Securing Data in Image and Audio Files using Steganography Technique

Saikiran N1* Rama M2 Kiran P2 Sreenath K1 Prasad U2 Dr. P. Thanapal3

¹Department of Information Technology, QIS College of Engineering and Technology, Ongole, India ²Department of Computer Science and Engineering, QIS College of Engineering and Technology, Ongole, India *³School of Information Technology and Engineering, Vellore Institute of Technology, Vellore, Tamilnadu, India, E.Mail: thanapal.p@vit.ac.in

*Corresponding Author: Dr. P. Thanapal (thanapal.p@vit.ac.in)

Abstract:

The security of information is regarded as one of the biggest issues in communication to safeguard information because of the development of computer technology and the internet. There are numerous stenographic techniques that can be used to covertly send information to a recipient using a suitable carrier, such as text, image, audio, video, or protocol. By utilizing additional mechanisms, such as audio and video files, the techniques of audio and video steganography can be employed to conceal sensitive information. The drawing of concealing info within other info is Steganography. In Steganography it is difficult to detect the being of any unseen gen. Digital images are the most common transporters. Because of recent advances in steganography, providing safety to personal insides, messages through digital images has become difficult. By means of steganalysis the presence of hidden information in carrier files can be easily revealed. This paper suggests a novel Steganography technique for secret set-ups between two isolated gatherings. The method involves Transfiguring a secret image into a text document, then encrypting the spawned text hooked on cypher text using a key (password) built encryption process, and finally embedding the cypher text on to a cover image. Only in specific pixels the hidden message bits will be inserted in this threshold-based scheme. The security to keep the message secret is attained by making it difficult for a third party to detect and retrieve the hidden message.

Keywords: Steganography, Steganalysis, Cryptography, Cipher text, Encryption.

1. INTRODUCTION

Encryption and decryption are used in open networks to transmit data securely. Because each type of documents has its own features, many methods can be castoff to protect intimate image data from illegal access. To conceal the unique memo and send the non-readable text memo to the receiver, which allows for secret message announcement over the net is the primary goal of any encryption and decryption algorithm. To ensure data security encryption is the widely used mechanism and majority of algorithms are only for script facts. The process of converting unique image records into another anonymous structure using a key that no one can identify is Encryption. Recovering the original data from an encrypted object is the process of Decryption. Because of use of the internet, copyright protection, modifying, illegal copying, tampering, have become critical issues [7].

To address all of these issues, there is an urgent need to develop techniques for this purpose [1]. Digital watermarking is the answer for multimedia records protection. Digital watermarking (data) is the procedure of whacking or entrenching an invisible signal (data) into a given signal. This invisible signal (data) is raised to as a watermark or metadata, and the given sign (data) is referred to as cover effort. The watermark must be embedded in the cover effort so that it can endure not only the greatest mutual signal distortions, but also those caused by malicious attacks. This shelter work canister be in the form of an audio, video and image file. A watermarking procedure is made up of two algorithms: implanting and withdrawal (or detection). Watermarking was first proposed centuries ago [2]. Watermarking technology has been used to confirm data in a variety of ways. Watermarking technology has also been used in computers. The majority of computer watermarking research has focused on embedding a watermark into video, images and audio files. Since the early 1990s [3], many researchers[21-51] have been interested in digital image watermarking, which has become an interesting protection measure. Watermarking generation become used to mark facts authenticity via way of means of many distinctive means. Watermarking generation takes stood utilized in laptop as well.

Greatest of the images on laptop watermarking generation develop for embedding a watermark into video, audio, and image files. Media watermarking studies is a totally energetic area and virtual copy.

RELATED WORK

The process of information embedding in the form of digital content without any degradation of perceptual content is known as data hiding [1]. Three well-known approaches for data concealment are steganography, cryptography and Watermarking. The concealment of writing in Greek is defined as Steganography. In this process we deal with the data which is included in other data. Steganography, as defined by Lou et al. [2], is the process of hiding the existence of statistics by concealing information in various carriers. Here, main goal is to keep hidden information from being discovered.

