Data Confidentiality Using Discrete Wavelet Transform With Performance Outcome

[1]Mayuri Marathe, [2]Surabhi Tankkar

[1]Student, [2]Assistant Professor
M.E Electronics & Telecommunication Engineering,
Alamuri Ratnamala Institute of Engineering and Technology, Shahpur, Thane, India

***Abstract*: Digital communication has been an important a part of the infrastructure. Several applications are used nowadays, and it's necessary that the communication we have a tendency to create ought to be secret. To safeguard information from unauthorized access varied strategies for information concealment like cryptography, hashing, authentication are developed and square measure in observe these days. The explosive growth of net resulted within the want of security and also the confidentiality of the sensitive information as prime and supreme importance and concern therefore, security of knowledge ignored associate open channel has become a basic issue and thus, the confidentiality and information integrity square measure needed to safeguard against unauthorized access. This has resulted in unstable growth within the field of knowledge security. Varied strategies are developed to cover secret information. The digital image is one among the simplest media to store information. It provides giant capability for concealment secret data. Image secret writing and decoding may be a thanks to hide (the information|the info|the information) ineffective thanks to bring home the bacon data security. The initial image is retrieved solely by decoding.**

Index Terms: DWT, Wavelet in image processing, Encryption, Data hiding

1. INTRODUCTION

1.1 Background

The internet is used extensively as digital communication medium nowadays, for most of the applications. With extensive use of the internet, security is being a prime issue to maintain the confidentiality of the data with fast speed. An authentication provides the protection from the unauthorized access [1].

Digital communication has been an essential part of the infrastructure. To protect data from unauthorized access various methods for data hiding have been developed and are in practice today. Data hiding techniques provide the security to corporate, Government and Military communication. These techniques provide the knowledge to investigate and avoid the threats.

The transmission speed in digital communication is an important aspect. To increase the speed of the communication, compression is the best way. By compressing the size of data, faster transmission speed can be achieved. The wavelet transform is the best tool to compress the image. Various methods have been developed to hide the confidential data. Digital images are one of the best media to store data. It provides a large capacity for hiding confidential information. Image encryption and decryption is a way to hide the data in an effective way to achieve data security. The original image is retrieved by decryption.

Data hiding is the process in which data is embedded within the digital image with the help of cryptography. Digital image requires much storage, long transmission bandwidth and long transmission time. The wavelet transform is used to compress an image. It gives the four sub-images. Compressed sub-images are used to hide the data to ensure the security and hide the existence of the confidential data. Different confidential data can be embedded between the sub-images [1].

Cryptography is technology which converts the plain text to cipher text. It hides the existence of confidential data. Digital data is used as cover to cover the confidential data. Digital image is used as cover to carry or cover the confidential data, which is to be transferred with an authentication over the network.

The wavelet transform decomposes the medium image into four sub-images. An unauthorized access can be avoided by hiding the data within sub-images. Cryptography is an art of scrambling data into an indeterminate form. The confidential data is encrypted using simple Ex-Or operation. Confidential data is entrenched into sub-images. Thus, this technique hides the existence of confidential data. The data can be retrieved by decryption**.**

Our main objective is to apply wavelet transform on an Image, Encrypt the confidential data using cryptography, Hide the confidential message (either text message or an audio) into sub-images and check the quality of reconstructed or retrieved audio.

2. LITERATURE REVIEW

2.1 Data hiding techniques

With the advancement of technologies, the security is the main issue in the process of communication. In any form of communication, the terms like security, reliability, and robustness are a common issue. The extensive use of the internet for communication increases the challenges of security. Over global communication channels, people send sensitive personal information, corporate document, and financial transactions. In such scenarios; security, integrity, authenticity and confidentiality of digital data should be provided [3].

The data hiding is achieved by covering the data with cover or medium. The covering of data can be achieved in three ways i.e. Data within an Image, Data within Video & Data within an Audio
Cover or medium used can be image, video or audio.

The confidential data is converted into a different form using different techniques. Three different data hiding techniques are i.e. Steganography, Watermarking & Cryptography

2.2 Components of Cryptography

- Plain text: It is the original data which should be protected during transmission
- Encryption algorithm: It is an algorithm which converts any plain text into cipher text with the help of encryption key.
- Cipher text: Cipher text is generated with the help of an encryption algorithm. It is also called as scrambled version of a plain text.
- Decryption algorithm: Decryption algorithm reverses the encryption algorithm. It is a process of converting cipher text into plain text with the help of decryption key.
- Encryption key: It is the key which converts the plain text into cipher text. It is embedded with the use of an encryption algorithm. This is known to the sender.
- Decryption Key: Decryption key can be different at decryption stage. These are not identical always. This key is known to the receiver. With the help of known key and decryption algorithm, plain text can be computed or retrieved.

2.3 Modern Cryptography

Modern cryptography deals with the binary bit sequences. It relies on publicly known mathematical algorithms for coding the information. Secrecy is obtained through a secret key. The computational difficulty of algorithms, the absence of the secret key, etc., make it impossible for an attacker to obtain the original information even if he knows the algorithm used for coding. The types of modern cryptography are

- Block cipher algorithm: In this scheme, a binary text is treated in block size. Block size is fixed upon the no of bits.
- Stream cipher algorithm: In this scheme, plain text is treated as one bit at a time. Technically stream cipher is block cipher with a block size of one bit. In this algorithm, a one-bit plain text is taken and encryption is performed. The simple Ex-OR operation is also used under stream cipher algorithm. It processes each bit of the plain data by bitwise Ex-OR operation with an encryption key.

