International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-3, September 2019

Scalable Methodology to Hide Audio Data in Cover Image using RGB and Gray Color based Key Positioning Image Steganography

Jagadish Gurrala, P Sanyasi Naidu

Abstract: ***This objective of this paper is primarily focused on RGB color and Gray scale color based key positioning steganography which has been used to overcome the disadvantages of the Least Significant Bit replacement algorithm and helps to embed the audio data in the color images. The given audio data of various sizes is used to embed in the green color channel of the 24 bit color image sequentially by the key based LSB positioning algorithm. Here the audio threshold is another major area where the focus has been laid as increasing the size of the audio data[26] which can be sent through an image without losing the quality of the audio. This method of hiding the audio data through an image helps to authenticate the sender[25] and verifies whether the data has been really sent to the valid user or is used to prevent morphed secret details by the attacker in the middle. The proposed algorithm has been tested against various existing algorithm to study how effectively the algorithm is working, and how effectively it overcomes the drawbacks of the present algorithms. The algorithm is scalable to serve the purpose of authenticating the different demographical region users living all over world and also to identify that the message is reaching only to the valid user[31].***

Keywords : LSB positioning, Steganography, Image security

I. INTRODUCTION

Image Steganography is the technique of the hiding a message in an camouflage images[25]. It has origin dated in 13th century. Over the last decade, many researchers surveyed various hiding techniques such as image to image, audio to audio, video to video, placing same entity in the same big enough entity. Steganography provides an add-on advantage of sending the data from under the nose of the attacker. The steganography techniques utilize the concept of embedding the data rather than encrypting the data. They use a cover file to veil up the data and send it through an insecure network channel. The receiver cannot receive a file unless he knows. The four main file formats that can be used for steganography are :-

1)Text.
2)Images.
3)Audio/Video.
4)Protocol.

Steganography which can be defined as the data hidden within the data is an emerging area which is used for secured data transmission over any public media. It is a process that involves hiding a message in an appropriate carrier like image or audio which depends on key based storage and retrieval. The Figure 1, displays the cover image as carrier to hold the content of audio signals through stego system encoding process to produce the stego image to travelling across medium. Steganography[27] is vividly presented for a comprehensive understanding. At receiver, destination party retrieve the estimate of message through stego system audio decoding method. Therefore the receiver gets the copy of estimate of message flawlessly. In next section, presents the cryptography concept more clearly.

A.Cryptography

Cryptography is the art of achieving security by encoding[28] messages to make them non readable and cryptanalysis is the technique of decoding messages from a non-readable format back to a readable format without knowing how they were initially converted from readable format to non readable format. Basically cryptology[29] is a combination of cryptography and cryptanalysis.

The uses of cryptography are spread over the areas of important communications such as those of spies, military leaders and diplomats. But, in recent years, with the blast of internet uses and users among the world, there has been a sudden urge for the data security and the cryptography techniques have been exploited for these purposes.

B.Encryption and Decryption

In the encryption process the data will be converted into a code[30] which can thus be accessed only by authorized parties. The attackers cannot attack unless they know the method by which only sensitive data can be revealed. For the process of encryption, authors need to have a key and a method by which authors have to modify the text or data into a cipher text which must be further decrypted to know what the text is. The sender and the receiver will agree upon a common key or different keys depending upon the necessity and the need of level of security.

In the decryption process, it is the reverse of encryption in which we map the cipher text to it's corresponding plain text or data using the key. It is usually done on the receiver's end using a key that has been agreed upon on previous hand by both the parties.