In ancient Greek there is a practice of tattooing on shaved head which carries the undisclosed message and leasing his hair raise back before transport him into territory of opponent, which takes expectancy of this announcement system was slow in months, was studied in steganography method [3]. About 440 B.C., the document is written by imperceptible top-secret ink i.e. lemon juice, is the greatest popular method of traditional steganography technique which is used for marking in order to hide the information. Second method is the usage use pinholes to mark specific characters in a file and create a signature or pattern [3]. Here, the popularity for steganography development by using computers and its usage occurred afterward 2000 year [4]. The key benefit of using procedure of steganography is a very modest safety apparatus. Because the steganographic communication was hidden inside other innocuous sources, this is one of the extremely hard to detect it deprived of knowing its existence and the suitable training system [5]. The steganography techniques used to conceal data i.e. Batch steganography, Bit-Plane Complexity Segmentation (BPCS), transformation steganography, Least Significant Bits (LSB), and Chaos Based Spread Spectrum Image Steganography (CSSIS).

Many researchers have studied how to fur data secret images by with the steganography method, eg. [6-10]. Warkentin et al. [6] proposed a technique aimed at hiding data within audiovisual files. In order to hide data in their steganography algorithm, the secret gratified must be concealed in a message which is covered. El-Emam [7], proposed an algorithm for steganography to conceal securely huge amounts of files. This steganography algorithm is used for the concealment of huge quantity of statistics (image, audio, text) file within a color bitmap (bmp) image. By using the replacement of bits with appropriate pixels the necessary image would be segmented and filtered. These pixels are chosen arbitrarily. Chen et al. [8] castoff the side competition to modify a method used in [9]. They concentrated on concealing the data in the image's edges. In contrast, Wu et al. [10] uses pixel-value differencing to partition the original image into two consecutive pixels of non-overlapping blocks. This study introduced by El-Emam [7] employs a concept. A bitmap (bmp) image is used to conceal the data. These pixels will be used to embed data inside the copy. The pixels of the stego image can be accessed to retrieve the hidden data from the image. There are 2 stages involved. The 1st stage is to develop a steganography algorithm in instruction to skin the data which is within the image, and the 2nd stage is to develop a decryption algorithm that which uses a data retrieving method and also to retrieve concealed statistics that which is concealed inside the stego image.

2. SYSTEM ANALYSIS

The current system is a manual and time-consuming process. As the global use of the internet grows, so does the need for increased security. Internet developers are constantly working to make the internet free of jamming. Many techniques and algorithms are proposed to accomplish this. They are also working on how hackers act smartly to hack information and inventing new techniques to thwart hackers' intentions. Techniques that attempt to improve the embedding payload or robustness should keep imperceptibility in mind. The effects of different embedding payloads on audio quality may vary. In this project, the LSB method was used for audio-video steganography in order to achieve efficient results with minimal distortion. Using LSB steganography, we proposed an encoding and decoding technique for hiding data in image and audio files. By substituting the Least Significant Bit in an image with the message bits to be hidden, we can hide messages using the LSB steganography technique. If our message is too large, it will start modifying the second most top part, and so on, and an impartial observer will notice the changes in the image.

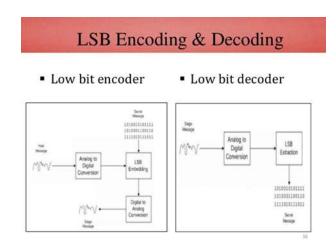


Fig:1 LSB Encoding & Decoding

LSB ENCODING AND DECODING ALGORITHM:

The deepest bit in a binary series of numbers is Least Significant Bit which is located at the far right of the string. LSB (Least Significant Bit) replacement is the procedure of regulating the cover images in smallest important bit pixels. This is a straightforward technique for implanting a communication into an image. The cover image LSB bits are cleared in this project. The MSB bits are then moved to replace the LSB bits. To accomplish this task, we use the commands in matlab:

1. bitand (which performs bitwise and operation)

