steganography is one of the best techniques used for ensuring data security[1]. Steganography requires a cover file to hold secret data. Cover may be a text file, image, audio or even video. Secret message may be a text file, cipher text, image or audio. Stego key is used for embedding and extraction

* *Author for correspondence*

process. Embedding of the secret message into a cover file should be carried out in such a way that the quality of the audio file is not compromised. After embedding the secret message into cover file, a stego file is generated and transmitted over the channel. To extract the secret message, receiver must also have the stego key. The main difference between cryptography and steganography is that cryptography scrambles the structure of the secret message to make it meaningless and unintelligible to an unauthorized person. It makes no attempt to hide the secret message. In contrast, steganography doesn't alter the structure of the secret message but hides it inside the cover file. Steganography even prevents the detection of the secret message[2,3].

2. Audio Steganography

Audio steganography requires modification of audio carrier signal in an imperceptible manner. Figure 1 gives general model of audio steganography. Inaudibility and robustness are two necessary requirements for any effective audio steganography algorithm. Inaudibility must be given the special attention since if the quality of the original audio carrier signal can't be preserved, steganography technology will fail[4].

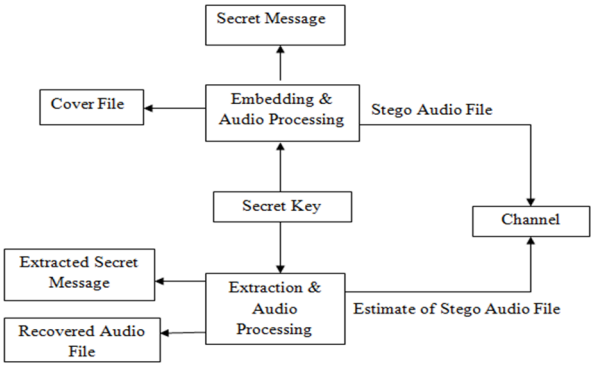


Figure 1. Audio steganography.

Research in audio steganography is not as mature as research in image steganography. One reason could be the Human Auditory System which is much more sensitive than Human Visual System. Also, inaudibility is much more difficult to achieve than invisibility of images. Steganography assumes that the cover file used to hide the secret message shouldn't raise any suspicion to malicious people. Moreover, audio files are more popular which makes them eligible enough to carry the secret message. Second reason could be most of the steganalysis attacks are more directed towards digital images hence leaving audio steganalysis relatively unexplored[5].

2.1 Requirements of Audio Steganography

2.1.1 Imperceptibility to Human Auditory System

Audio steganography requires the modification of audio carrier signal in an imperceptible manner. This is the fundamental requirement to ensure effective audio steganography. Also, inaudibility must be given special attention since if the quality of the audio file can't be preserved, users will not accept the audio steganography technology.

2.1.2 Robust to Various Kinds of Distortion

The stego file should be robust and sturdy against distortion such as amplification, compression etc.

2.1.3. Simplicity of Detection and Extraction

For the user who possesses the secret key to retrieve the secret message, it should be easy for him to extract the secret message. This ensures steganography is perfect and can only be deciphered by the intended user.

2.1.4. High Data Hiding Capacity

The audio carrier signal should be able to carry large amount of secret message without burdening the original audio carrier signal. Audio signals are represented by much less samples per time interval, which indicates that the amount of secret message capacity that can be embedded robustly and inaudibly in an audio file is much lower than amount of secret message that can be embedded in visual files. There is a tradeoff between capacity and robustness parameters where increase in capacity decreases the robustness level[4,5].

3. Audio Steganography Methods

Data embedding approaches in audio steganography are broadly classified into spatial domain and transform domain. Spatial domain techniques such as low bit encoding, echo hiding embed the secret message directly in the time domain. Spatial domain methods hide the secret message on the basis of geometric characteristics

of the audio carrier signal. Most of the spatial domain methods employ Least Significant Bit (LSB) techniques. Conventional LSB technique and its variant provide an easy way to hide information. Spatial domain methods are very tolerant to noise addition at low levels but with low data hiding capacity[6].