2.4Selection of Cryptography

It provides the security services as confidentiality and an authentication. A simple stream cipher algorithm that is Ex-OR operation is used for the cryptography. The data is not getting hidden as plain text. The wavelet transform is used to get the sub-images. The sub-images give the approximation, Horizontal, vertical and diagonal details, in which horizontal, vertical and diagonal are in little scramble form. Data is hidden within these sub-images.

Thus even if an image is received by an unauthorized person he cannot recognize the existence of the data within that image. It will be treated as a distorted or noisy image [3].

2.5 Wavelet Transform

The decomposition of a function when a time perspective is preferred in addition to information about frequency content is called time-frequency analysis. The wavelet transform is a useful tool for time-frequency analysis. The STFT “time-frequency window” is replaced by a “time-scale window” with similar properties, but some important differences.

Wavelets are becoming a popular tool in image processing. In discrete wavelet transform, the signal is passed through filters. The filter used is low pass filter and high pass filter, which separates out the details of an image. The sub-images are achieved by applying wavelet transform to the medium image. It is multi-resolution transform [4].

3. WAVELET TRANSFORM

Wavelet theory is an extension of Fourier theory in many aspects and it is introduced as an alternative to the short-time Fourier transform (STFT). The wavelet transform provides the time and frequency resolution. The mother wavelet is translated and scaled to get the resolutions

3.1 Wavelet in image processing

Wavelet is used in image processing that provides a multi-resolution decomposition of an image and results in a non-redundant image representation. The basis is called wavelets and these are functions generated by translation and dilation of the mother wavelet. The scaling and translation are achieved by the help of wavelet filters.

In wavelet analysis the signal is decomposed into scaled (dilated or expanded) and shifted (translated) versions of the chosen mother wavelet or function. A wavelet as its name implies is a small wave that grows and decays essentially in a limited time period. A wavelet is a small wave; it has to satisfy two basic properties

1. Time integral must be zero.

$$\int_{-\infty}^{\infty} \psi(t)dt = 0$$

2. Square of wavelet integrated over time is unity.

$$\int_{-\infty}^{\infty} \psi^2(t)dt = 1$$

The basis is obtained by translation and dilation of the mother wavelet as:

$$\psi_{a,b}(t) = \frac{1}{\sqrt{|a|}}\psi((t-b)/a)$$

Where,
a= dilation factor (Low-pass filter)
b=translation factor (High-pass filter)

Different wavelet filters are used to translate and scale the mother wavelet. Convolution with scaling or dilating factor is a low-pass filtering operation and convolution with translation or shifting factor is a high-pass filtering operation.

The discrete wavelet transform (DWT) is considerably used in the field of image processing due to its flexibility in representing non-stationary image signals and its ability in adopting to human visual characteristics. The wavelet representation provides a multi-resolution/multi-frequency expression of a signal with localization in both time and frequency. The video is the sequence of frames which are still images. Still, images are considered as 2-D signals. The single dimension transform is more efficient than an equivalent 2-D transform. Wavelet transform applied to such signals is done by using the 1-D transform version, that is applying it to the still image in both row-order and column-order. 3-D transform of video introduces the delay in the system [2].

3.2 Two Dimensional (2D) wavelet decomposition

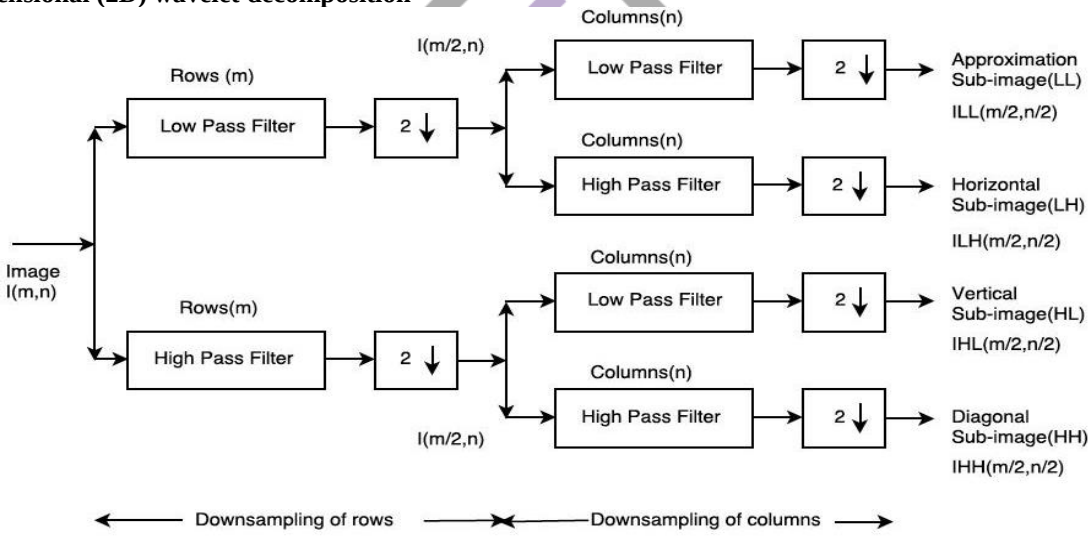

Figure 3.1: Two-dimensional wavelet decomposition

Wavelet separately filters and down samples the 2-D data (image) in the vertical (column) and horizontal (rows) directions. The rows of an input (source) image are I (m,n) filtered by low pass filter and high pass filter in a vertical direction and then down sampled by a factor of two (keeping the alternative sample). It divides the image vertically into two sub-images, upper part as average coefficients (I_{LL}) and lower as a horizontal detailed coefficient (I_{LH}). In the horizontal direction, columns of an image are filtered. It results in two more sub-images as a vertical detailed coefficient (I_{HL}) and diagonal detailed coefficient (I_{HH}).