Manuscript published on 30 September 2019
* Correspondence Author
Mr.G.Jagadish*,, Assistant Professor in Anil Neerukonda Institute of Technology & Sciences, Visakhapatnam since 2009.
Dr. Sanyasi Naidu, Associate Professor in Department of Computer Science and Engineering GITAM deemed to be University since

C.Steganography versus Cryptography

Steganography and Cryptography[1][2] are used for the purpose of data transmission over an insecure network without the data being exposed to any unauthorized persons. Steganography embeds the data in a cover image while cryptography encrypts the data. The advantage of steganography is that the look of the file doesn't change and it will not raise any doubt for the attacker to suspect that there may be some data hidden unlike cryptography that encrypts the data and sends it to over the network, which is easy for the attacker to know that the data has been encrypted and he/she can use various decrypting techniques to extract the desired data. The remaining paper is presents literature survey which discussed in section 2, and then deals with the proposed methodology and proposed architecture is improved in audio hiding in section 3 followed by experimentation setup and results, assessment of image quality and their comparison between existing techniques and proposed techniques and its evaluation results presented in the context of PSNR and RMSR as shown in section 4. In section 5 conclusion and future direction is mentioned.

II. LITERATURE SURVEY

A. Back ground

Steganography is an ancient idea of hiding information; the specific methods used have evolved during its long history [2]. In the context of contemporary information and communication technology, most research work was devoted to methods of hiding secret information in numerical data, text and images [1] transmitted between communicating parties. Such methods are generally independent of the communication logic and mechanisms, the communication protocol, that are used in particular communication networks. In these methods the transmitted user-data is a protocol-independent carrier of hidden information. Network steganography differs from such methods in that it based on using "manipulating" specific communication protocols' features to transmit secret information. Consider, for example, a query response type of exchange of messages for which the communication protocol assumes that the response should come within a specific time limit; otherwise, it is treated as excessively delayed and discarded. Communicating parties that want to use this protocol for steganographic purposes may make an agreement, which becomes their shared secret, that the responses carrying hidden information will be purposefully excessively delayed and that such responses will be read by the recipient (i.e., not discarded).

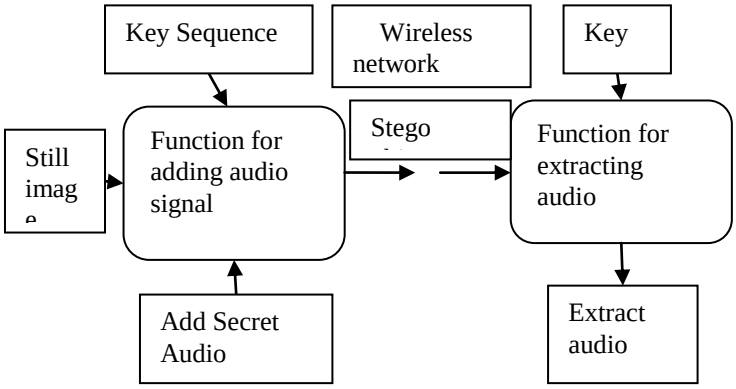

Fig 1. Model for New Image Steganography for audio hiding

The figure 1 shows how steganography works. The input is cover image, embedding data is audio data and using steganography function is to extract green color from RGB colors to perform key positioning system and produce output is stego image. With the advance of technology, Image Steganography has increased applications and varied ways of applying the techniques of Steganography. Steganography majorly consists of a cover file that carries the image through an insecure channel called as "Cover Image". Depending on the type of cover image, Steganography has been classified into 4 types. They are:

1. Image
2. Audio/Video
3. Prototype and
4. Text

We have used the concept of Image Steganography. Thus this provides to be the main advantage for steganography.

B. Constraints of Image Steganography

Image Steganography deals with the hiding of data within the Cover input image. The data can be any file, be it be an image, audio, text or another file. We have to wrap up the data using an image. We have chosen to bind audio data in an image. This kind of embedding an audio in an image helps to authenticate the sender, verify whether valid user is receiving the data or not and to find whether a third party attacker is present in the channel of communication or not. Since, image is used as a cover file, we have to make sure that the image must acquaint the data that is being embedded. Hence a 24 bit image format proved to be the best solution for hiding the data, since it holds a large memory space and convenient to hide a considerable amount of data. Furthermore, the threshold size of the image must be calculated for the given image size which will be explained in the later parts.The only one strategy that sender is used to follow is the input image is scalable and it supports both RGB and Gray scale images. It should be distinct and must only be available with him(sender). It should not be a monotonic pattern of color rather it should be hew of colors which can effectively veil the audio data .

