



PROCEEDING

IEEE COMNETSAT

2022

IEEE International Conference on
Communications, Network,
and Satellite.



Solo, Indonesia
November 3-5, 2022

ISBN : 978-1-6654-6030-9



Co-Host :



USM

Patron :



Copyright ©2022 by IEEE.
All rights reserved.

Copyright and Reprint Permission

Abstracting is permitted with credit to the source. Libraries are permitted to photocopy beyond the limit of U.S. copyright law for private use of patrons those articles in this volume that carry a code at the bottom of the first page, provided the per-copy fee indicated in the code is paid through Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923.

For reprint or republication permission, email to IEEE Copyrights Manager at pubspermissions@ieee.org.

IEEE Catalog Number: CFP2231S-ART

ISBN 978-1-6654-6030-9

Additional copies of this proceeding may be ordered to:
Institut Teknologi Telkom Purwokerto
Central Java, Indonesia 53147

Welcome Message from General Chair

The 11th Comnetsat 2022

(Thursday – Saturday), 03th – 05th November 2022



On behalf of the Organizing Committee, I am very delighted to welcome you all keynote speakers, presenters, and participants to the 11th 2022 IEEE International Conference on Communications, Network, and Satellite (IEEE Comnetsat 2022). IEEE Comnetsat is an annual conference of the IEEE Communications Society (ComSoc) Indonesia Chapter, the IEEE Indonesia Section, and the IEEE AESS/GRSS Indonesia Joint Chapter. This year, IEEE Comnetsat 2022 is organized by Institut Teknologi Telkom Purwokerto (ITTP) and Universitas Semarang (USM).

IEEE Indonesia Section has conducted many activities over 30 years in Indonesia. Regarding collaboration, the IEEE Indonesia section has a good and mutual relationship with ICT organizations, Industries, Governments, Universities, and the Community in Indonesia. We hope other high-quality conferences will be continued and strengthened so that the result will benefit and positively impact human beings, especially Indonesian people.

The core purpose of IEEE is to foster technological innovation and excellence for the benefit of humanity. Here, researchers, scientists, students, and practitioners come together to participate and present their latest research findings, developments, and applications related to the various aspects of the current state of technology and the outcome of ongoing research in the area of Communications, Networks, and Satellite Systems.

Despite the challenges, the IEEE Comnetsat 2022 Organizing Committee and volunteers worked very hard to complete the conference program, uphold the quality of conferences, and meet authors' expectations. IEEE Comnetsat 2022 aims to address the current state of technology and the outcome of ongoing research in the application of computer and communication, networks, satellite systems, broadband photonic systems, data science, and artificial intelligence.

Last but not least, I would also like to express sincere and special thanks to the IEEE Communications Society (ComSoc) Indonesia Chapter, the IEEE Indonesia Section, and the IEEE AESS/GRSS Indonesia Joint Chapter, which have shown great support to this event.

I hope you will benefit from this conference and enjoy networking with colleagues from across the globe for future collaboration globally. Your support will also make this a memorable and successful event.

Wishing you all to join us to make IEEE Comnetsat 2022 a successful and safe event. Thank you.

Sincerely,

Dr. Arfianto Fahmi, S.T., M.T.

General Chair

COMMITTEES

Advisory Board:

Dr-Ing Wahyudi Hasbi, M.Kom
Prof. Dr. Ir. Gamantyo Hendrantoro, Ph.D.
Dr. Ign. Wiseto P. Agung
Dr. Arifin Nugroho
Dr. Muhammad Ary Murti, M.T
Arief Hamdani Gunawan, SMIEEE
Dr. Bambang Setia Nugraha

General Chair :

Dr. Arfianto Fahmi, M.T

General Co-chair:

Dr. Anggun Fitriani Isnawati, M.Eng

Technical Program Committee (TPC)

Chair:

Dr. Wahyu Pamungkas, M. T

Co-Chair:

Dr. Tenia Wahyuningrum, M.T
Eko Fajar Cahyadi, S.T., M.T., Ph.D.