2. bitshift (which perform bit shifting)

For the binary representation of hidden data we use Least Significant Bit to overwrite in a cover image for the sake of each byte in which a minimal and invisible amount of modification is done by using 24 bit color so that these minimal modifications can't be visible to human eye and we use three adjacent pixels of RGB i.e. Red, Green and Blue encoding which has shown below:

```
100101010000010111001001
100101100000101111001010
100111110001010011001011
```

The hided data which is of 9bits can be compressed in order to overlay the 9bits of Least Significant bit of the 101001101 so that the changed bits are shown below:

Note: 50% of the Least Significant Bits are changed successfully by hiding 9 bits at a cost of 4 bits change.

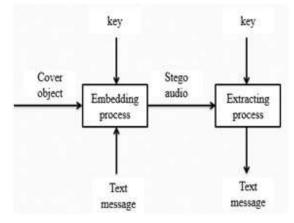


Fig: 2 Stegnographic technique Block diagram

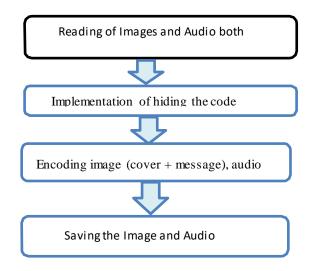


Fig: 3 Block diagram to represent hiding data



Fig: 4 Cover Image

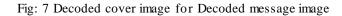




Fig: 5 Message Image



Fig: 6 Encoded Image



SECURED DATA HIDING IN AUDIO FILES USING AUDIO STEGANOGRAPHY ALGORITHM:

Superscript is hided where the data hiding is encoded by using a regular pair of motion vectors which are tempered by digital images and raw video as they are widely spread by water marking and data concealment. An identical message should be survived by using video lossy compression and the robustness attribute had less impact on the data size and reconstructed video.

The text bit stream is encoded as a phase angle difference between CMV sectors in data hiding for video files with phase of motion vector and a unique Steganographic Algorithm based on the motion vector phase. A few methods for disguising data in an audio file were previously discussed.

They are:

- Spread Spectrum.
- phase coding
- low bit encoding

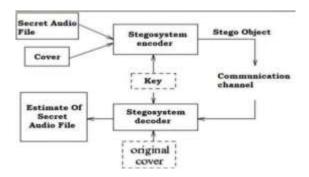


Fig:8 Audio Steganography Diagram

4. SYSTEM DESIGN: SYSTEM ARCHITECTURE:

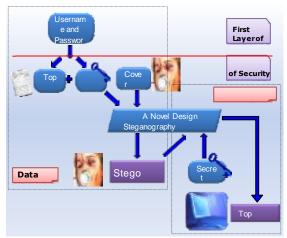


Fig: 8 System Architecture

Requirement document is the goal of design phase in order to provide a solution to the existing problem. In order to answer a domain opening moves are used. During the design phase, the system's requirements are met. To determine the quality of a software package designing is one of the important factor. For testing and maintenance there is a large impact in software. The result of the section is the style of the document. This document is intended as a solution blueprint and is later used during testing, implementation, and maintenance.

Generally, the design process is resolve into two stages System Design and Detailed Design. System design, also known as top- ranking design, aims to determine which modules should be part of the system, their conditions, and how they interact with one another to achieve the asked results. All of the system's main cognitive structure, train formats, affair formats, and major modules, as well as their specifications, are exactly placed at the top of the system style. The system or art of creating the design, factors, modules, interfaces, and knowledge for a system to meet similar conditions is known as system design. Druggies will read it because it applies systems proposition to development. In Detailed Design, the inner sense of each module laid out in software armature is determined. The fine print of a element square measure is sometimes laid out in a high- position style stoner review that's tone sufficient of the target language in which the operation software will ultimately be enforced throughout this section. The primary aim of system configuration is to distinguish modules, whereas the primary thing of conservative style is to plan the sense for each module.

