IMPACT: International Journal of Research in Engineering & Technology (IMPACT: IJRET)
ISSN (P): 2347-4599; ISSN (E): 2321-8843
Vol. 4, Issue 6, Jun 2016, 65-76

IMPLEMENTING DATA HIDING BY USING AUDIO AND COMPARING DIFFERENT MEDIUMS USED IN STEGNOGRAPGY

SHARANJEET SINGH, AMARDEEP SINGH & SHRUTI

Department of Computer Science, Guru Nank Dev University, Gurdaspur, India

ABSTRACT

Whenever we talk about secret information, then in that case confidentiality plays a vital role in between communicating parties. Cryptography and Stegnography are the two main pillars of information security. Cryptography is used just to scramble the information by apply various algorithm e.g Deffie - Hellmen etc, but it is able to reveal secret information: that eavesdropper will come to know that this specific information will contain some confidential data. But Stegnography is completely opposite to it. It simply hide the content, In it only sender and receiver will come to know about the confidential information. Now, in this research article We will show that how an audio message will secretly hides confidential data and send it over a medium without a man in the middle will come to know about it: by using Coagula by sender to embed the message in audio and Sonic Visualizer by receiver for decoding purposes. The message which is to be send it can be audio, video, text, image and etc, but here we concerned about image which contain secret information. When image is embed in audio signal then it become stego-signal. In it quality of audio does not suffer because quality is checked twice before and after the extraction of secret message. Quality of stego-image is measured by peak signal to noise ratio(PSNR), Structural Similarity Index Metric(SSIM), Now extracted image is measured by Signal to noise ratio(SNR) and Squared Pearson correlation coefficients(SPCC). Both the quality measures will show good results.

KEYWORDS: Information Security, PSNR, SSIM, SNR, SPCC, Coagula, Sonic Visualizer

INTRODUCTION

In these days Information Security is the biggest challenge for researchers. Though with cryptography we can achieve this challenge but it is not able to make invisible: every possible thing so, we use Stegnography which makes secret message invisible to the hacker. Stegnography is implemented by 3 techniques such as Temporal Domain, Transform Domain [7] and Hybrid Domain. But in this paper we worked on Transform domain technique because as we are concern with the audio message. In it we focused on frequency at a particular time so basically f (t) that is function of time plays a vital role while sending audio message. So, under transform domain Pitch Transformation method is used to measure frequency at any particular time. Instead of using Transform domain we can also switch to FFT which is Fast Fourier Transform but the major drawback of FFT is that it is not able to provide information about specific time and in audio signal time is very important. In Temporal domain the actual value is to be manipulated with this we didn't come to know about the coefficients. But in transform domain, it is further manipulated by different other domains like frequency domain [8,9,10,11,12] so that We come to know about the coefficients in which audio message is to be hidden. Hybrid Domain is rarely used because it is prone to attacks, because when we embed message in cover image then: it simply lose its quality and when it losses then any one can come to know about the confidential information.

We can hide audio, image, text, video and etc. As per our observation, generally secret image or text is to keep hidden in cover image and that image when it reached on its destination then it become stego-image because it contain hidden message. After implementation, We observe that the image on sender and receiver is same but the difference is in size like as you can see the cover image is of 4.70KB and the stego-image which contain hidden image (message) its size is 42.0KB. With this implementation we admit to say that stegnograpgy is better than cryptography because a lay man cannot identify the difference between these two images.

Implementation of Stegnography by Hiding Image Message

There are various steps to hide image in a cover image by using "Invisible Secret tool"

Step: 1 Firstly select the cover image as shown in figure 1 in which we need to hide secret message.

Step: 2 Now use Invisible Secret tool and in it we need to select the type of action in figure 3(b).

Step: 3 Now Browse the Carrier file or cover image which is shown in figure 1.