Technical Program Committee (TPC) Member:

Prof. Abdallah Makhoul (University of Franche-Comté, France)
Prof. Abdelmadjid Bouabdallah (Universite de Technologie – Compiègne, France)
Prof. Adão Silva (Instituto de Telecomunicações (IT)/University of Aveiro, Portugal)
Prof. Ahmed Mehaoua (University of Paris Descartes, France)
Prof. Alvaro Suárez-Sarmiento (University of Las Palmas de Gran Canaria, Spain)
Prof. António Rodrigues (IT / Instituto Superior Técnico, Portugal)
Prof. Arnaldo Oliveira (Universidade de Aveiro – DETI / Instituto de Telecomunicações – Aveiro, Portugal)
Prof. Aws Yonis (Ninevah University, Iraq)
Prof. Bang Chul Jung (Chungnam National University, Korea (South))
Prof. Bernd Wolfinger (University of Hamburg, Germany)

Prof. Bong Jun Choi (Soongsil University, Korea (South))
Prof. Carl Debono (University of Malta, Malta)
Prof. Carla Raffaelli (University of Bologna, Italy)
Prof. Carlos Becker Westphall (Federal University of Santa Catarina, Brazil)
Prof. Chao Fang (Beijing University of Technology, China)
Prof. Chao Shen (Xi'an Jiaotong University, China)
Prof. Chao-Tsun Chang (Hsiuping University of Science & Technology, Taiwan)
Prof. Chia-Ho Ou (National Pingtung University, Taiwan)
Prof. Demosthenes Vouyioukas (University of the Aegean, Greece)
Prof. Dennis Pfisterer (University of Luebeck, Germany)
Prof. Ding Wang (Nankai University, China)
Prof. Domenico Ciuonzo (University of Naples Federico II, IT, Italy)
Prof. Dushantha Nalin K. Jayakody (Tomsk Polytechnic University, Russia)
Prof. Eduard Babulak (Liberty University, USA)
Prof. Eirini Eleni Tsiropoulou (University of New Mexico, USA)
Prof. Eisuke Kudoh (Tohoku Institute of Technology, Japan)
Prof. Eric Renault (LIGM, Université Gustave Eiffel, CNRS, ESIEE Paris, France)
Prof. Fang Yang (Tsinghua University, China)
Prof. Fernando Velez (University of Beira Interior, Portugal)
Prof. Francesco Palmieri (Università di Salerno, Italy)
Prof. Fuhui Zhou (Nanjing University of Aeronautics and Astronautics, China)
Prof. Gamantyo Hendrantoro (Institut Teknologi Sepuluh Nopember, Indonesia)
Prof. Guy Pujolle (Sorbonne University, France)
Prof. Gyu Myoung Lee (Liverpool John Moores University, United Kingdom (Great Britain))
Prof. Hacene Fouchal (Université de Reims Champagne-Ardenne, France)
Prof. Hans-Juergen Zepernick (Blekinge Institute of Technology, Sweden)
Prof. Harald Øverby (Norwegian University of Science and Technology, Norway)
Prof. Harry Skianis (University of the Aegean, Greece)
Prof. Homayoun Nikookar (Netherlands Defence Academy, The Netherlands)
Prof. Ickho Song (Korea Advanced Institute of Science and Technology, Korea (South))
Prof. Ikmo Park (Ajou University, Korea (South))
Prof. Ioannis Moscholios (University of Peloponnese, Greece)
Prof. Jae-Hyun Park (Chung-Ang University, Korea (South))
Prof. Jenhui Chen (Chang Gung University, Taiwan)
Prof. Jiann-Liang Chen (National Taiwan University of Science and Technology, Taiwan)