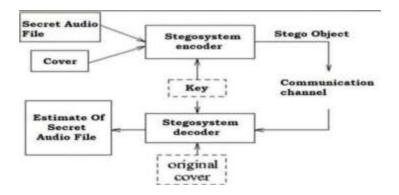


Fig:9 Audio block diagram.

5. CONCLUSION

We were able to successfully hide data in images and audio files in this project. Steganography is the transmission of secrets seemingly safe covers in order to hide the presence of a secret. Audio recording

steganography and results of it are becoming more widespread and very suitable. Residents are seeing to Steganography to avoid policies and permit messages secretly in the areas where cryptography, solid encryption are prohibited. Though the presented algorithm is simple and without flaws, it characterizes the weighty improvement from simple steganographic algorithms that don't practice keys. By spending algorithm, two revelries can communicate with a high degree of sureness that the communication cannot be detected. "Steganography" was designed with the goal of meeting as many user requirements as possible. Hence analysis and design phases were examined. The software engineering concepts were strictly followed. In addition, the principles ensured that the developed system was of high quality and met the needs of the users.

6. FUTURE ENHACEMENTS

It is not possible to create a system which can meets all of the requirements of a user. In the usage of a system, the user requirements change. Some future enhancements that can be made

- Upgrading of the system can be adaptable to desirable environment as the technology is emerging day by day.
- In the aspect of the future security issues, security can be improved using merging technologies like single sign-on.

7. **REFERENCES**

- [1] Artz, Donovan. "Digital steganography: hiding data within data." internet computing, IEEE 5.3 (2001): 75-80.
- [2] Amin, Muhalim Mohamed, et al. "Information hiding using steganography." Telecommunication Technology, 2003. NCTT 2003 Proceedings. 4th National Conference on. IEEE, 2003.
- [3] Shashikala Channalli, Ajay Jadhav, "Steganography An Art of Hiding Data" International Journal on Computer Science and Engineering Vol.1(3), 2009, 137-141
- [4] Morkel, Tayana, Jan HP Eloff, and Martin

S. Olivier. "An overview of image steganography." ISSA. 2005.

[5] Yuk Ying Chung, fang Fei Xu, "Development of video watermarking for MPEG2 video" City university of Hong Kong , IEEE 2006.

[6] Prof. Samir Kumar, Bandyopadhyay Barnali, Gupta Banik," LSB Modification and Phase encoding Technique of Audio Steganography Revisited". Vol.1 (4) IJARCCE 2012.

- [7] Chandrakar, Pooja, Minu Choudhary, and Chandrakant Badgaiyan. "Enhancement in Security of LSB based Audio Steganography using Multiple Files." International Journal of Computer Applications 73 (2013).
- [8] Taraghi-Delgarm, "Speech Watermarking", M.Sc. Thesis, Comptuer Engineering Department, Sharif University of Technology, Tehran, IRAN, May 2006

[9] M. Pooyan, A. Delforouzi, "LSB-based Audio Steganography Method Based on Lifting Wavelet Transform", in Proc. 7th IEEE International Symposium on Signal Processing and Information Technology (ISSPIT'07), December 2007, Egypt.

- [10] Singh, Pradeep Kumar, Hitesh Singh, and Kriti Saroha. "A survey on Steganography in Audio ." National Conference on Computing for Nation Development, Indiacom. 2009.
- [11] R.Anderson, F.Petitcolas: On the limits of the steganography, IEEE Journal Selected Areas in Communications, VOL .16, NO. 4, MAY 1998.

[12] Sridevi, R., A. Damodaram, and S. V. L. Narasimham. "Efficient method of Audio steganography by modified LSB algorithm and strong encryption key with enhanced security". Journal of Theoretical & Applied Information Technology 5.6 (2009).

[13] Pramatha Nath Basu, Tanmay Bhowmik,'On Embedding of Text in Audio – A case of Steganography' InternationalConference on Recent Trends in Information, Telecommunication and Computing.

[14] Fatiha Djebbar_1 and Beghdad Ayad2and Karim Abed Meraim3and Habib Hamam4 "Comparitive Study of Digital Audio Steganography Techniques" Survey paper2011.

