IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

AN APPROACH FOR STEGANOGRAPHY OF MULTIMEDIA DATA

[1]Aasima Khan, [2]Bhavitha K R, [3]Sunidhi Singh, [4]Shiddhika Goenka, Dr. H S Prasantha
[1]Student, [2]Student, [3]Student, [4]Student, [5]Professor
Department of Electronics and Communication Engineering
Nitte Meenakshi Institute of Technology, Bangalore, India

Abstract: In this new world of technology, communication using digital media has increased tremendously and this easy data exchange comes with the risk of intrusion. At times, the system itself can get affected by various types of malwares which leads to data loss. So, there is a need for a secure communication method to exchange sensitive data. Steganography is one such technique for hiding data over a media file in such a way that any eavesdropper will not be able to detect the presence of the hidden data. This paper proposes the LSB (Least Significant Bit) algorithm which hides data over different media files that are text, image and audio using python. In Image steganography, the cover images taken are of various types, i.e, binary, gray scale and color images. In audio steganography, we have also taken real-time audio as a cover file.

***Keywords*- LSB, Steganography, Python**

INTRODUCTION

With the rapid development of network technology, communication approaches have gone into a new era. Through devices like smartphones, laptops and personal computers, multimedia content can easily be created and transmitted over the Internet to specific people or groups. However, easy access and distribution convenience also increase the risk of eavesdropping when sensitive multimedia data is sent and received. There is a need to secure digital data to protect the confidentiality, integrity, authenticity, and availability of data only to the authorized users. Encoding data ensures its security by preventing unauthorized parties from gaining access to it and allowing only authorized parties to decode it. In Information technology and communication, security of data transmission is the most important factor. Securing of data can be done through techniques like Cryptography and steganography. Cryptography is the technique where we encrypt data into different formats so that it is incomprehensible to unauthorized users. In Cryptography, anyone can identify that data is hidden which can only be decrypted by the users having the encryption key.

Steganography is one such technique for hiding data over a media file in such a way that any eavesdropper will not be able to detect the presence of the hidden data. In case of steganography an encryption key may or may not be in use. There are different types of steganography i.e., Text, Image, Audio and Video Steganography.

1.1 Difference between Steganography and Cryptography

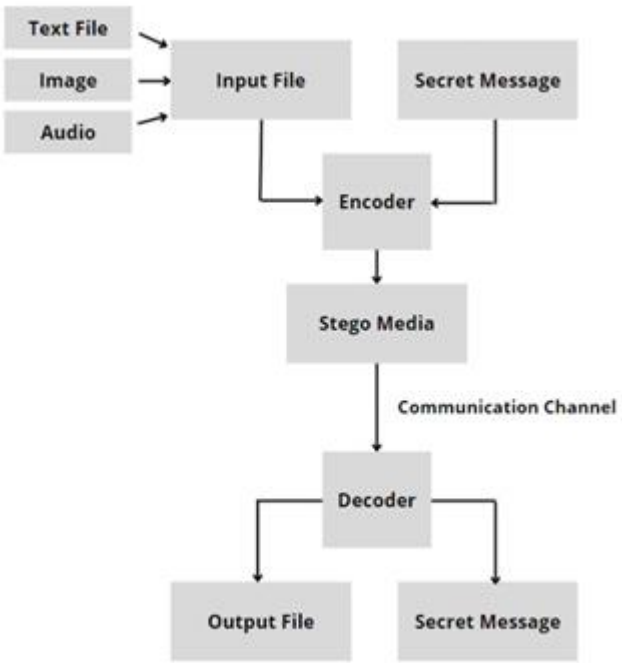
SN	Attributes	Steganography	Cryptography
1	Techniques	LSB, Spatial, Block complexity, Transform Domain	Transposition, substitution, Block ciphers
2	Secret key	May be used	Necessary, cannot work without key
3	Outcome	Stego image	Cipher text
4	Durability	Steganography basically hides the data under a cover Le it does not make any changes to the data	Cryptography, using an encryption algorithm. converts the plain text into cipher text i.e. it makes changes to the original data
5	Carrier	Image, Audio, Video, Text	Text Files

1.2 Application of Steganography

Applications of Steganography:

1) Communicating and storing secret information in a confidential manner.
2) Preventing data alteration.
3) The purpose of this is to facilitate secure secret communications when cryptographic encryption methods are not available.