The famous techniques used in the Image steganography[4][6] is Least Significant Bit Positioning technique. In the LSB concept, explores the less important to the region across pixels of the image.

C. LSB positioning technique in Image Steganography

This method is the most simple method of hiding data within the given image. The image contains least significant pixels which are utilized within the given input cover image. When converting an analog image to digital format, in the paper, the authors usually chose between three different ways of representing RGB colors:

1. 24-bit color: every pixel can have one in 2^24 colors, and these are represented as different quantities of three basic colors: red (R), green (G), blue (B), given by 8 bits (256 values) each.
2. 8-bit color: every pixel can have one in 256 (2^8) colors, chosen from a palette, or a table of colors.
3. 8-bit gray-scale: every pixel can have one in 256 (2^8) shades of gray.

LSB insertion modifies the LSBs of each color in 24-bit images, or the LSBs of the 8-bit value for 8-bit images.The most basic of LSBs insertion for 24-bit pictures inserts 3 bits/pixel. Since every pixel is 24 bits, the authors can hide using the following equations.

Every 3 hidden_bits in RGB image /pixel/24 data_bits/pixel = 1/8 hidden_bits/data_bits (1)

So for the equation 1, we hide 1 bit of the embedded message for every 8 bits of the cover image. But, being the simplest, LSB positioning has its own drawbacks[5][7]. It is highly vulnerable to noise and the data can be easily corrupted when passing through a noisy channel. This can distort the data and fail the main purpose of Image Steganography[30][31]. Thus, to overcome this drawback we have improvised this LSB positioning to a Green color substitution Based key positioning Algorithm, which can withstand the noisy channel and can hide the data effectively both in quality and quantity.

III. PROPOSED METHODOLOGY IN RGB IMAGE STEGANOGRAPHY

This proposed algorithm is to hide the audio data effectively in an image without any suspicion[10][13][15] of the data being hidden in the image. It is to work against the attacks by using a distinct new image that isn't possible to compare other techniques because the image which is taken from source is unique and contains time stamp details for supposed when the user click the scene on spot immediately date and time is mentioned inside the photo. The aim of the paper is to hide the audio in an image using steganography and ensure that the quality of concealing data remains the same.We used a method for hiding the audio in a distinct image file in order to securely send over the network without any suspicion about sensitive data (audio or image) being hidden. This process sends audio that can be used as an authentication for the user by the voice sent from the sender. This paper though requires a distinct image[18][19] which we can use as a carrier and hide the audio which is well within the limits of the threshold that the image can hide, that will secure the audio and get the attacker deceived from its true nature. The person will not be able to know until unless he gets to know the intention and the method of hiding and thus cannot guess the data that is being sent through the image.The main challenge lies[11][20-24] in increasing the amount of audio data that can be sent through the cover image and, how can it be securely sent over the network till the receiver. Also we need to ensure that cover RGB image will not be giving rise to any suspicion of the data being carried while travelling through the network.

A. Proposed Architecture for Improvement of audio data hiding

In the paper the input and out put of process is given.

At source:

Input file: 128*128 color image resolution

Output file:construction of stego image contains Cover image plus audio file wrapped in it.

At destination:

Input file: 128*128 stego image resolution
Output file: Extraction of audio file inside color image through process.

A.1. Algorithm for construction of Stego Image process:

1. Get a distinct RGB Cover image(a 24 bit format image).
2. Convert the image into a binary file with each pixel being specified in terms of it's red, green and blue channels.
3. Record an audio within the range of the threshold for the resolution of the image specified.
4. Convert the audio (.mf3)into it's binary format.
5. After step 4, place the binary audio data in the place of the green channel of each pixel along each row until the data has been completely placed.
6. After step 5 send this stego-image through the insecure channel.
7. After the receiver receives the data, he must extract the green channel bits from the stego- image.
8. Now the bits are integrated to get the audio back and to authenticate the sender.