Transform domain techniques employ Human perceptual properties and frequency masking characteristics of Human Auditory system for steganography. Human Auditory system has several characteristics which can be exploited by various methods of transform domain to hide the secret message[7]. Various methods falling under transform domain are spread spectrum, discrete wavelet transform, tone insertion, discrete Fourier transform, Fast Fourier Transform (FFT). Robustness in the hidden data is the main characteristic of transform domain method. The detailed comparison is presented in Table 1.

4. Methodology

4.1 Steganography Techniques

Data embedding approaches in audio steganography are broadly classified into spatial and transform domain. In this paper, audio steganography is implemented using two transform based approaches: Fast Fourier Transform (FFT) and QR decomposition technique.

4.1.1 Fast Fourier Transform

The Fast Fourier Transform method hides the secret information along the frequency distribution of the carrier audio signal. The method exploits certain characteristics of Human Auditory system. The Human Auditory system has several peculiarities that can be exploited for hiding secret information effectively. The 'masking effect' phenomenon masks weaker frequencies near stronger resonant ones. In this experiment, four different images are used as the secret watermark image as shown in Figure 1. Two single low frequency components are used as the audio carrier. Generally, the bigger the size of the watermark image is, the smaller is the watermark capacity and worse is the inaudibility of the stego signal. For the track with 44100 samples per second, block size of 8820 corresponds to the duration of 0.2s and hence frequency resolution is of 5Hz. The image is embedded in frames bit by bit and it is again reconstructed by collecting and putting together those bits at the receiver side. Here, FFT is used to embed the image in an audio carrier. FFT is the method to calculate the discrete Fourier Transform and its information. It actually breaks down the signal into sinusoids of different frequency domains[8]. FFT converts the continuous time domain into continuous frequency domain, including both magnitude and phase information. Using FFT technology it is possible to capture the waveform and analyze it for future requirement. The example demonstrates that the frequency domain of the audio signal can effectively be used to hide the secret information[9].

4.1.1.1 Flow Chart of Audio Steganography using FFT

The proposed flow chart is shown in Figure 2. The steps are as follows:

- Read the carrier audio signal.
- Calculate the length A1 of the digital audio signal.
- Read the secret watermark image.

Table 1. Comparison between various steganography techniques

Domain	Methods	Advantage	Disadvantage	Hiding Rate
Spatial domain	Low bit encoding [1][6]	High embedding rate, simple and easy	Noticeable to human ear, less robust to human ear	16kbps [6]
	Echo hiding [1][2][6]	Recovers easily from lossy data compression algorithms	Low capacity and low security	50bps [6]
Transform domain	Spread spectrum [1][6]	More robust	More vulnerable to time scale modifications	20bps [6]
	Discrete Wavelet Transform [1][6][7]	High embedding capacity	Inaccurate data retrieval	70kbps [6]
	Tone Insertion [1][2][6]	Imperceptibility of embedded data	Poor Transparency	250bps [6]
	Phase Coding [2][6][8]	Robust against signal distortion	Low capacity	333bps [6]

- Calculate the length A2 of the watermark image.
- As per the assumption check whether the A1 is eight times greater than A2.
- If A1 is greater than proceed with the proposed algorithm.
- Else display the message 'image is too large' and initialize the process from starting.
- Get the secret key to embed watermark using frequency domain of the carrier audio file.
- The stego audio file is created and is transmitted from the transmitter side.

The reverse operation is performed at the receiver side for retrieving the secret message embedded in the transmitted stego audio file.