The I_{LL} contains the average image information corresponding to a low-frequency band of multi scale decomposition. It could be considered as smoothed and sub sampled version of the source image I (m,n). It represents the approximation of source image I (m,n). I_{LH}, I_{HL} and I_{HH} are detailed sub-images which contain directional (horizontal, vertical and diagonal) information of the source image I(m,n), due to spatial orientation. Multi-resolution could be achieved by recursively applying the same algorithm to low pass coefficients from the previous decomposition [5].

There are many wavelets being used now a day for decomposition of signals and images. The main types/families are Daubechies, biorthogonal, coiflets, symlets and dmey.

1. Daubechies Wavelet: These compactly supported orthonormal wavelets. Daubechies wavelet transforms are defined in the same way as the Haar wavelet by computing running averages and differences through scalar products with scaling signals and wavelets. For high order Daubechies wavelets DbN, N denotes the order of wavelet and the number of vanishing moments.
2. Biorthogonal Wavelets: These are compactly supported wavelets for which symmetry and exact reconstruction is possible with FIR filters. The types are bior1.1, bior1.3, bior1.5, bior2.2, bior2.4 …etc. [6].

3.3 Inverse wavelet transform

Inverse 2-D wavelet transform is used to reconstruct the image I (x, y) , from sub-images I_{LL}(x , y) , I_{LH} (x , y) , I_{HL}(x , y) and I_{HH}(x , y). This involves column up sampling and filtering using low pass L and high pass filter H for each sub-images. Row up sampling and filtering with low pass filter L and high pass filter H of the resulting image and summation of all matrices would construct the image I (x, y)[7].

4. ENCRYPTION OF DATA USING CRYPTOGRAPHY

4.1 Encryption & Its Algorithm

Security of the confidential data is the main aspect. Encryption means conversion of plain data in cipher code or data. Plain data is the original data. Cipher code is the converted data which is meaningless and can't be read. It is nothing but the scrambled data.

Encryption is done with the help of encryption algorithm. An encryption algorithm makes the use of a key. The plain text is converted to the cipher code with the help of this key. The key is generated randomly every time. Stream cipher algorithm of simple Ex-OR operation is used for encryption of the confidential data. For Encryption process the plain text and encryption key should be of identical size [3].

Steps in Encryption algorithm are such as Get the confidential data, Generate the random key of the same size, Bitwise Ex-OR the confidential data with a random key, Get the cipher code.

4.2 Decryption & Its Algorithm

Decryption is a reverse process of an encryption. Here, the same key is used to decrypt the encrypted data. The confidential data can be recovered only if the key is known. The key is Ex-OR with the cipher code to get the confidential data back.

Steps in Decryption algorithm are Get the encrypted data, Get the same random key of the same size, bitwise Ex-OR the encrypted data with a random key, Get the plain data.

4.3 Data Embedding within Image

The cipher code is covered with medium or cover image. This ensures the security of the data. The cipher code is embedded within an image with Ex-OR operation. No key is required. An image size plays an important role in data hiding key generation. According to matrices rules to perform any logical operation on it, sizes of the both matrices should be same. The encrypted data is embedded within an image, thus the size of data hiding key is same as image size. The confidential data is encrypted using encryption algorithm. The Ex-OR operation is performed on encrypted data and image to embed the data within an image [1].

4.4 Ex-OR operation Rules

The Ex-OR operation is getting performed on matrices. Thus it has to follow some rules of matrices

1. Data type of matrices should be same.
2. Matrices should be identical.

5. PROPOSED METHOD FOR DATA HIDING

5.1 Flowchart for hiding & retrieving text in an Image

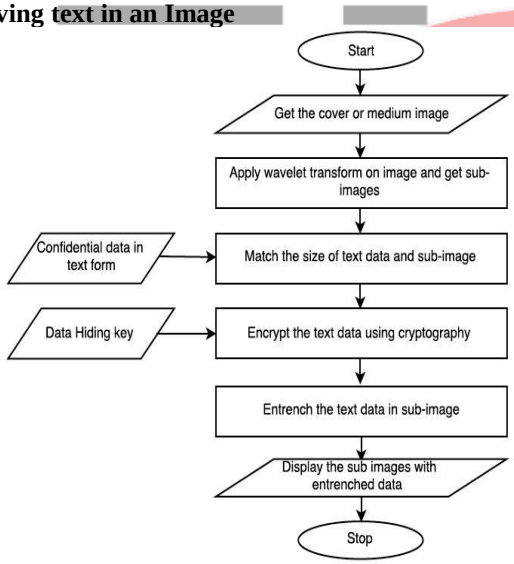

Figure 5.1(a): Flowchart for hiding text data

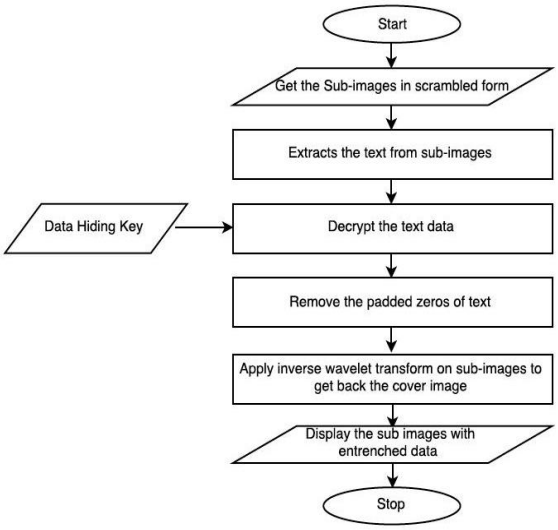

Figure 5.1(b): Flowchart for retrieving text data

An image is a 2D signal. 1D transform is applied as it is better than 2D transform. 1D transform avoids the delay. The wavelet transform is applied on the image to get sub-images. The data is encrypted with the help of encryption algorithm. An encrypted confidential data is hidden inside the sub-images after, the data is encrypted as per the size of sub-images. Thus the size of an encrypted data, sub-images and encryption key are identical.