1.3 Basic Steganographic model



The basic Steganography model consists of an input file, secret message, encoder, decoder and an output file. There can be various types of media files that can be taken as an input. We have used text, image and audio files as input. Now, this input file along with a secret message taken from the user is given to the encoder which hides the secret message over the input file. The output of the encoder is known as stego media. Stego media is the media with the secret message embedded in it. This stego media is then passed through the communication channel and given as input to the decoder when it reaches the receiver side. The decoder extracts the secret message from the stego media, resulting in the output file.

2.RELATED WORK

In [1], This paper presents two JPEG image encryption schemes that use 16×16 DCTs as intermediate stages. For the first encryption scheme, it is more efficient to compress JPEG images, but its security level is not as high, so it may be suitable for applications where compression is more important than confidentiality.

In [2], the author concluded that using crypto-steganography, one can achieve two levels of security.There will be no third-party interruption by using this technique because no one can even know that data is embedded into the image as there will be no noise created in the cover image.

In [3], this paper proposes an Unique Data Security using Text Steganography (UDSTS) to build a system that is able to transmit and receive encrypted messages embedded in rich text Format: *.DOC, *.RTF, EMAIL /Message Body/, etc. The user can choose the fake text and the program tells whether this fake text will suit the real text. The user is enabled to set a different password for every message he sends and therefore two different messages can be transmitted to two groups with two different passwords using the same fake text.

In [4], S. Gupta and R. Jain proposed method implementation and efficient steganography using discrete wavelet transform where a message is hidden on encrypted image i.e., embedded in the low level frequency band sub-band of the cover image.As a result, the file sizes of the original image and that of the stego-image will not differ much.

In [5], In this paper, S. D. Torvi, K. B. ShivaKumar, and R. Das concluded that text-to-text steganography is a less-known and simple form of steganography. Through their work, they have shown that text information can be used to hide plain text messages. It is also shown that the file size increase is in bytes, rather than in kilobytes.

In [6], In this paper, a steganography technique in JPEG images is proposed by A. Darbani, M. M. Alyan Nezhadi and M. Forghani. In the proposed method, the embedded message is added to the image after the discretization stage as a part of data may be lost after the discretization of frequency values.

In [7], In this paper the author has introduced text steganography by generating the text summary by using the reflection symmetry of the alphabets of English language. The proposed method checks the vertical and horizontal reflection symmetry properties of the characters present in the text and selects the sentence to generate a summary of the text. The generated text summary is the cover text i.e. the stego-text generated by the system.

In [8], This article improves LSB information hiding. Proposed a color image algorithm using a secret key,combining information hiding and cryptography, increasing visual functions of the human eye and identity-based authentication by digital signature and encryption technology to improve information security.Finally, through experiment and comparing the peak signal-to-noise ratio and security, improved LSB image steganography algorithm using encryption technology is better than normal LSB image steganographic method with better security and higher PSNR.

In [9], This paper has described a high payload audio steganography method that is based on the lifting wavelet transform. The researchers calculated a person's hearing threshold in the wavelet domain and used it as an embedding domain for their analysis. The proposed solution has high audio quality and full recovery.

In [10], In this paper, the study found that the gain adjustment may improve the conventional technique. The proposed technique can improve the speech quality without increasing the amount of data transmission.

In [11], The authors suggested an audio steganographic approach based on the wavelet audio to image transform in this research. To embed covert data within audio signals, the suggested approach makes use of an existing image steganographic scheme. The results of the experiments reveal that the suggested technique is resistant to MP3 compression.

In [12], The author of this research has developed an enhanced LSB replacement method for disguising text information in a text file in a color image. Each character of the secret message, including special characters such as space, enter,,?, $, and so on, is transformed to ASCII code, and then each value is converted to an 8-bit binary number using this procedure. Each character's bit is contained in the last LSB of each pixel of the cover image.