A.1. Experimentation Results

In the paper, authors have chosen open source operating system such as UBUNTU 6.1 and WINDOWS 7, which gets stego image under different image data set tested in simulation environment called visual studio version 2013, with c# tool.

A.2. RGB Color based Key Positioning Algorithm:

The authors proposed the Key based LSB positioning method[29] and have adopted from Least Significant Bit algorithm for the Steganography and have modified it to strengthen the algorithm to overcome it's drawbacks. We chose to replace green stream of a 24 bit image channel and replace the audio binary bits in those bit positions.

A.2.1 The following steps are applied for the algorithm:

Step 1: Consider a 24 bit image as cover image. (Make sure the image is distinct and has a lot of colour channels unlike a monotonous image of only a few colours and the colours are well spread.)

Step 2: Calculate the size of the image and find the threshold of the audio that can be embedded in that image from the table below.
Step 3: Record an audio of the given size .
Step 4: Convert both the image and audio into their corresponding binary formats.
Step 5 : Now replace the green channel of the 24 bit image with the audio bits.
Step 6: Send this image through the insecure channel .
Step 7: The receiver will receive the image.
Step 8: The receiver then extracts the green channel and get the audio that has been embedded.

TABLE 1: Threshold audio values of various cover image sizes:

Sno	*Size of the image*	*Threshold audio size*
1.	1136*640	266.25kb
2.	960*640	225kb
3.	320*480	56kb
4.	480*268	47.11kb

These are many sizes of the image which can actually support a good amount of the audio sizes. In the experimentation, the authors have chosen 480 by 268 images which produces good stego image quality with the help of 47.11kb threshold audio size details taken from formulation and derivation the equations.

B. *Calculating the threshold size of an audio for a given Image Size:*

Let the size of image be of dimensions p*q. Since it is a 24 bit image,
No. of bits in the image are given by : p*q*24.
In this paper, the authors were ready to embedding the data of audio only in green channel, which will be of 8 bits .
Hence number of such bits that can be replaced are : (p*q*24)/8 = (p*q*3)
This gives the number of bits of audio that can be placed in the given image.
To calculate bytes : (p*q*3)/8.
To calculate the size in Kb : (p*q*3)/8*1024.

C. *Evaluation on RGB color based Key positioning system:*

At beginning, MatLab R2013a reads the three different sizes of original image (Cover Image) to hide details without noticing to attackers (high imperceptibility). In the image shown in figure 2, the authors have to put secret audio details ranging from 47.11 to 225 KB inside green color channel. After execution, the audio file mf3/mp3/avi details were hidden in all green channel of LSB portions and get it stego image with slight variation on left portion of image such as in fig 3.

TABLE I. ASSESMENT OF IMAGE QUALITY THROUGH EVALUATION

Cover Image file name	**Evaluation on image through PSNR and MSE**		
	Techniques	***Cover image dimension***	***Size of Cover Image***
F16.jpg	Existing Audio data hiding technque(Hemalath et al)	512 * 512	768KB
Baboon.jpg	Existing Audio data hiding technque(Hemalath et al)	225 * 225	12.8KB
barbara.png	Existing Audio data hiding technque(Hemalath et al)	660* 660	205KB
F17.jpg	Proposed Technique(Green based key positioning scheme	225 * 224	7.49 KB
Baboon.jpg	Proposed Technique(Green based key positioning scheme	1060 * 753	231 KB
barbara.png	Proposed Technique(Green based key positioning scheme	1037 * 770	270KB

TABLE 2. Evaluation on different image sizes with PSNR and MSE values.

Dimensions	Size of Cover Image	Threshold Audio Size(KB)	PSNR value	MSE
512 * 512	768KB	225	36.7682	65.639
225 * 225	12.8KB	56	43.9881	20.537
660* 660	205KB	47.11	41.8279	6.652
3232 * 1080	226KB	225	45..0243	2.0448
1060 * 753	231 KB	56	50.0126	0.034
1037 * 770	270KB	47.11	49.765	1.564

To elaborate process there are three different kinds of jpg and png files F16, Baboon, and Barbara Produces stego images with less quality to better quality by measuring Peak Signal to Noise Ratio(PSNR) in correlation with results of Root Mean Square Error(RMSE) in MATLAB. It is observed that proposed method has shown better image quality with less noisy details , so that attacker is unnoticeable about it. The following the results were shown by comparing original image with stego image.