[15] Jayaram P1, Ranganatha H R2, Anupama H S3 "Information Hiding Using Audio Steganography-A Survey"IJMA 2011 Vol.3, No.3, August.

[16] Abdulaleem Z. Al-Othmanil, Azizah Abdul Manaf2 and Akram M. Zeki3 "A Survey on Steganography Techniques in Real Time Audio Signals and Evaluation"IJCSI, Vol.9, Issuse 1, No 1, January 2012. International Journal of Computer Applications (0975 – 8887) Volume 73– No.7, July 2013 24

[17] Dr.H.B.Kekre, ArchanaAthawale, B.SwarnalataRao, UttaraAthawale, Increasing the capacity of the cover audio signal by using multiple LSBs for information hiding, IEEE Third International Conference on Emerging Trends in Engineering and Technology, 2010.

[18] Masahiro Wakiyama[†], Yasunobu Hidaka[†], Koichi Nozaki "An audio steganography by a low-bit coding method with wave files" IEEE 2010 Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing.

[19] Jisna Antony, Sobinc.c, Sherly A.P, "audio steganography in wavelet domain-a survey", International Journal of Computer Applications, Volume 52-No.13, August 2012.

[20] Muhammad Asad, JunaidGilani Adnan Khalid, "An Enhanced Least Significant Bit Modification Technique for Audio Steganography", 978-1-61284-941-6/1112011 IEEE