3. METHODOLOGY

LSB Algorithm

LSB-Steganography is a steganography technique that hides messages within a media file by replacing the least significant bit of the media file with message bits to be hidden. The concept behind LSB embedding is that if we change a pixel's last bit value, the colour won't change substantially.Each color of a pixel is 1-byte information that shows the density of that colour. Image files are made up of pixels, and each pixel is made up of three colours . Every color we see in these photographs is created by combining these three hues. We know that in computer science, every byte is made up of 8 bits, with the first bit being the Most Significant Bit (MSB) and the last bit being the Least Significant Bit (LSB). This is where the idea of using steganography science came from; we used the LSB bit for writing our security information inside pictures.

The most basic method for concealing data within an image file is known as least significant bit (LSB) insertion. Using this method, we can overwrite the LSB of each byte in the cover image with the binary representation of the hidden data. The amount of change will be minimal and indistinguishable to the human eye if we use 24-bit color.
Taking an example, suppose that we have three adjacent pixels (nine bytes) with the following RGB encoding:

10010101 00001101 11001001 10010110 00001111 11001010 10011111 00010000 11001011

And we need to hide the following 9 bits of data. If we overlay these 9 bits over the LSB of the 9 bytes above, we get the following results:

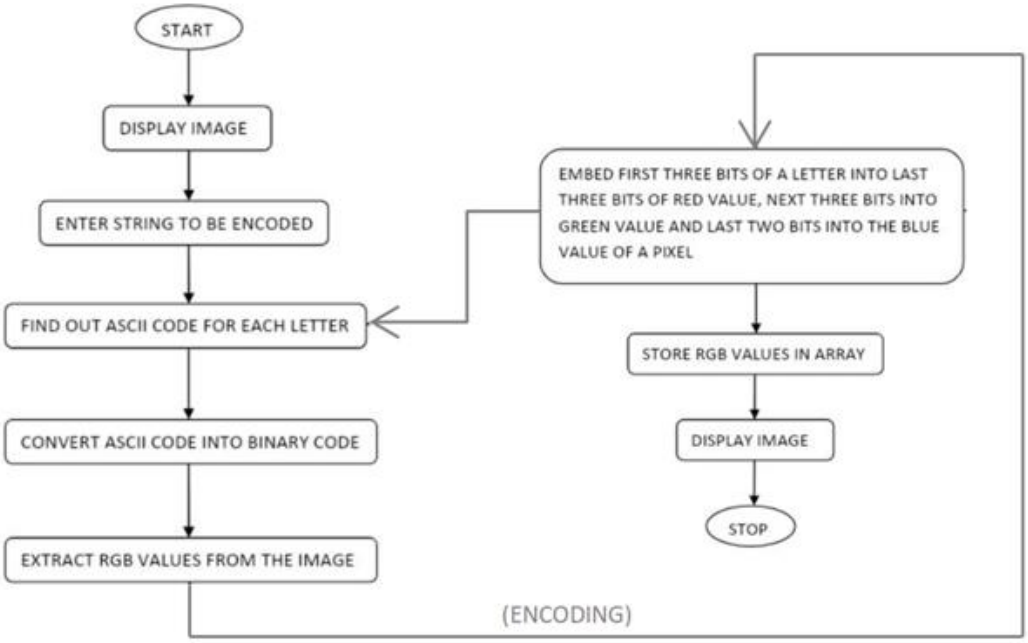
10010101 00001100 11001001 10010111 00001110 11001011 10011111 00010000 11001011