D. Evaluations on given Data set:

Exisiting algorithms

Cover Image Stego image

Fig 3. F16.jpg

Cover image Stego image

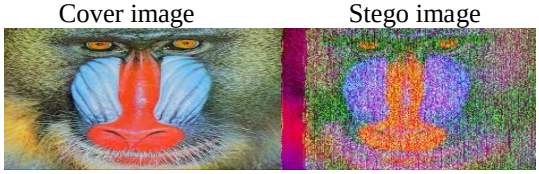

Fig 4. Baboon.jpg

Proposed algorithms

Cover Image Stego image

Fig 5. F17. jpg

Cover Image Stego image

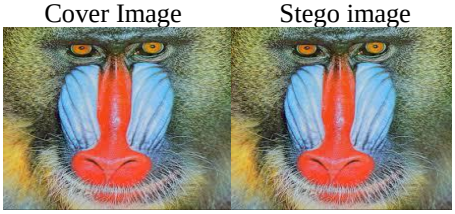

Fig 6. Baboon.jpg

In the given screen shot Application Programming Interface asks you to upload the audio clip to it and embeds this into API. Subsequently audio clip must encrypt audio into binary format and locate it into appropriate Green channels of Cover image. Then that stego image is ready to transfer to destination and followed by decrypting the stego image by extracting the stego image though green channel as shown in figure 4 onwards. In the comparison it is observed that Green color based key position technique shows good image quality by getting PSNR value which is 50, the maximum in relation to MSE which is minimum 2.0,0.034,1.564. There were zero differences between the original and recovered secret files through Human Visual Eye(HVE).

Finally the received RGB image is reached to end user who can extract the secret audio .mf3 file through application layer assuming TCP/IP protocol suite as illustrated in paper[7].

IV. QUALITY ASSESSMENT THROUGH METRICS

The authors have chosen two metrics to get the image quality intact without noticing to adversaries. Authors apply the metrics to verify the originality of stego image after decoding it at destination.

PSNR: It is the peak signal-to-noise ratio in decibels (dB). The PSNR is only meaningful for data encoded in terms of bits per sample, or bits per pixel. For better image quality, PSNR value is infinity and MSE is 0.

$$\text{PSNR} = = 10 \times \log_{10} \frac{MAX^2}{RMSE}$$

where MAX is the maximum pixel value, and RMSE represents the average of the root mean square errors for the RGB colors shown.

RMSE: It is the squared norm of the difference between the data and the approximation divided by the number of pixel elements.

$$\text{RMSE} = \frac{\sqrt{\sum_{i=1}^{n} (Pi - Oi)^2}}{n}$$

Where Pi is the distorted stego image pixel values and Oi is the original image pixels values of cover image ranging from i=1 to n, n is the total number of pixels.

V. CONCLUSION AND FUTURE DIRECTION

In this paper, authors mainly focuses on authenticating the images[27-29] with an own audio information[26] from the sender that needs to be sent through insecure channel. This helps to ensure that the data is being received from an authenticated person and only the desired receiver will be getting the actual audio from the receiver. This is done by utilizing the concept of steganography. In this process, we have actually hidden the audio in an image by converting it into a binary file and embedding it in the green channel of a 24 bit image[16-19]. This stego-image will be unwrapped and the audio will be detected only if the person knows the size and the places where the audio is hidden. The other important factor is the threshold of the size of the audio that can hidden in various sizes of the image. The embedding of the audio is done in the green channel of the image by choosing a distinct and a new image. Finally the end user can benefit by preventing chance for the attacker to analyze and detect the data being hidden. Also since the audio is hidden in the image there will be almost no chances for the attacker to know that the data is being hidden in the image. Any authenticate user who need to proves it, can send the audio from under different image data set. In future, this technique is not suitable to get stego image to send it because of steg-analysis. Authors get acquainted knowledge about visual cryptography to divide the secret data to be transmit through division process discussed in [2]. As the future scope of the work, it may be recommended to focus on the embedding video content inside an image.