Figure 1: Cover Image in which Meassgae is to be Hidden(4.70 KB)

Figure 2: Message which Kept to be Hidden form Eavesdropper

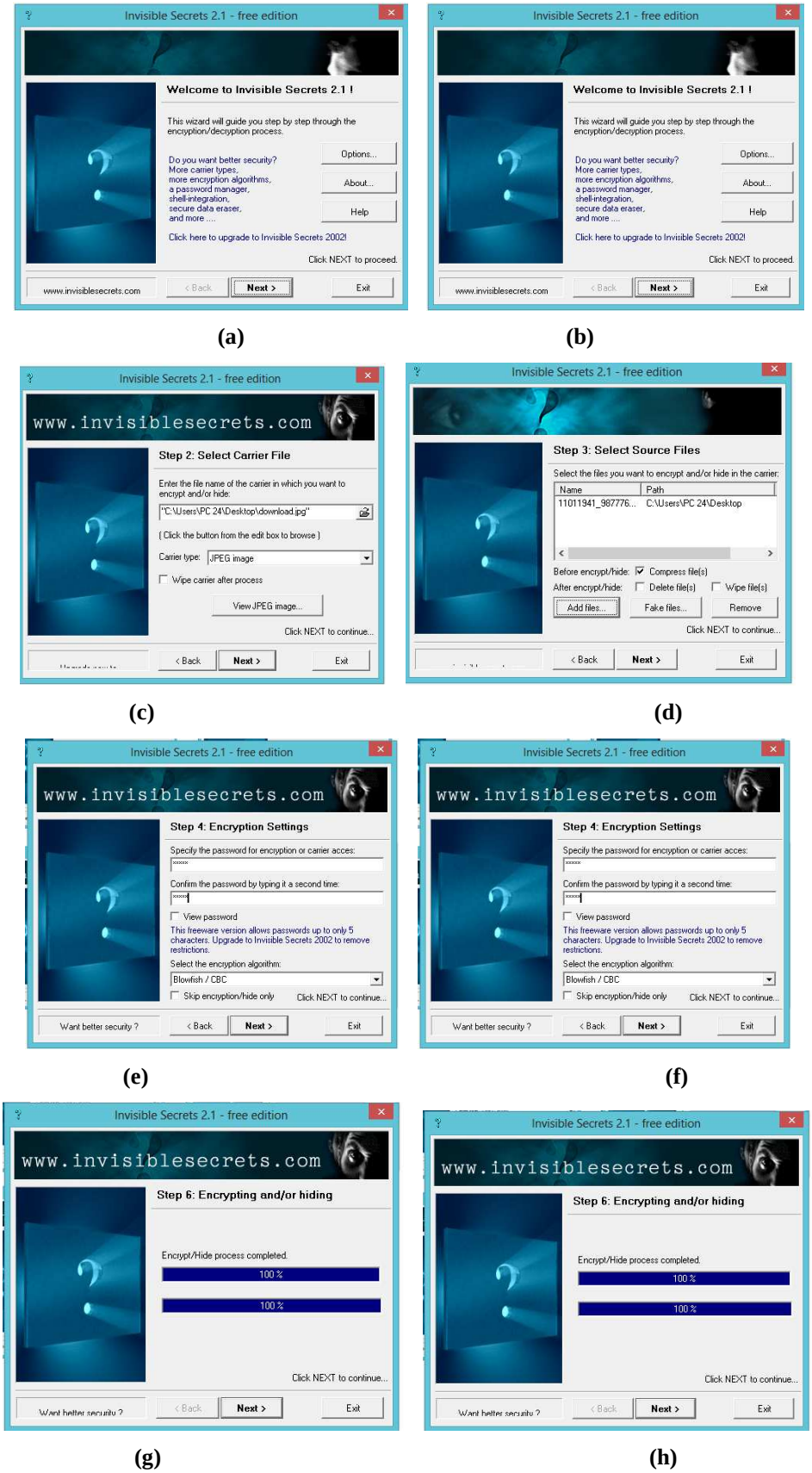

Figure 3: Implementation Process that how Stegnography Exactly Hide the Content

Figure 4: Stego Image in which Secret Message is to be hidden (Its size is 42.0 KB)

Step: 4. Now browse the message which is to be hidden or embed in the cover image like in figure3 (d).

Step: 5. Choose password to make it secure twisely and confirm it also by entering password again in figure 3(e).