Audio steganography

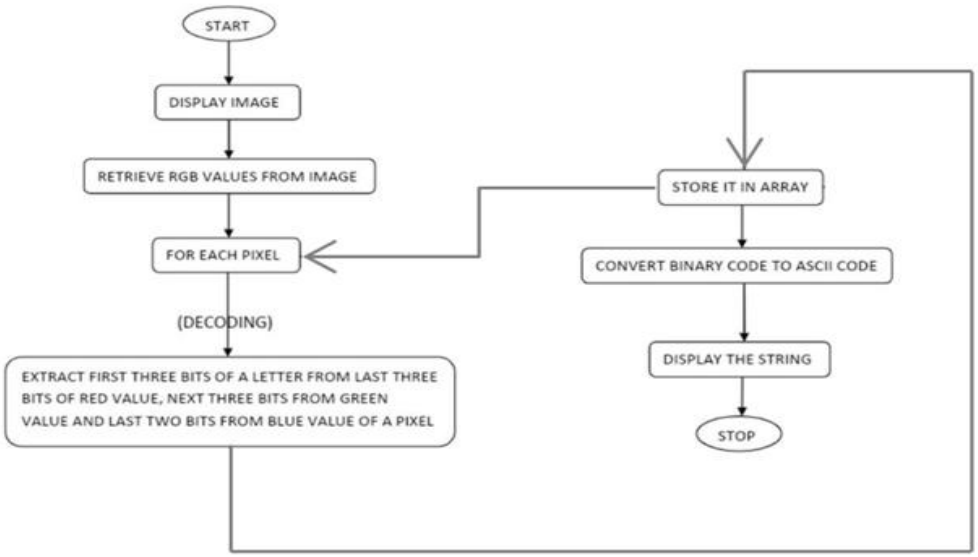
The goal of audio steganography is to conceal a secret message inside the audio. It is a method for securing the transfer of secret information or concealing its presence. If the communication is encrypted, it may also guarantee confidentiality to the secret message. The Least Significant Bit (LSB) coding method is the easiest approach to incorporate secret information in a digital audio file by substituting the least significant bit of the audio file with a binary message. As a result, the LSB technique can encode a vast quantity of hidden information into an audio recording.

The audio steganography process consists of following two steps:
1) In a cover-file, superfluous bits are identified. The bits that can be adjusted without affecting the quality or integrity of the cover-file are known as redundant bits.
2) The unnecessary bits in the cover file are replaced by bits of the secret information to embed the secret information in the cover file.

Flow Chart:



Encoding



Decoding

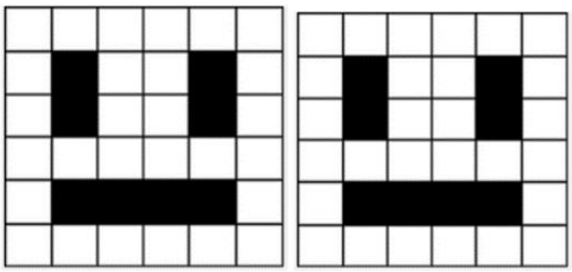
4. RESULTS & ANALYSIS

4.1 For image:

4.1.1 Binary Image:

Encode-

```
:: Welcome to Steganography ::
1. Encode
2. Decode
1
Enter image name(with extension) : binary.png
Enter data to be encoded : Steganography is practiced by those wishing to convey a secret message or code. While there are m
any legitimate uses for steganography, malware developers have also been found to use steganography to obscure the transmiss
ion of malicious code.  Forms of steganography have been used for centuries and include almost any technique for hiding a se
cret message in an otherwise harmless container. For example, using invisible ink to hide secret messages in otherwise inoff
ensive messages; hiding documents recorded on microdot -- which can be as small as 1 millimeter in diameter -- on or inside
legitimate-seeming correspondence; and even by using multiplayer gaming environments to share information.
Enter the name of new image(with extension) : binary2.png
```

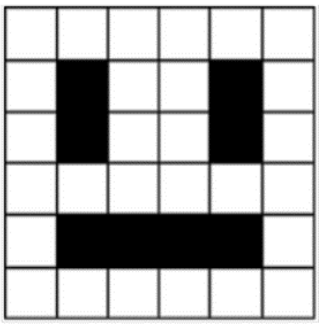


Input Image Encoded Image

The size of the input image is 12.3 KB. The dimensions of the image is 301*268. Width is 310 pixels and height is 268 pixels. The size of the encoded image is 12 KB. The dimensions of the output image is 304*266. Width is 304 pixels and height is 266 pixels.

Decode-

```
:: Welcome to Steganography ::
1. Encode
2. Decode
2
Enter image name(with extension) : binary2.png
Decoded Word : Steganography is practiced by those wishing to convey a secret message or code. While there are many legitima
te uses for steganography, malware developers have also been found to use steganography to obscure the transmission of malic
ious code.  Forms of steganography have been used for centuries and include almost any technique for hiding a secret message
in an otherwise harmless container. For example, using invisible ink to hide secret messages in otherwise inoffensive messag
es; hiding documents recorded on microdot -- which can be as small as 1 millimeter in diameter -- on or inside legitimate-se
eming correspondence; and even by using multiplayer gaming environments to share information.
```