Prof. Ji-Hoon Yun (Seoul National University of Science and Technology, Korea (South))
Prof. João Rebola (Instituto de Telecomunicações Lisbon, Portugal)
Prof. Joel Rodrigues (Federal University of Piauí (UFPI), Brazil)
Prof. Johann Marquez-Barja (University of Antwerpen & imec, Belgium)
Prof. Joongheon Kim (Korea University, Korea (South))
Prof. Jorge Sá Silva (University of Coimbra, Portugal)
Prof. Junping Geng (Shanghai Jiaotong University, China)
Prof. Kasturi Vasudevan (Indian Institute of Technology Kanpur, India)
Prof. Kazuo Mori (Mie University, Japan)
Prof. Klaus David (University of Kassel, Germany)
Prof. Knud Skouby (Aalborg University, Denmark)
Prof. Koichi Maru (Kagawa University, Japan)
Prof. Konstantin Mikhaylov (University of Oulu, Finland)
Prof. Kuo-Chang Ting (Minghsin University of Science and Technology, Hsinchu, Taiwan)
Prof. Lahcène Mitiche (University of Djelfa, Algeria)
Prof. Li Xu (Chinese Academy of Sciences, China)
Prof. Li Xu (Fujian Normal University, China)
Prof. Liudong Xing (University of Massachusetts, Dartmouth, USA)
Prof. Ljiljana Trajković (Simon Fraser University, Canada)
Prof. Lorenzo Vangelista (University of Padova, Italy)
Prof. Lu Lu (University of Chinese Academy of Sciences, Hong Kong)
Prof. Lyes Khoukhi (ENSICAEN, Normandie University, GREYC CNRS Lab., France)
Prof. Mamoun Alazab (Charles Darwin University, Australia)
Prof. Manoj Bs (Indian Institute of Space Science and Technology, India)
Prof. Marcelo Alencar (Federal University of Campina Grande, Brazil)
Prof. Marco Listanti (University of Rome “La Sapienza”, Italy)
Prof. Mario Tanda (Università di Napoli Federico II, Italy)
Prof. Mariusz Glabowski (Poznan University of Technology, Poland)
Prof. Michele Ruta (Politecnico di Bari, Italy)
Prof. Miguel Franklin de Castro (Federal University of Ceará, Brazil)
Prof. Miodrag Potkonjak (UCLA, USA)
Prof. Mitchai Chongcheawchamnan (Prince of Songkla University, Thailand)
Prof. Mohamad Yusoff Alias (Multimedia University, Malaysia)
Prof. Mohamed Mosbah (CNRS-LaBRI UMR 5800, University Bordeaux, Bordeaux-INP, France)
Prof. Mohammad Matin (North South University, Bangladesh)

Prof. Nabanita Das (Indian Statistical Institute, India)
Prof. Nhu-Goc Dao (Sejong University, Korea (South))
Prof. Nuno Pombo (University of Beira Interior, Portugal)
Prof. Pascal Lorenz (University of Haute Alsace, France)
Prof. Paulo de Lira Gondim (Universidade de Brasilia, Brazil)
Prof. Paulo Monteiro (Universidade de Aveiro, Portugal)
Prof. Paulo Pinto (Universidade Nova de Lisboa, Portugal)
Prof. Petra Perner (IBaI Leipzig, Germany)
Prof. Pravati Swain (National Institute of Technology, Goa, India)
Prof. Rafael Caldeirinha (Polytechnic Institute of Leiria, Portugal)
Prof. Richard Lin (National Sun Yat-sen University, Taiwan)
Prof. Ridha Hamila (Qatar University, Qatar)
Prof. Robert Schober (University of British Columbia, Canada)
Prof. Roberto Garello (Politecnico di Torino, Italy)
Prof. Rogerio Dionisio (Instituto Politecnico de Castelo Branco, Portugal)
Prof. Rosaura Palma-Orozco (Instituto Politécnico Nacional, Mexico)
Prof. Sabrina Sicari (University of Insubria, Italy)
Prof. Salahuddin Mohammad Masum (Southwest Tennessee Community College, USA)
Prof. Satoshi Takahashi (Hiroshima City University, Japan)
Prof. Seiji Fukushima (Kagoshima University, Japan)
Prof. Shashikant Patil (SVKMs NMiMS Mumbai India, India)
Prof. Simon Pietro Romano (University of Napoli Federico II, Italy)
Prof. Takuya Asaka (Tokyo Metropolitan University, Japan)
Prof. Telmo Fernandes (IPLeiria / Institute of Telecommunications, Portugal)
Prof. Theo Swart (University of Johannesburg, South Africa)
Prof. Vicente Casares-Giner (Universitat Politècnica de València, Spain)
Prof. William Lehr (Massachusetts Institute of Technology, USA)
Prof. Xiaochuan Sun (NCST, China)
Prof. Yi Shang (University of Missouri, USA)
Prof. Yi-Han Chiang (Osaka Prefecture University, Japan)
Prof. Yiu-Wing Leung (Hong Kong Baptist University, Hong Kong)
Prof. Yoon-Ho Choi (Pusan National University, Korea (South))
Prof. You-Chiun Wang (National Sun Yat-Sen University, Taiwan)
Prof. Yousaf Bin Zikria (Yeungnam University, Korea (South))
Prof. Zalan Heszberger (Budapest University of Technology and Ec., Hungary)