Step: 6. Now give some name to the image file and click to finish button (figure 3(f)) to complete the process.

Step: 7. At last same image file is appeared and visually it does not make any difference as shown in figure 4.

Pitch Transformation

In pitch transformation, some functions are selected and those values are non-zero in small intervals to explore the properties of f(t).Now same way it is further translated in other intervals of time. There are various kinds of pitch which are discovered and one of the simplest is: Faar Pitch. Information that is produced in real life is absolute i.e it come in some numbers not in functions. When some data is integer then to map we require Integer Pitch transformation.

Most popular cover images are colored images and gray-level images. Now a days, colored images are mostly used as comparative to gray level because in gray level we deal with different intensity of only two colors i.e black and white but in colored we deal with different intensities of three colors i.e red, green and blue. In colored sometimes we deal with HUV also. Color image stegnography is done by color image domain which is used to generate the 3-levels of corresponding coefficients so that it is easier to hide the message in them.

In this paper we are concerned with audio signal and it is analog: So message is in audio and it is hidden in digital media i.e image so for analog to digital periodically sampling is required. Audio signal can be of.wav or MP3 but normally we use.wav because it does not require pre-processing. Audio Signal consist of various tracks and those tracks are further consist of 4096 bands and these are divided in two parts of 2048 each. On these divides sub-parts some filters are being applied to enhance the quality of an image.

When Pitch transformed is applied on some image then it decomposed into four sub-parts Low-Low, High-Low, Low-High and High-High. Low-Low consists with approximation coefficient. Out of all the sub-bands only low-low contains significant features.

Peak Signal to Noise Ratio

Peak Signal to noise ratio is given by:-

$PSNR=10* \log_{10} {}^{MAX}/_{MSE}$

Where, MAX indicates the maximum value of the pixel e.g 255 and MSE indicated Mean square error between original image and stego-image.

MSE=1/M*N[ε(i=1 to M) ε(i=1 to N) |O(i,j) D(i,j)|]

Where, O (i,j) is original and D(i,j) if os stego-image.

Higher the value of PSNR better will be the quality of the image. It is measured in decibel (db).

Structural Similarity Index Metric

It is an objective image quality and it is superior to other measures. PSNR deals with the errors in an image but SSIM is concerned about Structural information. Structural information is that how a particular set of pixel is strongly connected with each other. It also considers the dependency of a particular pixel because with this we come to know about the image that how it is visually appears. It is further divided in three parameter:

Light Distortion

It consider with the brightness of an cover image. If image is bright then it will be easier to hide the content in it. It is computed as:-

Light distortion= (MSE/x+2y+3z)+(MSE/x+y+z)

Information distortion

It is concerned with the overall information about the image i.e its global view or local view and it also check that how nearer/farther the pixels are. It is computed as:-

Information distortion=2α (Γ+1)-βn

Where, α and β are the both constants.

Contrast Matching Distortion

It is used to match the contrast at different pixel-level so that it is easier to embed the hidden coefficient. It is measured up to some threshold value. It is calculated by:-

Contrast information=2*information distortion [log (base 2) (|(x+y) (x-y)|)]

Signal to Noise Ratio

It is static value so it does not change. It is used to measure the amount of unwanted noise in the actual audio data which is hidden. The lesser value of SNR implies the better quality of an image. It is measure in db. It is computed as follows:-

SNR=2*log (base 10) (1ε (x=1 to n-1)+O(I,j)/MSE)

Squared Pearson Correlation Coefficient

It is used to measure the similarity between different identity, signals and images like in cover image and in stego- image. Higher the value of SPCC then higher the quality of an image.

SPCC= ((x-x1) (y-y1)/√ε(i=1 to m-1)√ε(i=1 to n-1))

LITERATURE REVIEW

It is suggested that to hide massage in audio: frequency domain is better than time domain because as human eye is highly sensitive to small changes in light but not in signal which is used in video to convey the color differencing.

LSbSr [4] is one of the representation where L is light and Sb, Sr both are the components of signal. Sb and Sr are both used to increase the overall image quality. As in this paper we are hiding image congaing password and the maximum size of secret message is 3*W*H where W is width and H is height of the image [5]. But the main problem is the quality of audio is decreased after embedding message.