Decode Image

4.1.2 Gray scale image:

```
:: Welcome to Steganography ::
1. Encode
2. Decode
1
Enter image name(with extension) : lena.png
Enter data to be encoded : Steganography is practiced by those wishing to convey a secret message or code. While there are m
any legitimate uses for steganography, malware developers have also been found to use steganography to obscure the transmiss
ion of malicious code.  Forms of steganography have been used for centuries and include almost any technique for hiding a se
cret message in an otherwise harmless container. For example, using invisible ink to hide secret messages in otherwise inoff
ensive messages; hiding documents recorded on microdot -- which can be as small as 1 millimeter in diameter -- on or inside
legitimate-seeming correspondence; and even by using multiplayer gaming environments to share information.
Enter the name of new image(with extension) : lena22.png
```

Input image

Encoded image

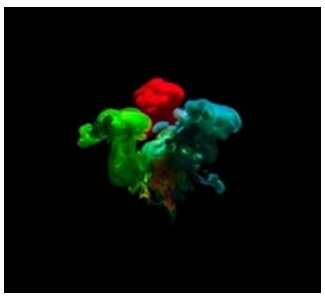
Decoded image

The size of the input image is 214 KB. The dimensions of the image is of 742*745. Width is 742 pixels and height is 745 pixels.

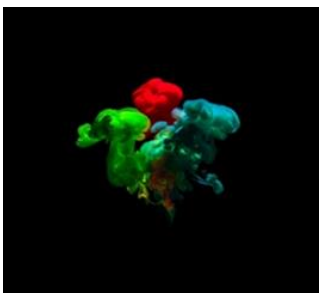
The size of the encoded image is 170 KB. The dimensions of the image is of 742*745.. Width is of pixels and height is of pixels.

4.1.3 Color Image:

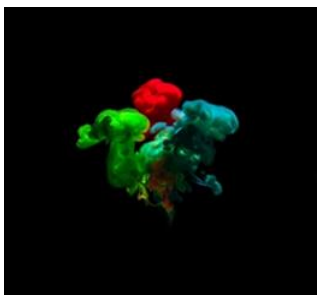
```
:: Welcome to Steganography ::
1. Encode
2. Decode
1
Enter image name(with extension) : color.jpg
Enter data to be encoded : Steganography is practiced by those wishing to convey a secret message or code. While there are m
any legitimate uses for steganography, malware developers have also been found to use steganography to obscure the transmiss
ion of malicious code.  Forms of steganography have been used for centuries and include almost any technique for hiding a se
cret message in an otherwise harmless container. For example, using invisible ink to hide secret messages in otherwise inoff
ensive messages; hiding documents recorded on microdot -- which can be as small as 1 millimeter in diameter -- on or inside
legitimate-seeming correspondence; and even by using multiplayer gaming environments to share information.
Enter the name of new image(with extension) : color22.png
```



Input



Encoded Image



Decoded Image

The size of the input image is 180 KB. The dimensions of the image is of 2500*2500 . Width is 2500 pixels and the height is 2500 pixels.

The size of the input image is 180 KB. The dimensions of the image is of 2500*2500 . Width is 2500 pixels and the height is 2500 pixels.

4.2 For audio:

Steps to hide secret information using LSB are:

a. Convert the audio file into bit stream.
b. Convert each character in the secret information into bit stream.
c. Replace the LSB bit of audio file with the LSB bit of character in the secret information.

Input:

The size of the input audio file is 336 KB. Input audio file taken is in real time form. Firstly we have taken the audio in real time, then have encoded the secret message onto the audio file.

Output:

The size of the output audio file is 336 KB.