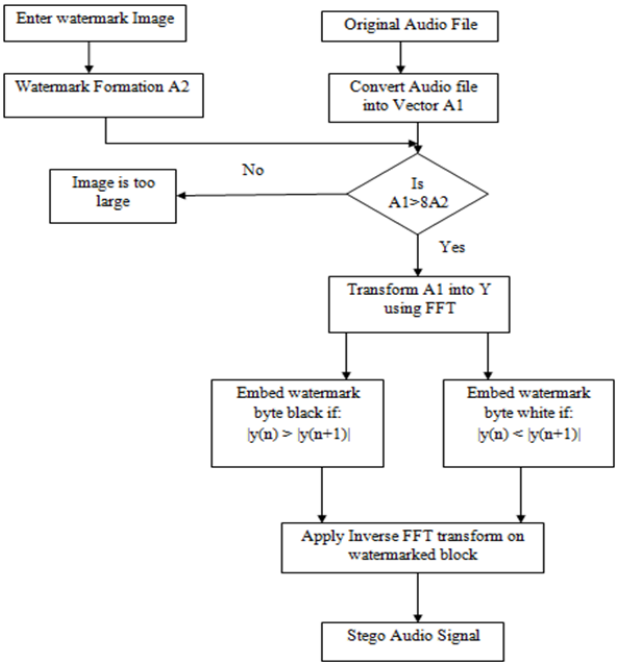


Figure 2. Flow chart of audio steganography using FFT.

4.1.2 QR Decomposition Technique

The QR decomposition is also known as QR factorization. The QR decomposition of a matrix refers to the decomposition of a matrix into an orthogonal matrix and an upper triangular matrix. QR decomposition of a real square matrix A is decomposition of matrix A as:

A= QR

Where Q is the orthogonal matrix (i.e. Q^T. $Q = 1$) and R is the upper triangular matrix.

Digital image is embedded in the carrier audio signal using QR decomposition technique. Cover file is again the carrier audio signal which is in .wav format. Initially, a digital image to be embedded in the audio file is the black and white image. The algorithm is checked for different input images[2,11].

4.1.2.1 Embedding Procedure

The procedure is illustrated in the flow chart shown in Figure 3 and described in details in steps as: The first step is to frame the audio carrier signal. The number of frames equals the number of bits that are supposed to be embedded in an audio carrier signal. After framing the host carrier signal and equal length frames are obtained, each frame should be taken out of its vector state and converted into two-dimensional matrices. Different types of images are used as the watermark secret message and are embedded in the audio carrier of .wav format using the QR decomposition technique. The overall steps in the embedding procedure are as follows:

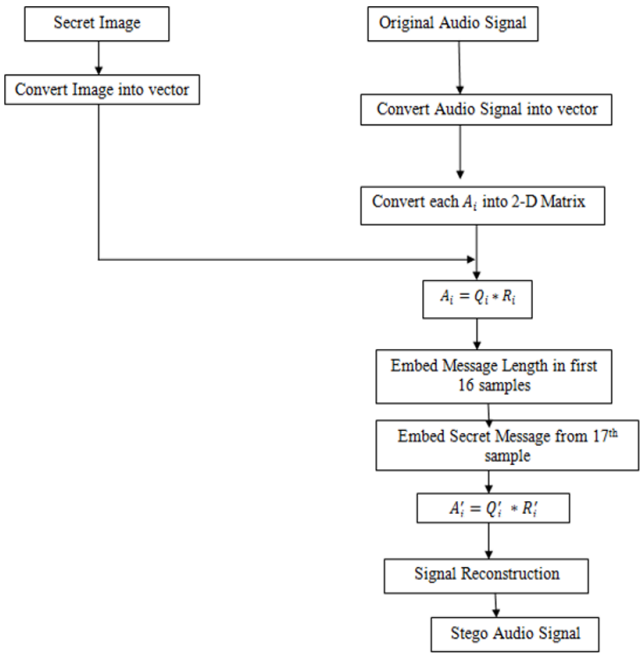


Figure 3. Embedding procedure.

- Insert input audio signal.
- Calculate size of audio signal.
- Insert secret image to be embedded in the audio carrier.
- Calculate rows and columns of secret image.
- Preprocessing is done on the secret image.
- Audio carrier signal is decomposed using QR decomposition to obtain upper triangular matrix R.

[Q R]= qr [A].

- Embed message length in first 16 samples.
- Embed secret image from 17th sample.
- Calculate matrix R'.
- Apply inverse QR operation to obtain A'.

A'= Q*R'.

