Dhirajlal Gandhi College of Technology

Achievements of Faculty Members

Papers Published in International Conferences

AY 2021-2022

SRI VENKATESWARAA
COLLEGE OF TECHNOLOGY
BHB Nagar, Vadakal, Sriperumbudur - 602105

International Conference on Science, Engineering and Technology

CERTIFICATE

ICSET 2k22

This is to Certify that Dr./Mr./Mrs.

RUBINI P

has presented a paper entitled

WEATHER ANTENNA USING RTL-SDR

in Virtual 3rd International Conference on Science, Engineering and Technology (ICSET 2k22) held on 26th & 27th May 2022 organised by Sri Venkateswaraa College of Technology, Chennai

Convenor

Principal

SRI VENKATESWARAA
COLLEGE OF TECHNOLOGY
BHB Nagar, Vadakal, Sriperumbudur - 602105

International Conference on Science, Engineering and Technology

ICSET 2k22

CERTIFICATE

This is to Certify that Dr./Mr./Mrs.

VETRISELVAN N

has presented a paper entitled

WEATHER ANTENNA USING RTL-SDR

in Virtual 3rd International Conference on Science, Engineering and Technology
(ICSET 2k22) held on 26th & 27th May 2022 organised by
Sri Venkateswaraa College of Technology, Chennai

Convenor

Principal

INTERNATIONAL CONFERENCE ON EMERGING BIOMATERIALS FOR ADVANCED APPLICATIONS (ICEBAA-2022)

Jointly Organized by

Department of Physics & Department of Chemistry, Periyar University, Salem, Tamil Nadu
NAAC A++ Grade - State University - NIRF Rank 73, ARIIA Rank 10

Department of Clinical Research, Sibar Institute of Dental Sciences (SIDS), Guntur, Andhra Pradesh

Endorsed by

Society for Biomaterials & Artificial Organs (India) &
Society for Tissue Engineering & Regenerative Medicine (India)

Silver Jubilee Year
(1997-2022)

stermi

Certificate of Participation and Poster Presentation

This is to certify that

S. VIJAYANATH, Dhirajlal Gandhi College of Technology.

has participated and presented a research paper entitled

Porous ZnO/Carbon nanocomposites derived from metal organicFrameworks for highly efficient dye sensitized solar cells.

in ICEBAA-2022 virtual conference on 21.04.2022 & 22.04.2022.

Dr. Vivekanand S Kattimani	Prof. Dr. D. Gopi	Dr. E.K. Girija	Dr. L. Krishna Prasad	Prof. R. Jagannathan
Organizing Secretary	Convener	Convener	Dean	Vice Chancellor
SIDS	Periyar University	Periyar University	SIDS	Periyar University

Performance Analysis of Stego-Image Security in Machine Learning

[1]*Sheela V.K*

Assistant Professor, Department of Information Technology
, Viswajyothi college of Engineering and Technology,
Kerala, India
sheelajeevakumar@gmail.com

[2]*A. Nedumaran*

Department of Electrical and Computer Engineering, Wollo
University, Kombolcha Institute of Technology, Ethiopia
maran.van @gmail.com

[3]*P.Vidhya Saraswathi*

Department of Computer Applications,
Kalasalingam Academy of Research and Education,
Krishnan koil, TN, India,
vidhyasaraswathi.p@gmail.com

[4]*P. Karthika*

Department of Computer Applications,
Kalasalingam Academy of Research and Education,
Krishnan koil, TN, India,
karthikasivamr@gmail.com

Abstract—A numerical way to deal with steganalysis is introduced in this paper with straight steganography being the primary core interest. A numerically formal meaning of steganalysis is given trailed by definitions for uninvolved and dynamic steganalysis. The steganalysis issue is figured as visually impaired framework ID and conditions for recognizability (effective steganalysis) are determined. A methodology to deliberately misuse any accessible spatial and worldly variety data for proficient steganalysis is additionally examined. Test results are given for steganalysis of Gaussian circulated, spread range picture steganography and watermarking. The proposed procedure is seen to deliver great outcomes for an assortment of execution measures.