Get back the sub-images with scrambled form. The confidential data can be extracted sub-images. Decryption of the confidential data is done with same data hiding key. Padded zeroes are removed to get back an original size of confidential data. An inverse wavelet transform is applied on the sub-images to get back the cover image [1].

5.2 Flowchart for hiding & retrieving audio message/samples

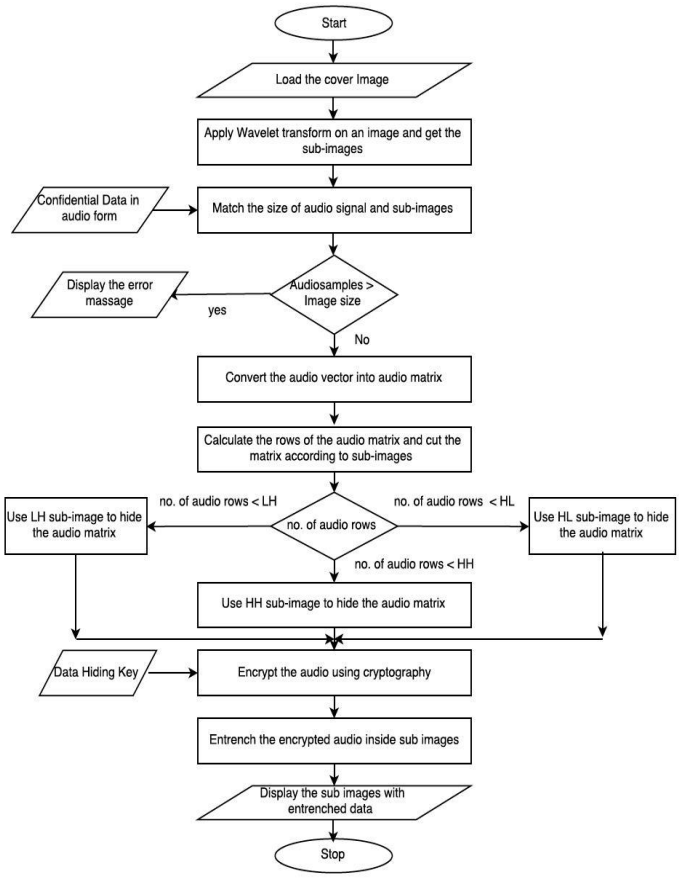

Figure 5.2(a): Flowchart for hiding audio samples

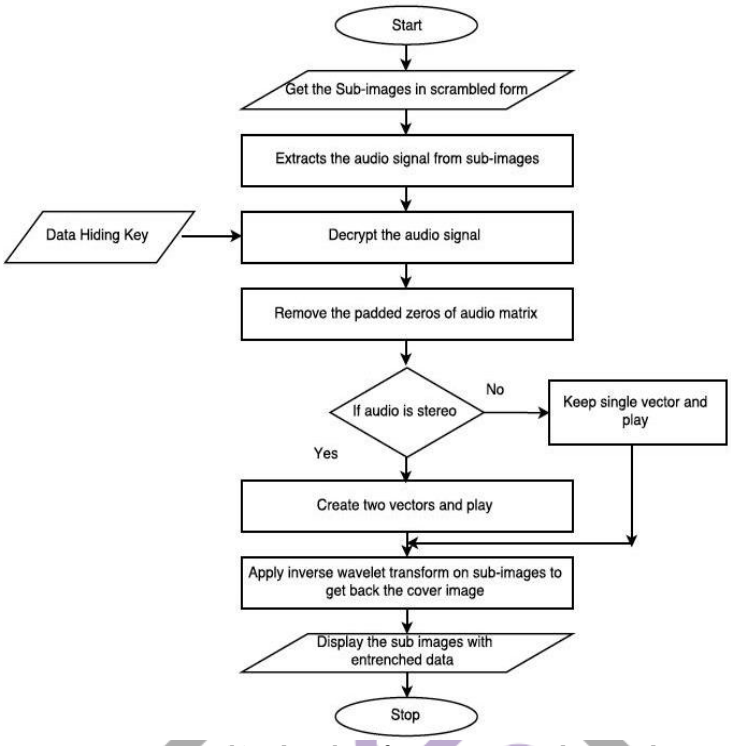

Figure 5.2(b): Flowchart for retrieving audio samples

An audio is nothing but the vector of samples. The samples of an audio are large in numbers. The wavelet transform is applied to cover image. Read the vector of an audio signal. Convert the vector into the matrix with columns numbers equals to the sub-image columns, to match the sizes of sub-images and an audio signal. Calculate the samples of an audio signal, if samples are greater than thrice of sub-image size display the error message. Selection of sub-image is depending upon the rows of an audio matrix. Hide the audio within LH sub-image if rows of an audio matrix are less than rows of sub-image. LH and HL sub-image are used when rows are less than twice of sub-image rows. When rows are less than thrice of sub-image rows, hide audio within three sub-images (LH, HL, and HH). LL is kept untouched to ensure the high PSNR and less MSE.

An audio signal is extracted from scrambled sub-images. An audio signal is decrypted using same data hiding key. The original vector of an audio signal is retrieved as per the type i.e. Mono or Stereo. The cover image is reconstructed by applying an inverse wavelet transform on sub-images.