4.1.2.2 Extraction Procedure

The extraction process is performed as shown in Figure 4. The various steps for extracting the secret image from the carrier audio signal are as follows:

- Like the embedding step, after receiving and framing the audio signal, intended frames are converted into two-dimensional matrices. Then QR decomposition is conducted on them based on equation:

A'= Q' * R'.

- Extract message length from first 16 samples.
- Extract secret message from the 17th sample and calculate b based on the equation

$ifz\ (i) = 1, \qquad b(i) = -1 * b\ (i)$

$a = b/\ (2\hat{}(nbits - 1))$

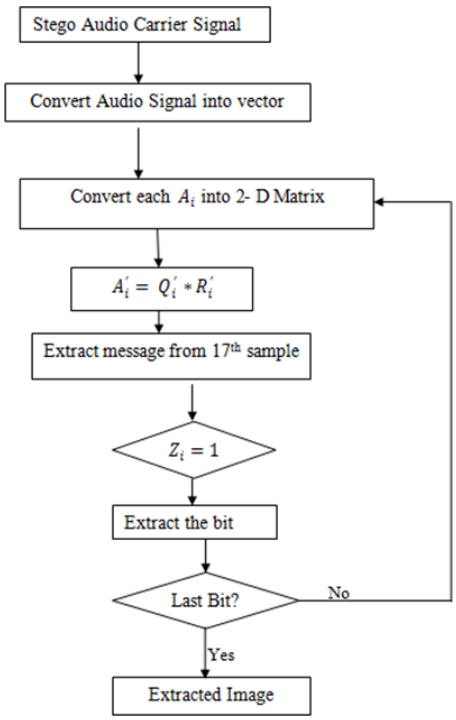


Figure 4. Extraction procedure.

4.2 Image/Audio Quality Measurements

The image signal is subjected to many kinds of distortions as it passes through stages such as processing, compressing and transmitting. Measuring the quality of the image is a complicated task as human opinion is affected by physical and psychological parameters. There are many techniques for measuring the quality of the signal. MSE, PSNR, WPSNR, SSIM, SNR are the most commonly used image quality measures[12,13].

PSNR is an abbreviation for Peak Signal-to-Noise Ratio (PSNR). It is defined as the ratio between maximum possible power of a signal and the power of distorting noise that affects the quality of the signal. The PSNR is usually expressed in terms of logarithmic decibel scale using Equation 1.

The mathematical representation of the PSNR is as follows:

$$PSNR = 20\log_{10}\left(\frac{MAX_f}{\sqrt{MSE}}\right) \qquad \text{Eq. 1}$$

Where the **MSE** (Mean Squared Error) is:

$$MSE = \left(\frac{1}{(m*n)} * sum\left(sum\left((f-g)^2\right)\right)\right) \qquad \text{Eq. 2}$$

f represents the matrix of original signal
g represents the matrix of degraded signal
m represents the number of rows of signal
n represents the number of columns of signal
$\mathbf{MAX}_f$ is the maximum signal value that exists in original signal which is known to be good signal.

5. Result Analysis

The paper implements audio steganography using Fast Fourier Transform and QR decomposition technique. After the secret image is embedded in the audio carrier, the strength of the stego audio is calculated using PSNR. The results are shown in the subsequent sections as follows:

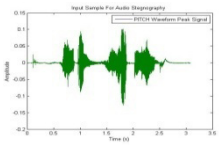
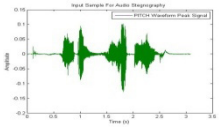
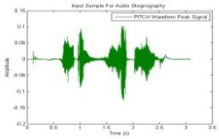
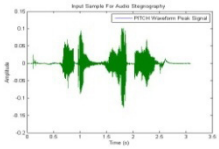
5.1 By using Fast Fourier Transform

Four input images are embedded and extracted using FFT. Table 2 shows the input and extracted images with the calculated PSNR.

5.2 By using QR Decomposition

Different images were embedded and extracted using QR decomposition technique. Table 3 depicts the results using QR decomposition.