- Dr. Aashish Mathur (Indian Institute of Technology Jodhpur, India)
- Dr. Abderrahmen Mtibaa (University of Missouri St. Louis, USA)
- Dr. Adriaan van Wijngaarden (Bell Laboratories, Nokia, USA)
- Dr. Adrian Kliks (Poznan University of Technology, Poland)
- Dr. Ajay Singh (Indian Institute of Technology Jammu, India)
- Dr. Ala Khalifeh (German University of Jordan, Jordan)
- Dr. Alban Duverdier (Centre National D'Etudes Spatiales (CNES), France)
- Dr. Alberto Gotta (ISTI-CNR, Italy)
- Dr. Alessandro Carrega (CNIT, Italy)
- Dr. Alexandru Vulpe (University Politehnica of Bucharest, Romania)
- Dr. Amitava Mukherjee (Globsyn Business School, Kolkata, India)
- Dr. Angelos Liveris (Wavelab Inc, USA)
- Dr. Anna Antonyová (University of Prešov in Prešov, Slovakia)
- Dr. Anwer Al-Dulaimi (EXFO Inc., Canada)
- Dr. Argyrios Kyrgiazos (University of Surrey, United Kingdom (Great Britain))
- Dr. Arianna D'Ulizia (CNR, Italy)
- Dr. Atef Abdrabou (UAE University, United Arab Emirates)
- Dr. Aveek Das (Palo Alto Networks, USA)
- Dr. Barry Evans (University of Surrey, United Kingdom (Great Britain))
- Dr. Bongkyo Moon (Quantum Informatics Research (QIR), Korea (South))
- Dr. Bramah Hazela (Amity University Uttar Pradesh India, India)
- Dr. Cahya Damarjati (Universitas Muhammadiyah Yogyakarta, Indonesia)
- Dr. Carlo Augusto Grazia (University of Modena and Reggio Emilia, Italy)
- Dr. Cedric Adjih (INRIA, France)
- Dr. Chaker Abdelaziz Kerrache (University of Laghouat, Algeria)
- Dr. Chau Yuen (Singapore University of Technology and Design, Singapore)
- Dr. Chayan Bhar (National Institute of Technology Warangal, India)
- Dr. Chi-Fu Huang (National Chung Cheng University, Taiwan)
- Dr. Chih-Lin Hu (National Central University, Taiwan)
- Dr. Chinmoy Kundu (University College Dublin, Ireland)
- Dr. Chongwen Huang (Zhejiang University, China)
- Dr. Chunqiang Hu (Chongqing University, China)
- Dr. Cicek Cavdar (KTH Royal Institute of Technology, Sweden)
- Dr. Dariusz Wiecek (National Institute of Telecommunications, Poland)
- Dr. De Mi (University of Surrey, United Kingdom (Great Britain))