References

1. PeiyaLiab KwokTungLob , “Joint image encryption and compression schemes based on 16 × 16 DCT”, Journal of Visual Communication and Image Representation,2018
2. K. C. Nunna and R. Marapareddy, "Secure Data Transfer Through Internet Using Cryptography and Image Steganography," 2020 SoutheastCon, 2020
3. K. Malathi, R. Kavitha and M. K. Liza ,"Pixel based method for Text to Image Encryption," 2020 4th International Conference on Electronics, Communication and Aerospace Technology (ICECA), 2020.
4. S. Gupta and R. Jain, "An innovative method of Text Steganography," 2015 Third International Conference on Image Information Processing (ICIIP).
5. S. D. Torvi, K. B. ShivaKumar and R. Das, , "An unique data security using text steganography," 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom), 2016
6. A. Darbani, M. M. AlyanNezhadi and M. Forghani, "A New Steganography Method for Embedding Message in JPEG Images," 2019 5th Conference on Knowledge Based Engineering and Innovation (KBEI), 2019
7. Anandaprova Majumder, Suvamoy Changder, A Novel Approach for Text Steganography: Generating Text Summary Using Reflection Symmetry, Procedia Technology, Volume 10,2013
8. Muhammad, Khan & Ahmad, Jamil & Farman, Haleem & Zubair, Muhammad. , A Novel Image Steganographic Approach for Hiding Text in Color Images using HSI Colour Model. Middle-East Journal of Scientific Research.
9. Jassim, F. A, “A Novel Steganography Algorithm for Hiding Text in Image using Five Modulus Method”, 2013.
10. Rasheed, Zainalabideen. Steganography Technique for Binary Text Image. International Journal of Science and Research 2013 (IJSR).
11. R. B. Krishnan, P. K. Thandra and M. S. Baba, "An overview of text steganography," 2017 Fourth International Conference on Signal Processing, Communication and Networking (ICSCN), 2017.
12. Chanu, Yambem Jina, Khumanthem Manglem Singh and Themrichon Tuithung. “A Robust Steganographic Method based on Singular Value Decomposition.” (2006).
13. Sirisha, B.. (2020). Image steganography based on SVD and DWT techniques. Journal of Discrete Mathematical Sciences and Cryptography.
14. A. Singh, H. Singh, “An Improved LSB based Image Steganography Technique for RGB Images”, IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT), 2015.
15. N. Akhtar, S. Khan, P. Johri, “An Improved Inverted LSB ImageSteganography”, Interational Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT), 2014, IEEE.
16. Deepesh Rawat, Vijaya Bhandari, "Steganography Technique for Hiding Text Information in Color Image using Improved LSB Method" M. Pooyan, A. Delforouzi, “LSB-based Audio Steganography Method Based on Lifting Wavelet Transform”, in Proc. 7th IEEE International Symposium on Signal Processing and Information Technology (ISSPIT 07), December 2007, Egypt.
17. Pooyan, A. Delforouzi, “LSB-based Audio Steganography Method Based on Lifting Wavelet Transform”, in Proc. 7th IEEE International Symposium on Signal Processing and Information Technology

18. Xuping Huang, Ryota Kawashima, Norihisa Segawa, Yoshihiko Abe. "The Real-Time Steganography Based on Audio-to-Audio Data Bit Stream".
19. Xuping Huang, Ryota Kawashima, Norihisa Segawa, Yoshihiko Abe International Conference on Intelligent "Information Hiding and Multimedia Signal Processing" © 2008 IEEE.
20. Dr. H S Prasantha, "NOVEL APPROACH FOR IMAGE COMPRESSION USING MODIFIED SVD", International Journal of Creative Research Thoughts (IJCRT), Volume 8, Issue 8, Page 2234-2243, Aug 2020
21. Dr. H S Prasantha, "IMPLEMENTATION OF IMAGE COMPRESSION USING FAST COMPUTATION OF SVD ON DM642", International Journal of Creative Research Thoughts (IJCRT), Volume 8, Issue 8, Page 2364-2368, Aug 2020
22. Prasantha, H, H Shashidhara, K N B Murthy, and M Venkatesh. "Performance Evaluation of H.264 Decoder on Different Processors." International Journal on Computer Science & Engineering. 1.5 (2010): 1768. Web. 7 Apr. 2013.
23. H. S. Prasantha, H. L. Shashidhara, and K. N. Balasubramanya Murthy. Image compression using SVD. In Proceedings of the International Conference on Computational Intelligence and Multimedia Applications, pages 143–145. IEEE Computer Society, 2007.
24. Gunasheela K S, H S Prasantha, "Compressive sensing for image compression: survey of algorithms", Proceedings of Emerging Research in Computing, Information, Communication and Applications, ERCICA, Springer publication, Bengaluru, 2018
25. K N Shruthi, B M Shashank, Y. SaiKrishna Saketh, H.S Prasantha and S. Sandya, "Comparison Analysis Of A Biomedical Image For Compression Using Various Transform Coding Techniques", IEEE, pp. 297-303, 2016