



Notice for the PhD Viva-Voce Examination

Mr Gurunath R (Registration Number: 1942062), PhD scholar at the School of Sciences, CHRIST (Deemed to be University), Bangalore will defend his PhD thesis at the public viva-voce examination on Thursday, 9 November 2023 at 10.30 am in Room No. 044, Ground Floor, R & D Block, CHRIST (Deemed to be University), Bengaluru - 560029.

Title of the Thesis : **Artificial Intelligence-Based Steganography Model for Social Media Data Set**


Discipline : **Computer Science**

External Examiner : **Dr Amit Dua**
(Outside Karnataka, Maharashtra and Uttar Pradesh)
Associate Professor
Department of CSIS
BITS Pilani, Pilani Campus
Rajasthan

External Examiner : **Dr Daya Sagar Gupta**
(Within Karnataka, Maharashtra and Uttar Pradesh)
Professor
Department of Computer Science and Engineering
Rajiv Gandhi Institute of Petroleum Technology
Jais Amethi
Uttar Pradesh - 229304

Supervisor : **Dr Debabrata Samanta**
Associate Professor
Department of Statistics and Data Science
School of Sciences
CHRIST (Deemed to be University)
Bengaluru - 560029
Karnataka

The members of the Research Advisory Committee of the Scholar, the faculty members of the Department and the School, interested experts and research scholars of all the branches of research are cordially invited to attend this open viva-voce examination.



Registrar

Place: Bengaluru
Date: 20 October 2023

ABSTRACT

Steganography, one of the data security mechanisms under our investigation, shields legitimate messages from hackers and spies by employing data hiding. Data protection is currently the top priority due to the significant advancements in information technology due to high-security concerns. Traditional techniques for maintaining data confidentiality include steganography and cryptography; the distinction is that steganography does not naturally arouse suspicion, whereas cryptography does. Traditional linguistic steganographic methods suffer from limitations in automation, accuracy, and the volume and substance of cover and concealed text. The robustness and undetectability properties of these approaches also require improvement. Third-party vulnerability is often too high for conventional techniques to handle. Artificial intelligence is increasingly replacing traditional model creation in steganography. Information transmitted through Online Social Networks (OSN) is obviously not safe. Steganography along with encryption can make a difference with regard to privacy of information in transit.

The research study aims to build algorithms or models and assess steganography's robustness, security, undetectability, and embedding ability. Two distinct types of data concealing employed for investigation: text and image. The results were encouraging when we initially tested our Laplacian model using image steganography and compared with benchmark methods. The second experiment, which is based on AI, generates the cover text using secret information, examines the security and robustness of steganography.

The study compared suggested text steganography model, 3-bit data concealing, with other existing techniques in order to ascertain the undetectability factor. The first experiment used MATLAB tools, and the second used the markovify python module, RNN (Recurrent Neural networks), and the Huffman tree. Further format-based steganography methods utilized in the following experiment. proposed research revealed that the security of the embedded information would be compromised along with the undetectability factor when the amount of embedding data exceeds a particular level.

Keywords: Steganography, Data Hiding, Online Social networks, RNN, Markov chain, Huffman Tree, Artificial Intelligence, Laplace transform

Publications:

1. **Gurunath, R.**, Alahmadi Ahmed H., Samanta Debabrata, Khan Mohammad Zubair and Alahmadi Abdulrahman (2021). A novel approach for linguistic steganography evaluation based on artificial neural networks. *IEEE Access*, 9, 120869- 120879. @ SCI-Q1, SCOPUS
2. **Gurunath, R.**, Klaib Mohammad Fadel Jamil, Samanta Debabrata and Khan Mohammad Zubair (2021). *Social Media and Steganography: Use, Risks and Current Status*. *IEEE Access*, 9, 153656-153665. @ SCI-Q1, SCOPUS
3. **Gurunath, R.** and Samanta Debabrata (2022). A novel approach for semantic web application in online education based on steganography. *International Journal of Web-Based Learning and Teaching Technologies (IJWLTT)*, 17(4), 1-13. @SCIQ3, SCOPUS, IGI Global
4. **Gurunath, R.**, Samanta, D. (2020). Studies on encrypted secret data storage techniques analogous to steganography. *International Journal of Advanced Science and Technology*, 29(2), 3705-3711. SCOPUS, IJAST
5. **Gurunath, R.**, Samanta, D. (2021). *Advances in Text Steganography Theory and Research: A Critical Review and Gaps. Multidisciplinary Approach to Modern Digital Steganography*, 50-74. Book chapter, IGI Global, @SCOPUS, IGI GLOBAL
6. **Gurunath, R.**, Samanta, Debabrata and Pandey, Digvijay (2022). *Insights Into Deep Steganography: A Study of Steganography Automation and Trends*. *Cyber Security and Network Security*, 129-155. Book Chapter, WILEY-SCRIVENER, IEEE Xplore