ACKNOWLEDGMENT

The authors would like to thanks Dr.Sivaranjani Reddy, Professor & HOD,Anil Neerukonda Institute Of Technology &Sciences,Visakhapatnam, for her great support. Authors would also thanks to Mrs. Sabirunnisa Gouse, Assistant professor Dept. of English, ANITS , for her strong support in helping to shape the paper and proofreading the manuscript and making numerous helpful suggestions. The authors would also like to thank the Prof.Tammi Reddy, HOD, Dept. of CSE, GIT,GITAM Deemed to be University, and the anonymous reviewers for their insightful and helpful comments.

REFERENCES

1. Neil F. Johnson, “Exploring Steganography-Seeing the Unseen,” Phil. Trans. Roy. Soc. London, IEEE Computer,February 1998,vol 31, no 2, pp.26-34.
2. Moni Naor and Adi Shamir, “Visual cryptography. in Proceedings of Advances in Cryptology”, EUROCRYPT 94, LNCS Vol. 950, pages 1-12. Springer - Verlag, 1994.
3. Reena Kharat and P.Sanyasi Naidu, “Secure Authentication in Online Voting System Using Multiple Image Secret Sharing” in ICCUBEA 16, IEEE xplore 2016.
4. W. Bender, W. Butera, D. Gruhl, R. Hwang, F.J. Paiz and S. Pogreb, “Applications for data hiding,” IBMSystems Journal, 39 (3&4)(2000) 547-568.