6. SIMULATIONS AND RESULTS

Simulation is processed on MATLAB 2018b. Different images have been used as a medium image. The wavelet transform is applied on the images to get the sub-images. These sub-images are used to embed the cipher code. Simulations steps are

1. Apply wavelet transform on medium image
2. Encrypt the confidential data
3. Hide the encrypted data
4. Decrypt the data
5. Apply inverse wavelet on image
6. Calculate the reconstruction quality metrics

The image is used as cover. Two approaches have been developed for data hiding i.e. Text data within an image and Audio data within an image

6.1 Text Data within an Image

Text data is nothing but the vector of integer value of characters. This vector is converted to the matrix. The size of this matrix is same as sub image by padding zeroes to the vector of text data. It helps in encryption of data. Data hiding key is also the of same matrix size to satisfy the matrix operation rules.

Figure 6.1: Original image

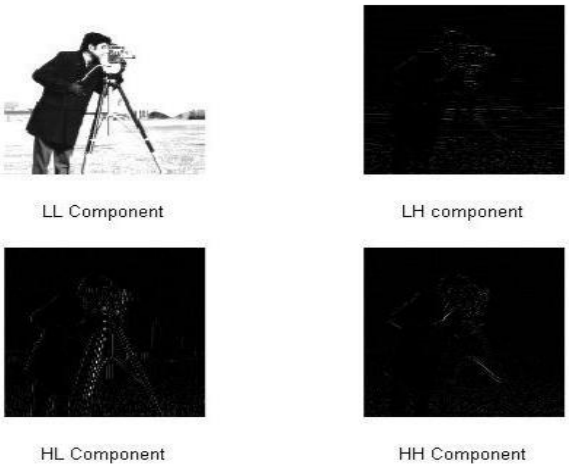

Figure 6.2: Wavelet decomposition

Figure 6.1 shows the original image. DWT is applied to the original image results in four sub-images. They are LL, LH, HL and HH sub-images. Figure 6.2 shows the sub-images of the original image. The 'bior 5.5' wavelet is used for the decomposition.

Figure 6.3: Input screen is added to type the confidential data

Input screen for entering the confidential data is shown in figure 6.3. The character length of this input dialogue box can be defined. Here the length is 100 characters.

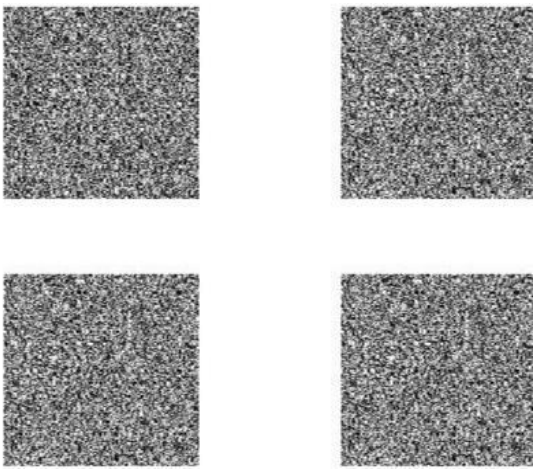

Figure 6.4: Sub-images with data embedded

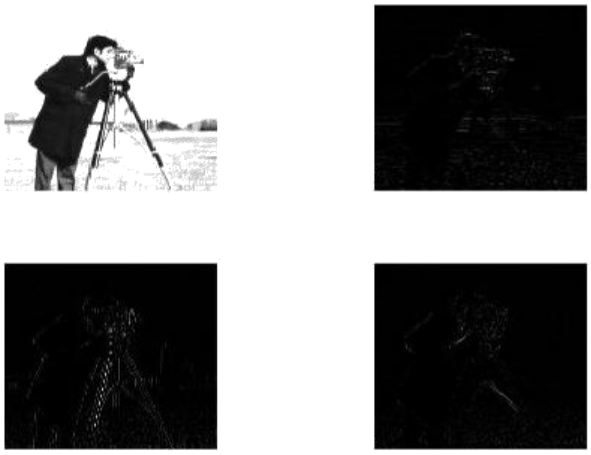

Figure 6.5: Extraction of sub-images and encrypted data

Cryptography converts the plain data into the scrambled form. The encrypted data is in a scrambled matrix form. This is embedded inside the sub-images with the Ex-OR operation. Thus sub-images of figure 6.4 is in scrambled form, which looks like distorted images. Thus providing authentication and confidentiality security services by means of cryptography.

Extraction of the sub-images and encrypted data is done at the receiver side. It gives back the original sub-images and encrypted data. The decryption is done with decryption algorithm. It is the reverse process of an encryption. The same key is used for symmetric key encryption. The message box is used to display the decrypted message. Figure 6.6 shows the retrieved data on the message box.

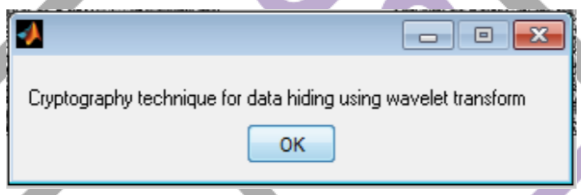

Figure 6.6: Retrieved confidential data

Figure 6.7: Retrieved/Reconstructed image

Figure 6.7 shows reconstructed image. The inverse wavelet transform is applied to the sub-images to get back the original image. The inverse wavelet transform uses the same wavelet. The reconstructed image is blurred in quality. Thus some modifications have been developed.

6.2 Effect of wavelet on image

The basic idea of application of wavelet transform is filtering image that is a 2D signal by low pass filter and high pass filter. Low pass filter passes the low frequencies and high pass passes the high frequencies. This is done by the down sampling or up sampling of the image. According to the Nyquist, only half of the frequency samples are enough for faithful reconstruction of the original image. Wavelet reduces the redundancy of the image. Compression of the image totally depends on the image redundancies. Thus, approximated coefficients at first level decomposition carry the most of the information.