Keywords— Steganalysis; Security; Machine Learning; Steganography; Spectrum Image

I. Introduction (Heading 1)

Steganalysis is a generally new part of exploration. While steganography (which is fairly not quite the same as watermarking) manages procedures for concealing data, the objective of steganalysis is to identify as well as gauge conceivably concealed data from watched information with practically zero information about the steganography calculation or potentially its boundaries[1]. Any reasonable person would agree that steganalysis is both a craftsmanship and a science. The craft of steganalysis assumes a significant function in the choice of highlights or qualities an ordinary stego message may display while the science helps in dependably testing the chose highlights for the presence of concealed data[2]. While it is conceivable to plan a sensibly decent steganalysis strategy for a particular steganography calculation, the drawn out objective must be to build up a steganalysis system that can work adequately at any rate for a class of steganography techniques.

II. Literature Review

In a customary steganography set-up figured as a detainee's concern, Alice wishes to send a mystery message to Bob by concealing data in a spread message. The stego message (spread + message) goes through Wendy (a superintendent) who examines it to decide whether there is anything dubious about it[3],[4],[5],[6]. Wendy could perform one or a few tests to choose if the message from Alice to Bob contains any mystery data. On the off chance that her choice is negative, at that point Wendy advances the message to Bob— Wendy goes about as an inactive superintendent. Then again, Wendy can adopt a moderate strategy and alter all the messages from Alice to Bob regardless of if any data is covered up by Alice. For this situation, Wendy is called a functioning superintendent[7]. Obviously, Wendy will have imperatives, for example, the greatest reasonable contortion while altering the message and so forth. For instance, on the off chance that the spread messages are advanced pictures, at that point Wendy can't alter the stego message to a degree that perceptually huge contortions are instigated.

III. Implementation of Machine Learning Method

We consider the situation where the steganography key is the equivalent for at any rate two stego messages[8],[9],[10]. This is certifiably not a prohibitive presumption since Alice and Bob could trade a steganography key at first and later utilize this key to implant and concentrate different mystery data. For instance, the steganography key could be the pixels of a picture where the mystery message is shrouded, for example, in LSB picture steganography.
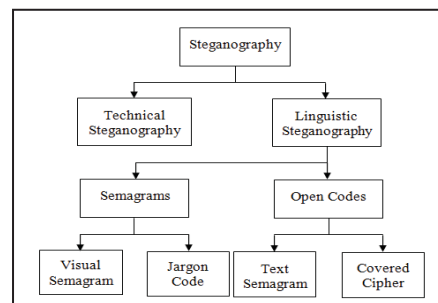

Fig. 1. *Simplifies of Steganography Security*

Big Data Link Stability-Based Path Observation for Network Security

Nedumaran Arappali, Melaku Tamene Mekonnen, Wondatir Teka Tefera, B. Barani Sundaram, and P. Karthika

Abstract Wireless ad hoc network [WANET] systems are creating multihop communication structure between the mobiles to transfer the data groups. The remarkable qualities of remote frameworks cause the correspondence to interface among the conflicting mobiles. To manage high convey ability and biological blocks, most physical directing shows will not believe the stable associations during pack communication, which prompts the elevated delay and bundle reducing in the mastermind. The proposed research work recommends a way perception support physical steering convention that specifies POPR for WANET. The anticipated guiding show merges the relative partition, course and mid-expand forwarder center point with transfer thickness to propel data toward the objective in order to recover physical sending among the connection point. Multiplication results illustrate the projected directing convention, which performs superior to the existing arrangements.

Keywords Physical routing protocol · Direction · Traffic density · Link stability · Network security

1 Introduction

Transformation past specialists think about wireless ad hoc networks (WANETs) that empower unavoidable accessibility among mobiles and do not rely upon expensive framework system [1]. Correspondence among mobiles and earlier establishment release a lot of different sorts of talented applications for explorers with drivers. The applications are ought to give security with reassurance and help drivers to

N. Arappali (✉) · M. T. Mekonnen · W. T. Tefera
Department of Electrical and Computer Engineering, Wollo University, Kombolcha Institute of Technology, Kombolcha, Ethiopia

B. Barani Sundaram
Department of Computer Science, College of Informatics, Bule Hora University, Bule Hora, Ethiopia

P. Karthika
Department of Computer Application, Kalasalingam Univerity, Viruthunagar, Tamilnadu, India