5. Mr. Vikas Tyagi, "Data Hiding in Image using least significant bit with cryptography", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 4, April 2012
6. R.Poornima1 and .J.Iswarya2, "An Overview of Digital Image Steganography," International Journal of Computer Science & Engineering Survey (IJCSES) Vol.4, No.1,February 2013M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.
7. A. Fatnassi ¬ H. Gharsellaoui ¬¬ S. Bouamam," A New Hybrid Steganalysis Based Approach for Embedding Image in Audio and Image Cover Media," IFAC,Elsevier, 2016, pp 1809-1814.
8. Hemalatha et al., "Wavelet transform based steganography technique to hide audio signals in image",Elsevier,2015
9. Gerami P, Ibrahim S, Bashardoost M. "Least significant bit image steganography using particle swarm optimization and optical pixel adjustment", Int J Comput Appl 2012;55(2):975–8887.doi:10.5120/8727-2602.
10. Chen W.J., "Color image steganography scheme using DFT, SPIHT codec, and modified differential phase-shift keying techniques". Appl. Math. Comput. 2008;196:40–54. doi:10.1016/ j.amc.2007.05.063.
11. Wu C, Kao S, Hwang M. "A high quality image sharing with steganography and adaptive authentication scheme". J Syst Softw 2011;84:2196–207. doi:10.1016/j.jss.2011.06.021.
12. Qu Z, Chen X, Zhou X, Niu X, Yang Y. "Novel quantum steganography with large payload". Opt Commun 2010;283(23):4782–6. doi:10.1016/j.optcom.2010.06.083.
13. Fazli S, Kiamini M, 2008. "A high performance steganographic method using JPEG and PSO algorithm". In Proceedings of the12th IEEE International Multitopic Conference, Karachi (pp. 100–5).
14. Li X,Wang J. "A steganographic method based upon JPEG and particle swarm optimization algorithm", Inf Sci (Ny) 2007;177(15):3099–109. doi:10.1016/j.ins.2007.02.008.
15. W. Bender, W. Butera, D. Gruhl, R. Hwang, F.J. Paiz and S. Pogreb, "Applications for data hiding," IBMSystems Journal, 39 (3&4)(2000) 547-568.
16. Lu, P., et al. "An improved sample pairs method for detection of LSB embedding in Information Hiding". 2005.
17. I. Cox, T. Kalker, and Y. Ro, "Digital Watermarking," Editors. 2004, Springer Berlin / Heidelberg. p. 204-211.
18. Dumitrescu, S. and X. Wu "A new framework of LSB steganalysis of digital media" Signal Processing, IEEE Transactions on,Vol. 53, pp. 3936-3947, 2005.
19. Cheddad, A., Condell, J., Curran, K., & Mc Kevitt, P. "Digital image steganography: Survey and analysis of current methods" Signal processing, Vol. 90(3), pp. 727-752, 2010.
20. D. R. L. Prasanna, L. Jani Anbarasi and M. Jenila Vincent "A Novel Approach for Secret Data Transfer using Image Steganography and Visual Cryptography" ICCCS'11, February 2011.
21. T. Kalker, A.D. "A general framework for structural steganalysis of LSB replacement in Information Hiding". 2005.
22. Hardik Patel, Preeti Dave "Steganography technique based on DCT coefficients" International Journal of Engineering Research and Applications, Vol. 2, pp.713-717, Jan-Feb 2012.
23. Cheddad, A., Condell, et al. "block-based adaptive steganography combined with the LSBMR" Signal processing, Vol. 45(3), pp. 427-434, 2002.
24. Souvik Bhattacharyya, Indradip Banerjee and Gautam Sanyal "A survey of steganography and steganalysis technique in image, text, audio and video as cover carrier" Journal of Global Research in Computer Science Vol. 2, April 2011.
25. J. Cox, J. Kilian, T. Leighton, and T. Shamoon, "A secure, robust watermark for multimedia," in Information Hiding, Springer Lecture Notes in Computer Science, vol. 1174, pp. 183–206, 1996.
26. "Auditory masking and MPEG-1 audio compression," E Ambikairajah, AG Davis, WTK Wong, IEE Electronics & Communication Engineering Journal v 9 no 4 (Aug 97) pp 165- 175.
27. Fredrish, "Liability and Computer Security: Nine Principles", RJ Anderson, in Computer Security -ESORICS 94, Springer LNCS v 875 pp 231-245
28. Fredrich, "Stretching the Limits of Steganography", RJ Anderson, in Information Hiding, Springer Lecture Notes in Computer Science v 1174 (1996) pp 39- 48.
29. William, "The Eternity Service", in Proceedings of Pragocrypt 96 (GC UCMP, ISBN 80-01-01502-5) pp 242-252.
30. RJ Anderson, MG Kuhn, "Tamper Resistance- a Cautionary Note", in Proceedings of the Second Usenix Workshop on Electronic Commerce (Nov 96) pp 1- 11.
31. R Anderson, C Manifavas, "Chameleon- A New Kind of Stream Cipher",appear in Proceedings of the 4th Workshop on Fast Software Encryption (1997).

AUTHORS PROFILE

Mr.G.Jagadish, currently pursuing Ph.D from GITAM, deemed to be university since 2014 under the esteemed guidance of Dr.P.sanyasi Naidu. He has received his Masters' in Computer Science & Technology- specialization in computer networks from CSSE in 2009, Andhra University. He is currently working as Assistant Professor in Anil Neerukonda Institute of Technology & Sciences, Visakhapatnam since 2009. He has an excellent command on programming, network security, steganography and presented many papers internationally. He is the currently member of ACM- 7008666.

Dr. Sanyasi Naidu, received doctorate in Computer Science Engineering from Andhra University in the year of 2011. He is currently working as a Associate Professor in Department of Computer Science and Engineering Department at GITAM deemed to be University since 2001. He got Best performer award in the year of 2010 in teaching. His main interests lie in Image Processing, Computer Networks, Network Security, Cryptography, Formal Languages Automata Theory, C, Java. He is a life member of Indian Society for Technical Education. He is published 43 national and international journals and conference in his strength.