6.3 Quality of an audio

The wavelet transform is an invertible transform. After the decryption of an image, an inverse wavelet is applied to get a cover image. The quality of a retrieved audio can find out using quality metrics. The Mean square error (MSE) metric used to compare audio compression quality [12]

6.4 Audio Samples

An audio is a vector of samples. The values of these samples are in floating points. The values of these vectors could be the millionth of any value. As this algorithm makes use of Ex-OR operation, as per the rules it should be signed integers. Thus to convert the floating points in signed integers scaling has been performed on the audio vector. Scaling does not affect the reconstruction quality metrics.

While performing scaling on audio vector it was a challenge to get signed integers, as the vector has the millionth of any value The image used to hide an audio is in the int8 data range. Thus scaling by thousand gave magnified version of an audio and scaling by ten thousand gave distorted audio as it was exceeding the data type range.

6.5 Scaling of audio samples in into data type

It gives the integer value if it is scaled by ten thousand. Scaling other than ten thousand changes the original audio quality, either it magnifies or degrades or distorts the audio quality at the receiver.

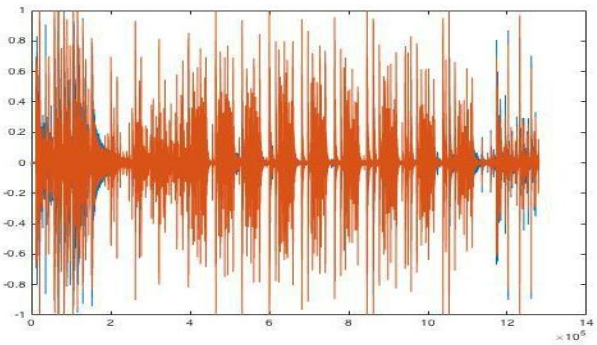

Figure 6.10: Original audio Samples

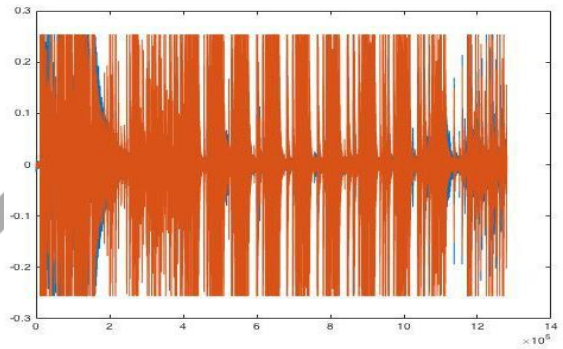

Figure 6.11: Retrieved audio samples when scaled by five hundred (Magnified version)

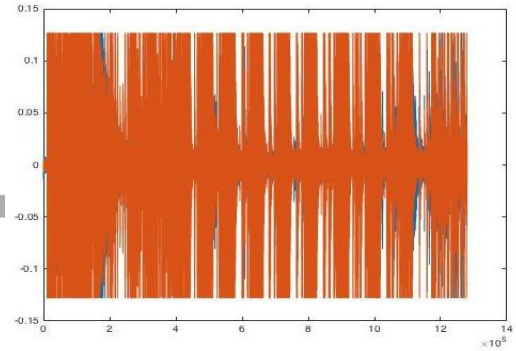

Figure 6.12: Retrieved audio samples when scaled by Thousand (Magnified version)

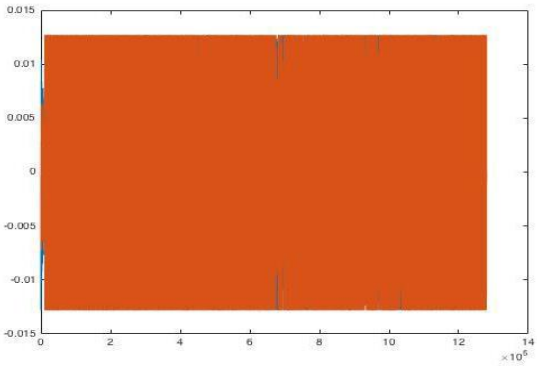

Figure 6.13: Retrieved audio samples when scaled by ten thousand (Distorted version)

Figure 6.11, 6.12 and 6.13 shows the retrieved audio when scaled at different values. Scaling of audio with some hundreds of value gives the magnified version of the audio as shown in figure 6.11. Figure 6.12 and figure 6.13 shows the scaling is in the range of thousands of the actual value, causes distortion in the audio. Scaling by thousands and above crosses the range of int8 data type. Thus introduces the distortion in the retrieved audio.

Thus to resolve the problem associated with scaling of an audio data type of audio and image has been changed. Instead of int8 data type, int16 has used. It results in signed integers for the millionth of values also. As the data type has changed, the range is increased.

6.6 Scaling of audio samples in int16 data type

It gives the integer value if it is scaled by ten thousand. Scaling other than ten thousand changes the original audio quality, either it magnifies or degrades or distorts the audio quality at the receiver.