PSNR is basically used to check the similarity of the image before and after embedding secret message but this property is not suitable in the case of audio, it is only suitable for images like as implemented above in figure 3.

SSIM is the property which is used to check the quality of audio signal when image is embedded: but still there are some issues regarding quality of audio so to come out of it OFDM (Orthogonal frequency division multiple access)[6] is to be used but at receiver side the original cover is to be used. As there is problem with size of audio signal but now it can be removed by using Pitch transformation method which is explained above. To test the stego image quality it will checked by various attacks [1] like Gaussian noise, Sharpening, Gaussian blur and gamma correction [2]. So all these attacks are checked stegnogapgy algorithm for steganalytic attack like histogram test and RS attack. RS attack is used to detect all the secret message those are replaced by LSB along with their size [3]. So to prevent secret message from all these attacks it is required to increase the edges of the image with this capacity and quality of the cover image will increase. In case of audio, we use Coagula technique which comes under Pitch transformation: by this secret information cannot be visualized because it simply a kind of sound wave. Encoding and decoding of secret message is shown in Proposed Work Section. Other then audio we have several techniques in which secret data is stored in images like optimal Least Significant Bit[19-20], Chaotic Based Encryption[13], Pixel Value Differencing proposed by Wu and Tsai, Particle Swarm Optimization strategy[8,9,10] and reversible Data Hiding using weighted matrix[14-18] etc. In Experimental and result analysis section we present the comparison between different mediums with respect to few parameters.

PROPOSED WORK

In this paper, image is to be hidden which contain confidential information such as password etc: now this image is to be hidden in audio in such a way that message cannot be visualized to anyone. This process requires embedding of image in audio which is done by sender and decoding of image from audio which is done by receiver. In embedding, Coagula technique is required and in decoding, Sonic visualize technique is required.

Embedding Process:-

Input: Secret data in the form of image and audio message

Output: Stego.wav after embedding secret message

Step 1: Create the image, which contain some confidential information such as codes and passwords etc.

Step 2: Now open that image with Coagula.

Step 3: From settings, click on render image without noise.

Step 4: After this you can hear a sound track over the secret message.

Step 5: Now click to Stop.

Step 6: Finish

So it is the embedding process done by Coagula and it creates.wav type signal which is actually a sound track.

Extracting hidden message from Stego.wav:-

Input: Stego image (STEGO.wav)

Output: Hidden Message (HIDE.jpeg)

Step 1: At receiver side user need Sonic Visualizer to decode the message from sound track.

Step 2: In Sonic Application, click to open and the a window displays and out of it we need to browse.wav file which is done be coagula.

Step 3: So it will display waveforms, and user can play it.

Step 4: To decode the message click on add spectrogram and after that 'all channel mixed'

Step 5: After that user can see the actual message

Step 6: Now he/she can adjust its coordinates for its better visual quality

Step 7: Finish

User can adjust its color also for the better visual quality of message.