- [21] Dr. M. Thangamani, Jafar Ali Ibrahim, Information Technology E-Service Management System, International Scientific Global Journal in Engineering Science and Applied Research (ISGJESAR). Vol.1. Issue 4, pp. 13-18, 2017. <u>http://isgjesar.com/Papers/Volume1,Issue4/paper2.pdf</u>
- [22] Ibrahim, Mr S. Jafar Ali, K. Singaraj, P. Jebaroopan, and S. A. Sheikfareed. "Android Based Robot for Industrial Application." International Journal of Engineering Research & Technology 3, no. 3 (2014).
- [23] Ibrahim, S. Jafar Ali, and M. Thangamani. "Momentous Innovations in the Prospective Method of Drug Development." In Proceedings of the 2018 International Conference on Digital Medicine and Image Processing, pp. 37-41. 2018.
- [24] Ibrahim. S. Jafar Ali. and M. Thangamani. "Prediction of Novel Drugs and Diseases for Hepatocellular Carcinoma Based on Multi-Source Simulated Annealing Based Random Walk." Journal of medical systems 42, no. 10 (2018): 188. <u>https://doi.org/10.1007/s10916-018-1038-y</u>ISSN 1311-8080, <u>https://acadpubl.eu/hub/2018-119-16/1/94.pdf</u>
- [25] Jafar Ali Ibrahim. S, Mohamed Affir. A "Effective Scheduling of Jobs Using Reallocation of Resources Along With Best Fit Strategy and Priority", International Journal of Science Engineering and Advanced Technology(IJSEAT) – ISSN No: 2321-6905, Vol.2, Issue.2, Feb-2014, <u>http://www.ijseat.com/index.php/ijseat/article/view/62</u>
- [26] M. Thangamani, and Jafar Ali Ibrahim. S, "Knowledge Exploration in Image Text Data using Data Hiding Scheme," Lecture Notes in Engineering and Computer Science: Proceedings of The International MultiConference of Engineers and Computer Scientists 2018, 14-16 March, 2018, Hong Kong, pp352-357<u>http://www.iaeng.org/publication/IMECS2018/IMECS2018 pp352-357.pdf</u>
- [27] M. Thangamani. and Jafar Ali Ibrahim. S. "Knowledge Exploration in Image Text Data using Data Hiding Scheme." Lecture Notes in Engineering and Computer Science: Proceedings of The International MultiConference of Engineers and Computer Scientists 2018. 14-16 March, 2018, Hong Kong, pp352-357http://www.iaeng.org/publication/IMECS2018/IMECS2018 pp352-357.pdf
- [28] S. Jafar Ali Ibrahim and M. Thangamani. 2018. Momentous Innovations in the Prospective Method of Drug Development. In Proceedings of the 2018 International Conference on Digital Medicine and Image Processing (DMIP '18). Association for Computing Machinery, New York, NY, USA, 37–41. <u>https://doi.org/10.1145/3299852.3299854</u>
- [29] S. Jafar Ali Ibrahim and Thangamani, M "Proliferators and Inhibitors Of Hepatocellular Carcinoma", International Journal of Pure and Applied Mathematics (IJPAM) Special Issue of Mathematical Modelling of Engineering Problems Vol 119 Issue. 15. July 2018
- [30] Thangamani, M., and S. Jafar Ali Ibrahim. "Ensemble Based Fuzzy with Particle Swarm Optimization Based Weighted Clustering (Efpso-Wc) and Gene Ontology for Microarray Gene Expression."In Proceedings of the 2018 International Conference on Digital Medicine and Image Processing, pp. 48-55. 2018. <u>https://dl.acm.org/doi/abs/10.1145/3299852.3299866</u>
- [31] Dr.R.Chinnaiyan, Abishek Kumar (2017) "Reliability Assessment of Component Based Software Systems using Basis Path Testing", IEEE International Conference on Intelligent Computing and Control Systems, ICICCS 2017, 512 517
- [32] Dr.R.Chinnaiyan, AbishekKumar(2017), "Construction of Estimated Level Based Balanced Binary Search Tree", 2017 IEEE International Conference on Electronics, Communication, and Aerospace Technology (ICECA 2017), 344 - 348, 978-1-5090-5686-6.
- [33] R.Chinnaiyan, S.Somasundaram (2012), Reliability Estimation Model for Software Components using CEP", International Journal of Mechanical and Industrial Engineering (IJMIE), ISSN No.2231-6477, Volume-2, Issue-2, 2012, pp.89-93.
- [34] R.Chinnaiyan, S. Somasundaram (2011), "An SMS based Failure Maintenance and Reliability Management of Component Based Software Systems", European Journal of Scientific Research, Vol. 59 Issue 1, 9/1/2011, pp.123 (cited in EBSCO, Impact Factor: 0.045)
- [35] R.Chinnaiyan, S.Somasundaram(2011), "An Experimental Study on Reliability Estimation of GNU Compiler Components A Review", International Journal of Computer Applications, Vol.25, No.3, July 2011, pp.13-16. (Impact Factor: 0.814)
- [36] R.Chinnaiyan, S.Somasundaram(2010) "Evaluating the Reliability of Component Based Software Systems ", International Journal of Quality and Reliability Management, Vol. 27, No. 1., pp. 78-88 (Impact Factor: 0.406) Dr.R.Chinnaiyan, AbishekKumar(2017), Estimation of Optimal Path in Wireless Sensor Networks based on Adjancy List, 2017 IEEE International Conference on Telecommunication, Power Analysis and Computing Techniques (ICTPACT2017), 6,7,8th April 2017, IEEE

Vol. 6 No. 1(January-June, 2021)