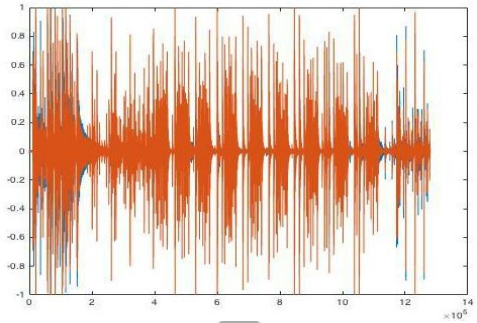

Figure 6.14: Retrieved audio samples when scaled by ten thousand (Exact replica of original samples)

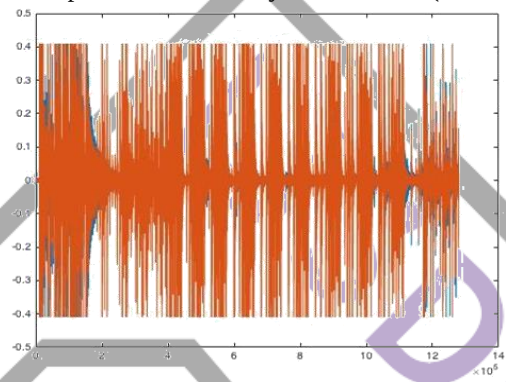

Figure 6.15: Retrieved audio samples when scaled by eighty thousand (Magnified Version)

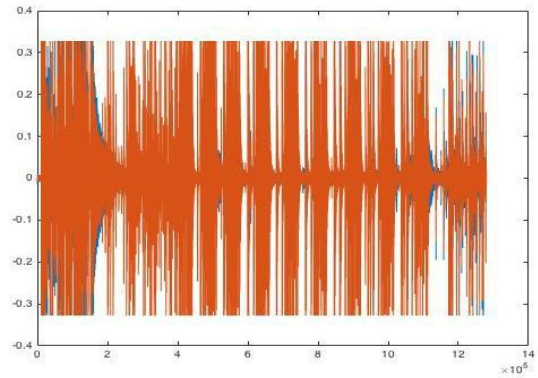

Figure 6.16: Retrieved audio samples when scaled by one lakh (Magnified Version)

The magnified version of the audio samples is retrieved when scaled above ten thousand values. Figure 6.15 and figure 6.16 shows the magnified version of the audio samples. Ten thousand is the perfect value in int16 data type to get the original audio samples back when retrieved. Thus figure 6.14 shows the actual retrieved audio samples.Int16 data type and ten thousand values for scaling are chosen to get the perfect and original quality of audio samples.

6.7 An audio samples within sub-images.

Int16 data type and scaling of audio samples with ten thousand values gives the original audio samples when retrieved. Recorded audio can be hidden inside the sub-images as per the rows of an audio matrix. The simple Ex-OR operation is used to embed the audio signal inside sub-images.

Figure 6.17: Original Image

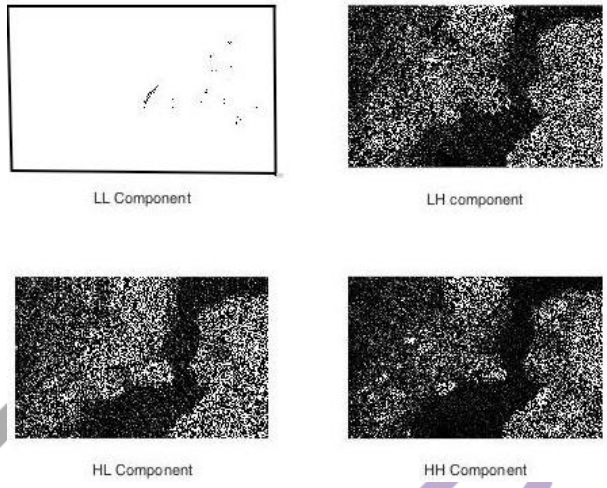

Figure 6.18 Wavelet decomposition of an image (Four sub-images)

Figure 6.17 shows the medium image used to hide the audio signal. An audio sample is the vector of floating points. An audio can be mono or stereo. Mono contains one vector and stereo contains two vectors.

The wavelet transform is applied on the image to get four sub-images. To improve the reconstruction quality metrics an approximated sub-image is transferred as intact. As per the proposed method audio samples are converted to a matrix with column size fixed as per the sub-image columns. According to the size of an audio sample, it is cut as per the sub-images size and entrenched within the sub-images. Audio samples can be accommodating within either horizontal (LH) or vertical (HL) or diagonal (HH) sub-images as per the matrix size. Figure 6.18 shows the sub-images of the image.

An audio can be selected as per the choice. An audio samples size decides the sub-images. If the size of an audio samples is greater than quadruple of sub-image it will display the sample size error message indicating audio samples are greater than the available space.

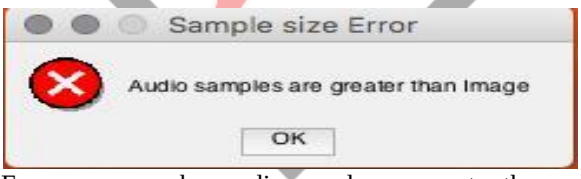

Figure 6.20: Error message when audio samples are greater than available space

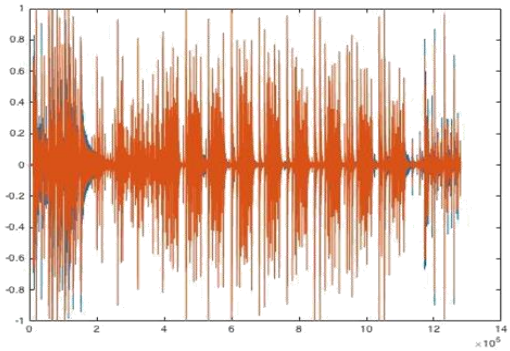

Figure 6.21: Original audio signal when it is less than available space

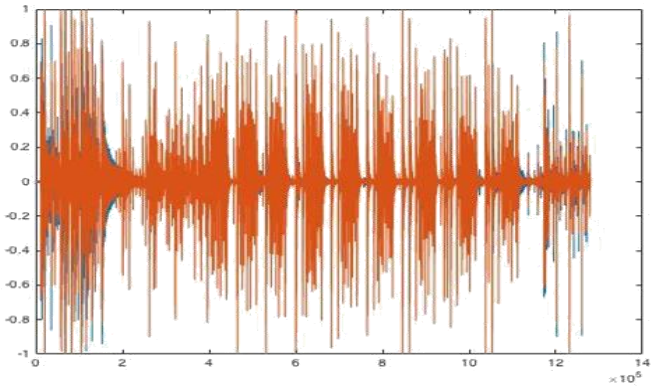

Figure 6.23: Reconstructed audio samples

Audio samples (song) has been reconstructed along with the image. Figure 6.23 shows the reconstructed audio samples which are an exact replica of figure 6.21. The exact replica of audio samples is achieved because of proper scaling and data type used.