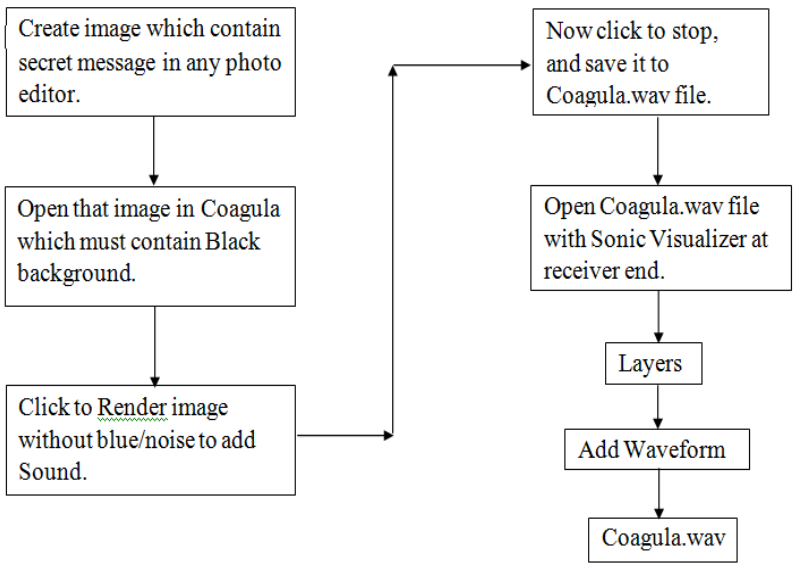

Figure 5: Process of Embedding and Decoding

EXPERIMENTAL RESULTS AND ANALYSIS

This section shows the result of escaping data by using coagula and decoding at receiver end by sonic visualizer. As in above figure 5 shows the complete process of embedding and decoding, which is done by different tools. On the other side it shows the comparison between different mediums those are used to implement stegnography and each and every medium has its own advantage.

Encoding-by Coagula

As above in proposed work: that we use audio to embed secret information so that it if hidden from hacker. Suppose we create some image which contain confidential information like password and it is embedded by coagula so now its output is in coagula.wav type i.e some sound track will play as shown figure 6. Coagula is a tool which is used to hide data inside audio. After hiding, then it create coagula.wav file which contain some confidential information but itself its an audio file

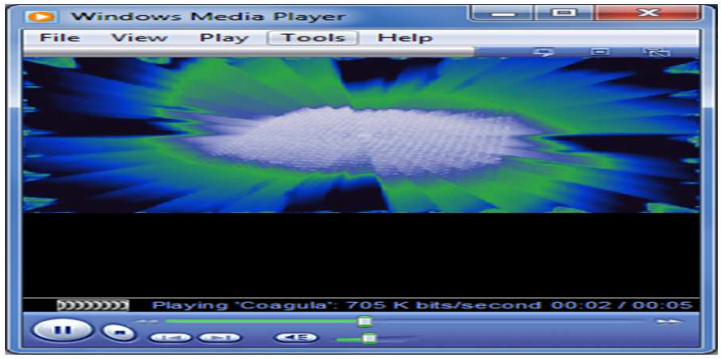

Figure 6: Audio Signal Contain Confidential Information

Decoding Process- by Sonic Visualizer

Now when the audio is send to receiver over some medium: after that message will be decoded by Sonic Visualizer and with this we can adjust its visual quality also as per particular comfort. In Sonic visualize, some waveforms will displayed such as in figure 7 and the password or the actual message will be displayed in figure 8.

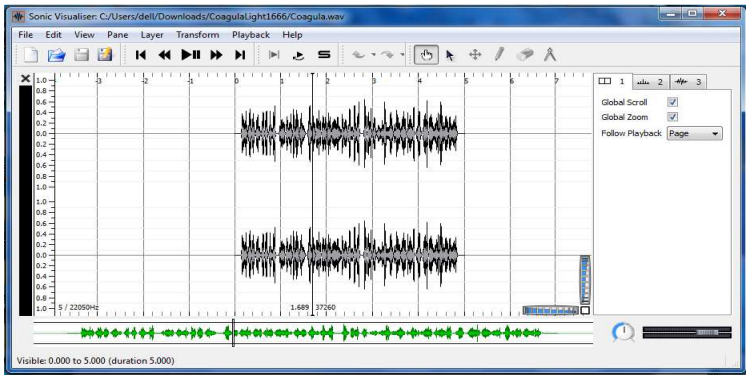

Figure 7: Waveforms in Sonic Visualize of above Audio Signal

Coagula, which is used for encoding at sender side is suitable to windows only, this tool does not support other platforms like Linux, Unix and mac etc. So it is platform specific. Generally, it deals with colors also if the image which

contain hidden message is brighter at some portion in secret image then during embedding through Coagula higher sound will be produced. Using Coagula, some sort of glitch and pitchy sound will generate that is there will be no any rap or no and electric sound in it.