International Journal of Mechanical Engineering

- [37] Ibrahim. S. Jafar Ali. and M. Thangamani. "Enhanced singular value decomposition for prediction of drugs and diseases with hepatocellular carcinoma based on multi-source bat algorithm based random walk." Measurement 141 (2019): 176-183. https://doi.org/10.1016/j.measurement.2019.02.056
- [38] Compound feature generation and boosting model for cancer gene classification Ibrahim, S. Jafar Ali Ibrahim., Affir, A.M., Thangamani, M.International Journal of Engineering Trends and Technology, 2020, 68(10), pp. 48–51, Doi No:doi:10.14445/22315381/IJETT-V68I10P208 <u>https://ijettjournal.org/Volume-68/Issue-10/IJETT-V68I10P208.pdf</u>
- [39] Innovative drug and disease prediction with dimensionality reduction and intelligence based random walk methods, Ibrahim, S.J.A., Thangamani, M.International Journal of Advanced Trends in Computer Science and Engineering, 2019, 8(4), pp. 1668–1673, <u>https://www.warse.org/IJATCSE/static/pdf/file/ijatcse93842019.pdf</u>
- [40] R. Ganesan, M. Thangamani, S. Jafar Ali Ibrahim, "Recent Research Trends and Advancements in Computational Linguistics", International Journal of Psychosocial Rehabilitation Vol 24, no 8 (2020):1154-1162, DOI: <u>10.37200/LJPR/V24I8/PR280128</u>
- [41] C. Narmatha, Dr. M. Thangamani, S. Jafar Ali Ibrahim, "Research Scenario of Medical Data Mining Using Fuzzy and Graph theory", International Journal of Advanced Trends in Computer Science and Engineering, Vol 9, No 1 (2020): 349-355
- [42] Dr.R.Chinnaiyan, R.Divya (2018), "Reliable AIBasedSmartSensorsforManagingIrrigationResources in Agriculture", Lecture Notes on DataEngineeringandCommunicationsTechnologies,SpringerInternationalconferenceonComputerNetworksandInventiveCommunicati onTechnologies(ICCNCT-2018),August2018
- [43] Dr.R.Chinnaiyan,S.Balachandar(2018), "Reliable Digital Twin for Connected Footballer", LectureNotesonDataEngineeringandCommunicationsTechnologies, SpringerInternationalconferenceonComputerNetworksandInvent iveCommunicationTechnologies(ICCNCT- 2018), August 2018
- [44] Dr.R.Chinnaiyan,S.Balachandar(2018), "Centralized Reliability and Security Management of DatainInternet of Things (IoT) with Rule Builder" Lecture Notes on Data Engineering and Communications Technologies, Springer Internat ional conference on Computer Networks and Inventive Communication Technologies (ICCNCT 2018), August 2018 (Online)
- [45] Dr.R.Chinnaiyan, AbishekKumar(2017)"Reliability Assessment of Component Based Software Systems using Basis Path Testing", IEEEInternational Conference on Intelligent Computing and Control Systems, ICICCS2017, 512-517
- [46] Dr.R.Chinnaiyan,AbishekKumar(2017,"ConstructionofEstimatedLevelBasedBalancedBinarySearchTree",2017IEEEInternationalConferenceonElectronics,Communication,andAerospaceTechnology(ICECA2017),344 348,978-1-5090-5686-6.
- [47] Dr.R.Chinnaiyan, AbishekKumar(2017), Estimationof Optimal Path in Wireless Sensor Networks basedonAdjancyList,2017IEEEInternationalConference on Telecommunication,Power Analysisand Computing Techniques (ICTPACT2017),6,7,8thApril2017,IEEE978-1-5090-3381-2.
- [48] Dr.R.Chinnaiyan, R.Divya (2017), "Reliability Evaluation of Wireless Sensor Networks", IEEE International Conference on Intelligent Computing and Control Systems, ICICCS 2017, 847–852
- [49] Dr.R.Chinnaiyan, Sabarmathi.G(2017), "InvestigationsonBigDataFeatures, ResearchChallengesandApplications", IEEEInternational Conference on Intelligent Computing and ControlSystems, ICICCS 2017, 782–786
- [50] G.Sabarmathi,Dr.R.Chinnaiyan(2018), "EnvisagationandAnalysisofMosquitoBorneFevers AHealthMonitoringSystembyEnvisagative Computing using Big Data Analytics"inICCBI2018– Springeron19.12.2018to20.12.2018(RecommendedforScopusIndexedPublicationIEEEXploredigital library)
- [51] G.Sabarmathi, Dr.R.Chinnaiyan, ReliableDataMiningTasksandTechniquesforIndustrialApplications, IAETSDJOURNALFORADVA NCEDRESEARCHINAPPLIEDSCIENCES, VOLUME 4, ISSUE 7, DEC/2017, PP-138-142, ISSN NO:2394-8442

International Journal of Mechanical Engineering