Table 2. Audio steganography using Fourier Transform

S.No	Audio Signal	Original Image	PSNR Embed (dB)	Extracted Image	PSNR Extraction (dB)
1			13.4		63.69
2			5.3165		43.38
3			9.61		52.0772
4			6.1283		40.19

5.3 Comparison between FFT and QR Decomposition Technique

Table 4 shows the various input images embedded in the audio carrier signal using Fast Fourier Transform and QR approach. PSNR is calculated in both the cases and both techniques are compared based on the calculated PSNR value.

As depicted from the Figure 5, PSNR of extracted images by using the QR approach is better than the Fast Fourier Transform for all the input images. Also, experimental results have shown that the image after embedding and extraction are not the same in case of FFT. Some information is destroyed after extracting the secret image as can be seen from Table 4. Hence, it can be said that FFT is not the good technique to be applied in audio steganography. Hence, from the experiment we can say, implementation of QR decomposition technique in audio steganography is better than the existing FFT based method and has proven to be very efficient.

Table 3. Audio steganography using QR decomposition

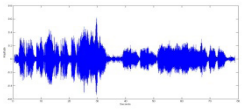
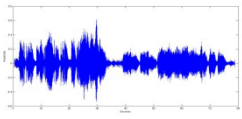
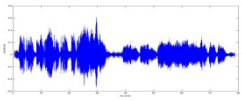
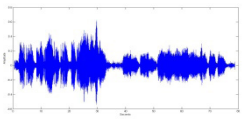
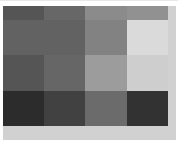
S. No.	Audio Signal	Original Image	PSNR(dB)	Extracted Image
1			44.3	
2			36.57	
3			35.57	
4			33.17	

Table 4. Comparison between (FFT) and QR approach in audio steganography

S.No	Embedded Image	Extracted Image Using FFT	PSNR (dB)	Extracted Image Using QR Decomposition	PSNR (dB)
1			44.13		63.69
2			36.57		43.38
3			35.57		52.0772
4			33.1758		40.19

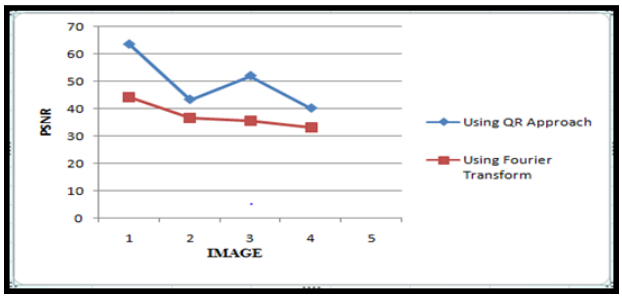


Figure 5. Comparison between Fast Fourier Transform and QR approach.

Table 5. Comparison with different methods

S. No	Researcher	Technique	Accuracy
1	Q. Su et al. [14]	QR on image	36
2	Golea et al.[15]	SVD	40
3	Su et al. [16]	Schur	38
4	Bilal & Rajiv	QR on audio (proposed method)	60

Table 5 gives the PSNR values that are obtained by different methods. By comparison, it can be seen that the accuracy of the proposed method is more than Q. Su et al.[14] based on QR decomposition on image, Golea et al.[15] based on Singular Value Decomposition (SVD) and Su et al.[16] based on schur. As depicted from Figure 6, the accuracy of the proposed system is more than the existing methods.

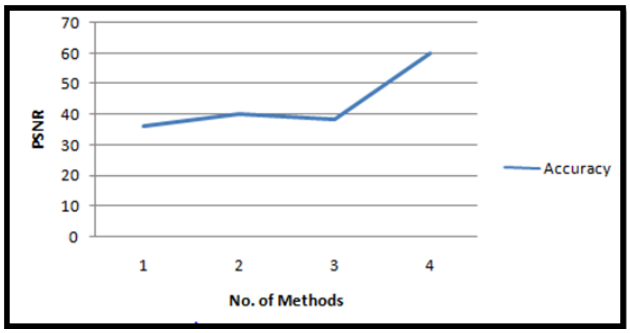


Figure 6. Comparison of proposed method with different methods.