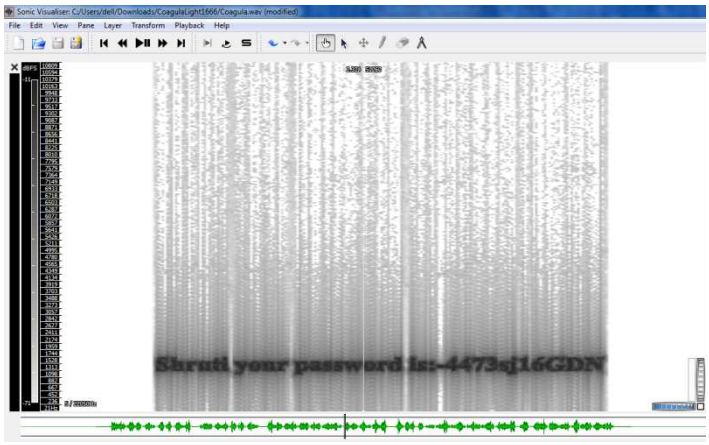

Figure 8: Actual Message which is Hidden by Audio

If we discuss about Sonic Visualizer, then it is compatible with windows, mac, Linux and Unix too, as it is free software, distributed under the GNU general public License (v2 or later) and available for all the platforms. It was developed in 22nd of October 2015 at the center for digital music at queen Marry University of London. It is an application used for viewing and analyzing the contents of music audio files. The goal of Sonic Visualizer is to first program where we reach for when want to study a musical recording rather than simply listen to it. Sonic Visualizer will be specific for musicologist, archivists, signal processes researchers and anyone else looking for a friendly way to have a look at what lies inside the audio file.

Comparing Results of Various Digital Mediums

But as in results we observe that audio can embed secret data, similarly there are various other medium which can escape secret data like image, video and audio as we discussed above. Stegnography is a branch of information hiding carried out by embedding important data e.g text and image in multimedia such as images, audio and video. Since the digital images are popularly used medium on internet and take benefit of human limited visual perception of colors and also provide large embedding capacity ratio. So that's why images are prove to be most suitable carriers for stegnograpgy stratigies.

Table 1: Shows the Comparison in different Mediums of Implementing Stegnograpgy by Various Parameters

Parameters	Image	Audio	Video
Visibility	Because of different combination of color visibility of message is poor	visibility is hard to be detected	Visibility of message can be possible because of splitting in frames.
Complexity	Less complex	More Complex	More complex then image
Capacity	Provides larger embedding capacity	Provides Less Capacity	Depends upon frames
Detection Rate	High	Low	Depend upon length of message

As in table1, shows the comparison between different mediums. So after observing this we can not conclude that audio is best escaping medium because in audio, few parameters suffers while those aren't in other mediums. Similarly, image and video mediums are suffers due to few parameters. So selection of medium is as per according to the demand of application.