6.8 Benefit of sub-images for audio samples

The wavelet transform provides four sub-images. An approximated sub-image is kept untouched. Remaining three sub-images is used to hide the audio. Basically, an audio is a vector which could be stereo or mono. The length of these vectors is so large with its large duration.

The sub-images are half of the size of the original image. This provides twice size to hide audio with security.

As the data, hiding is the main motto we are using all the sub-images. Neglecting the reconstruction of an original image or quality of the reconstructed image, we are using all the sub-images.

Actual size of the image = 1600 X 2560
Size of sub-image = 808 X 1288
Total size available to hide an audio = 4 X sub-image size
An audio smaller than quadruple of sub-image could be hidden inside the sub-images.

6.9 Audio quality metrics

Scaling of an audio gives the integer value for floating points. Change in the data type gives the rounded integer value. Thus while retrieving back the floating points are rounded to the next value, causes the change in the actual audio sample values. It introduces the error.

An audio is only being processed to accommodate it within the image. Thus the error introduced is minor. No compression of an audio is taking place in processing. The aim of finding the MSE of retrieved audio is to find out the difference between the original audio and reconstructed audio.

Table 6.1: MSE value of reconstructed audio

Audio file name	MSE	Samples	Sample Rate (Fs)
Taal.mp3	0.008	1117440×2	44100
Water_drop.mp3	4.00E-06	249974×2	44100
Zakir.mp3	0.0027	1279827×2	44100
indiantabla.mp3	0.0791	1436191×2	48000
Oh everything is alight.wav	2.12E-04	84885×2	48000

Table 6.1 shows the MSE value for various reconstructed audios. All audios are stereo in nature. As shown in the table the MSE is less for all the reconstructed audios.

7. CONCLUSIONS

Wavelet is applied to image successfully. Four sub-images can be used for data hiding. Application of wavelet on medium image increases the memory size, which can be used to accommodate an audio within it.

Confidential data can be of text data or audio signal. Audio signal has been hidden and retrieved successfully. The maximum size that can be entrenched inside the image is quadruple of sub-image. The quality of an audio signal is good as only scaling has been performed on an audio vector. MSE is low because of the less processing of an audio. Thus the quality of the reconstructed audio is good.

Data embedding of confidential data in the form of text was successful. Data is fully recovered along with an image.

8. FUTURE SCOPE

The proposed method is restricted to the size of an Image. An audio signal of long duration cannot be hidden inside an image due to the sampling rate. Audio samples should be less than image matrix (4*sub-images). Thus future scope of this approach can be

1. The hiding of the compressed long duration audio samples within the image.
2. The hiding of long duration audio samples without compression within the video.

REFERENCES

[1] M. P. Uddin, M. Saha, S. J. Ferdousi, M. I. Afjal and M. A. Marjan, "Developing an Efficient Solution to Information Hiding through Text Steganography along with Cryptography," in The 9th International Forum on Strategic Technology (IFOST), Bangladesh, 2014.

[2] G.Suresh, Dr.K.A.Parthasarathi "Data Hiding Approach Based on Stationary Wavelet Transform" IEEE Conference Number – 33344 July 8, 2014, Coimbatore,India

[3] Rintu Jose and Gincy Abraham, "A Separable Reversible Data Hiding in Encrypted Image with Improved Performance" International Conference on Microelectronics, Communication and Renewable Energy (ICMiCR-2013).

[4] Wang, W. J., Huang, C. T., & Wang, S. J. (2011). VQ applications in steganographic data hiding upon multimedia images. Systems Journal, IEEE, 5(4), 528-537.

[5] SmitaBorse Data Hiding in Encrypted Images Using Transpose Based Reserving Room before Encryption & Discrete Wavelet Transform , Proceedings of the International Conference on Intelligent Sustainable Systems (ICISS 2017)IEEE Xplore Compliant - Part Number:CFP17M19-ART, ISBN:978-1-5386-1959-9

[6] G. Prashanti, Information Technology, Vignan's Lara institute of Technology and Science, Guntur, India. "Data Confidentiality using steganography and cryptography techniques" 2017 International Conference on circuits Power and Computing Technologies [ICCPCT]

[7] Hemalatha S, U. Dinesh Acharya, Shamathmika, Department of Computer Science and Engineering Manipal Institute of Technology, Manipal, University Manipal, India MP4 Video Steganography in Wavelet Domain

[8] Karen Lees, "Image Compression Using Wavelets", May 2002.

[9] Javed Akhtar, Dr Muhammad Younus Javed, "Image Compression with Different Types of Wavelets", International Conference on Emerging Technologies Peshawar, Pakistan 13-14 November 2006.

[10] Sourabh ChandraAssistant ProfessorDepartment of Computer Science&Engineering, Calcutta Institute of TechnologyKolkata, India A comparative survey of symmetric and asymmetrickeycryptography2014 International Conference on Electronics, Communication and Computational Engineering (ICECCE)

[11] Wei Sun, Rong-Jun Shen, Fa-Xin Yu and Zhe-Ming Lu* "Data Hiding in Audio Based on Audio-to-Image Wavelet Transform and Vector Quantization" 2012 Eighth International Conference on Intelligent Information Hiding and Multimedia Signal Processing