6. Conclusion:

Many new steganography techniques exist which provide better protection to digital data. In this work, a survey on various audio steganography techniques has been carried out. Audio steganography is implemented using two transform based approaches: Fast Fourier Transform and QR approach. Implementation of Fast Fourier Transform in audio steganography demonstrates that the frequency domain of the audio signal can effectively be used to hide the secret message. But it is not the sophisticated

algorithm as the poor quality image is recovered. Low value PSNR signifies that the recovered signal is more corrupted with noise.

Audio steganography is also implemented using QR decomposition technique. Secret message is embedded in the carrier audio signal using QR decomposition technique. The algorithm is checked for various types of images. PSNR of extracted images by using the QR approach is better than the FFT for all the input images as the calculated PSNR value is above 40 dB. From the result we can say, implementation of QR decomposition technique in audio steganography is better than the existing FFT based method and has proven to be very efficient.

7. References

1. Djebbar F, Ayad B, Meraim KA, Hamam H. Comparative study of digital audio steganography techniques. Journal on Speech and Music Processing. Springer; 2012 Dec; 1:1–16.
2. Valarmathi R, Kadhar Nawaz GM. Secure data transfer through audio signal with LSA. Indian Journal of Science and Technology. 2015 Jan; 8(1):17–22.
3. Wadhwa A. A survey on audio steganography techniques for digital data security. International journal of advanced research in computer science and software engineering. 2014 Apr; 4(4):618–22.
4. Ali AH, Mohammad A. Digital audio watermarking based on the discrete wavelets transform and singular value decomposition. European Journal of Scientific Research. 2010 Jan; 39(1):6–21.
5. Chadha A, Satam N. An efficient method for image and audio steganography using Least Significant Bit (LSB) substitution.International Journal of computer application. 2013 sep; 77(13):37–45. 1083, 2013 Sep; 77(13):37–45.
6. Delforouzi A, Mohammad P. Adaptive digital audio steganography based on integer wavelet transform. Circuits, Systems and Signal Processing. 2008 Apr; 27(2):247–59.
7. Bilal I. Rajiv K, Roj MS, Mishra PK. Recent advancement in audio steganography. International Conference onin Parallel, Distributed and Grid Computing (PDGC), IEEE; Solan; 2014. pp. 402–5.
8. Valarmathi R, Kadhar Nawaz GM. Secure data transfer through audio signal with LSA. Indian Journal of Science and Technology. 2015 Jan; 8(1):17–22.
9. Ali AH, Mohammad AA, Bata L. DWT-based audio watermarking.Int Arab J Inf Technol. 2011 July; 8(3):326–33.
10. Rameshkumar P, Monisha M, Santhi B. Enhancement of information hiding in audio signals with efficient LSB based methods. Indian Journal of Science and Technology. 2014 Jun; 7(S5):80–5.
11. Zamani M, Manaf AA, Abdullah SM. Correlation between PSNR and bit per sample rate in audio steganography. In 11th International Conference on Signal Processing. 2012. p. 163–8.
12. Nehru G, Dhar P. A detailed look of audio steganography techniques using LSB and genetic algorithm approach. IJCSI International journal of computer science issues. 2012 Jan; 9(1):402–6.
13. Delforouzi A, Pooyan M. Adaptive digital audio steganography based on integer wavelet transform. Springer, Circuits, Systems and Signal Processing. 2008 Apr; 27(2):247–59.
14. Kumar R, Kumar A, Ahmed P. A benchmark dataset for devnagari document recognition research. 6th International Conference on Visualization, Imaging and Simulation (VIS'13); Lemesos: Cyprus. 2013. p. 258–63.
15. Qingtang S, et al. Color image blind watermarking scheme based on QR decomposition. Signal Processing. 2014; 94:219–35.
16. Golea NEH, Seghir R, Benzid R. A bind RGB color image watermarking based on singular value decomposition. Hammamet. In AICCSA; 2010 May 16-19. p. 1–5.
17. Su Q, Niu Y, Liu X, Zhu Y. Embedding color watermarks in color images based on Schur decomposition.Optics Communications. 2012 Apr; 285(7):1792–802.