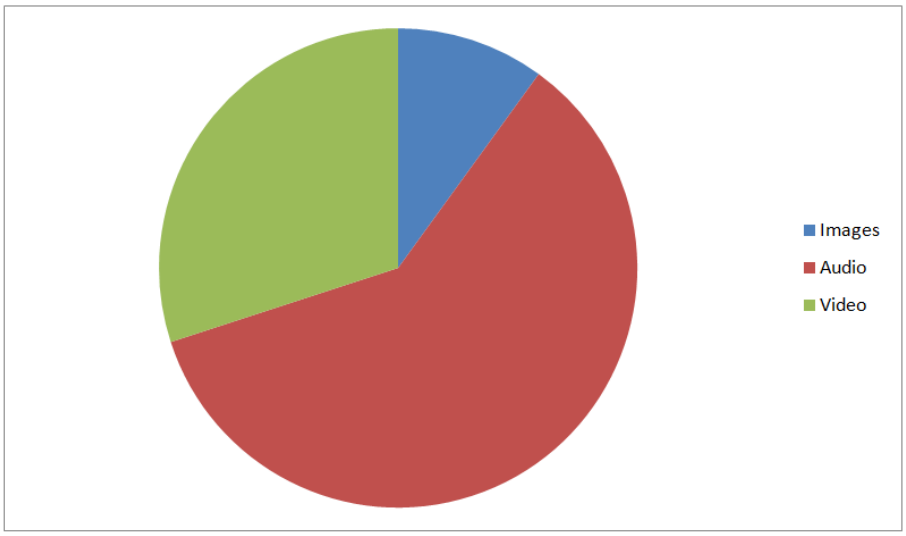

Figure 9: Pie Chart Represents the Complexity between Different Medium

As we observe from figure 9, that complexity of audio is very high as comparative to image and video. Though complexity takes place in other two mediums also but there level is bit smaller then audio. As audio deals with frequency domain method which makes it complex while escaping secret data inside audio. Traveling across network is also become cumbersome process. In Figure 9, shows the embedding capacity of image, audio and video.

As image medium provides maximum embedding capacity, in the case of jpeg image format and after that in video which depend upon its frames. In video embedding capacity is directly proportional to frames i.e large number of frames supports huge amount of embedding capacity.

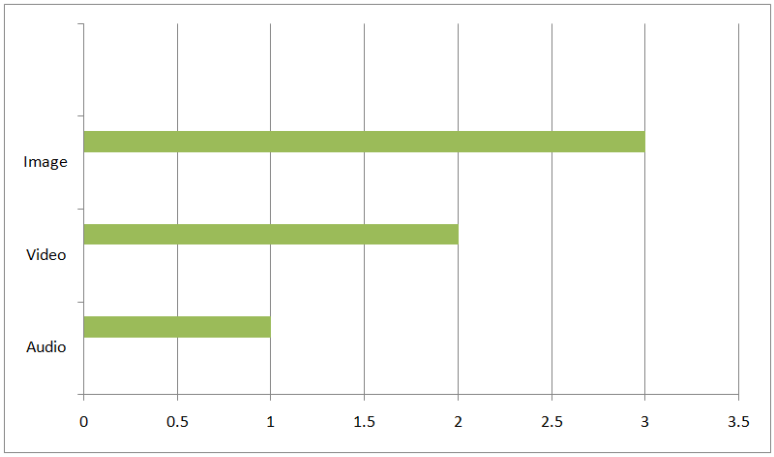

Figure 9: Bar Graph Shows the Escaping Capacity in Different Medium

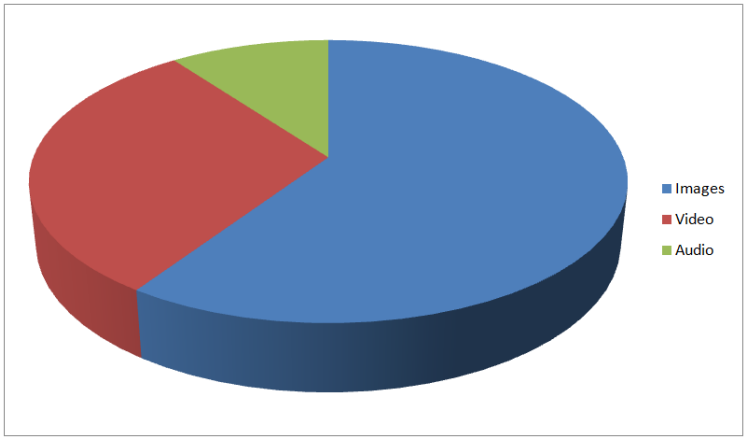

Figure 10: Pie Chart Represents the Detection Rate in Different Medium

As embedding capacity is less in audio than others, hence detection rate is also less as comparative to other medium. In Figure 10, shows the detection rate of different mediums i.e in audio detection rate is much lesser then others so with respect to this parameter audio is proved to be superior then other.

CONCLUSIONS

In this paper, secure and high capacity method is used for image stegnography. Using Pitch transformation message is to be hidden in audio by Coagula. So that it may not reveal its existence: and on receiver end it is further decoded by Sonic Visualizer. Message which is to be encoded in Coagula, it must be of.jpeg or.bmp type: if there is another type then quality may suffers or secret message may be revealed by eavesdropper. Image which contain secret information it is of RGB so that we have huge amount of intensities as compare to gray level. Secret message is preserved by discreet values of SNR and SPCC. As secret message can be hidden in any cover medium either image, audio or video, but we cannot judge the superior out of them because as it is presented in result section that in few parameters like complexity and embedding capacity image is proved to be best and sometimes video also but if we look forward to detection rate and visibility then audio will be ranked first.

REFERENCES

1. Vijay Kumar and Dinesh Kumar. Performance Evaluation of DWT based Steganography. IEEE 2nd International Advance Computing Conference, 2010. pp 223-228.
2. 11. AlWeKanso, Hala S. Own. Steganographic algorithm based on a chaotic map. Communication Nonlinear Science Numerical Simulation, 17, 2012. pp 3287–3302.
3. 12. S. Geetha, V. Kabilan, S.P. Chockalingam, N. Kamaraj. Varying radix numeral system based adaptive image steganography. Information Processing Letters 111, 2011. pp 792–797.
4. Shejul, A. A., Kulkarni, U.L. A Secure Skin Tone based Steganography (SSTS) using Wavelet Transform. International Journal of Computer Theory and Engineering, Vol.3, No.1, 2011. pp. 16-22.
5. M. I. Khalil. Image steganography: Hiding short messages within digital images. JCS&T, Vol.11, No. 2. pp 68-73.

6. Jose Juan Garcia-Hernandez, Ramon Parra-Michel, Claudia Feregrino-Uribe, Rene Cumplido. High payload data-hiding in audio signals based on a modified OFDM approach. Expert Systems with Applications 40, 2013. Elsevier publications. Pp 3055–3064.
7. Wavelet transform based steganography technique to hide audio signals in image. Hemalatha Sa,1, U. Dinesh Acharyaa, Renuka Aa aDepartment of Computer Science and Engineering, Manipal Institute of Technology, Manipal Universuty, Manipal 576104, India
8. C.C. Chang, T.S. Chen, L.Z. Chung, A steganographic method based upon JPEG and quantization table modification, Information Science 141 (2002) 123–138.
9. I.J. Cox, J. Kilian, F.T. Leighton, T. Shamoon, Secure spread spectrum watermarking for multimedia, IEEE Transactions on Image Processing 6 (12) (1997) 1673–1687.
10. L. Ghouti, A. Bouridane, M.K. Ibrahim, S. Boussakta, Digital image watermarking using balanced multiwavelets, IEEE Transactions on Signal Processing 54 (4) (2006) 1519–1536.
11. H. Noda, M. Niimi, E. Kawaguchi, High-performance JPEG steganography using quantization index modulation in DCT domain,Pattern Recognition Letters 27 (5) (2006) 455–461.
12. F.Y. Shih, Y.-T. Wu, Robust watermarking and compression for medical images based on genetic algorithms, Information Sciences 175 (3) (2005) 200–216.
13. S. Mazloom, A.M. Eftekhari-Moghadam, Color image encryption based on cou-pled nonlinear chaotic map, Chaos Solitons Fractals 42 (3) (2009) 1745–1754.
14. K. Jung, K. Yoo, Data hiding method using image interpolation, Comput. Stand.Interfaces 31 (2009) 465–470.
15. C. Lee, Y. Huang, An efficient image interpolation increasing payload inre-versible data hiding, Expert Syst. Appl. 39 (2012) 6712–6719.
16. Y.-C. Tseng, Y.-Y. Chen, H.-K. Pan, A secure data hiding scheme for binary images,IEEE Trans. Commun. 50 (8) (2002) 1227–1231.
17. L. Fan, T. Gao, Y. Cao, Improving the embedding efficiency of weight matrix-based steganography for grayscale images, Comput. Electr. Eng. 39 (2013)873–881.
18. Biswapati Jana, High payload reversible data hiding scheme using weighted matrix, department of computer science, optik 127 (2015) 3347-3358.
19. R.Z. Wang, C.F. Lin, J.C. Lin, Image hiding by optimal LSB substitution and genetic algorithm, Pattern Recognition 34 (3) (2001)671–683.
20. C.K. Chan, L.M. Cheng, Hiding data in images by simple LSB substitution, Pattern Recognition 37 (3) (2004) 469–474.