- Dr. Debashis De (West Bengal University of Technology, India)
- Dr. Deepak Mishra (IIST, India)
- Dr. Deyun Gao (Beijing Jiaotong University, China)
- Dr. Dimitri Papadimitriou (University of Antwerp – imec, Belgium)
- Dr. Dimitris Chatzopoulos (Hong Kong University of Science and Technology, Hong Kong)
- Dr. Donghyun Kim (Georgia State University, USA)
- Dr. Ekasit Nugoolcharoenlap (Rajamangala University of Technology Rattanakosin, Thailand)
- Dr. Elyas Rakhshani (Delft University of Technology, TU Delft, The Netherlands)
- Dr. Felice Manlio Bacco (National Research Council (CNR), Italy)
- Dr. Felipe Cruz-Pérez (Cinvestav-IPN, Mexico)
- Dr. Fernando Guiomar (Instituto de Telecomunicações, Portugal)
- Dr. Floriano De Rango (University of Calabria, Italy)
- Dr. Francesco Gringoli (CNIT/University of Brescia, Italy)
- Dr. Gang Wang (PCTEL, Inc., USA)
- Dr. Ghadah Aldabbagh (King Abdulaziz University, USA)
- Dr. Giuseppe Ruggeri (University of Reggio Calabria, Italy)
- Dr. Go Hasegawa (Tohoku University, Japan)
- Dr. Guixin Ye (Northwest University, China)
- Dr. Gustavo Marfia (Università di Bologna, Italy)
- Dr. Haibo Dai (Nanjing University of Posts and Telecommunications, China)
- Dr. Hang Li (University of Technology Sydney, Australia)
- Dr. Hemant Purohit (Jodhpur Institute of Engineering & Technology, India)
- Dr. Heri Wijayanto (University of Mataram, Indonesia)
- Dr. Hing Keung Lau (Hong Kong Institute of Vocational Education (Tuen Mun), Hong Kong)
- Dr. Hiromasa Habuchi (Ibaraki University, Japan)
- Dr. Honghai Zhang (Google, USA)
- Dr. Hyung Jae Chang (Troy University – Montgomery, USA)
- Dr. Ibrahim Develi (Erciyes University, Turkey)
- Dr. Ilija Basicovic (University of Novi Sad, Serbia)
- Dr. Ioakeim Samaras (Intracom Telecom, Greece)
- Dr. Jad Nasreddine (Rafik Hariri University, Lebanon)
- Dr. Javier Gozalvez (Universidad Miguel Hernandez de Elche, Spain)
- Dr. Jean-Marc Kelif (Orange Labs, France)
- Dr. Jia Hu (University of Exeter, United Kingdom (Great Britain))
- Dr. Jin Cao (Xidian University, China)

- Dr. Jing Chen (Wuhan University, China)
- Dr. Jingjing Cui (University of Southampton, United Kingdom (Great Britain))
- Dr. John Vardakas (IQUADRAT Informatica S. L. Barcelona, Spain)
- Dr. Joong-Lyul Lee (University of North Carolina at Pembroke, USA)
- Dr. Jose Santa (Technical University of Cartagena, Spain)
- Dr. José Luis Hernandez Ramos (European Commission – Joint Research Centre (JRC), Belgium)
- Dr. Jukka Lempiainen (Tampere University of Technology, Finland)
- Dr. Kandasamy Selvaradjou (Pondicherry Engineering College, India)
- Dr. Karisma Trinanda Putra (Universitas Muhammadiyah Yogyakarta, Indonesia)
- Dr. Keping Yu (Waseda University, Japan)
- Dr. Kevin (Qixiang) Pang (Lakehead University, Canada)
- Dr. Khoirul Anwar (Telkom University, Indonesia)
- Dr. Kiho Lim (William Paterson University of New Jersey, USA)
- Dr. Kostas Peppas (University of Peloponnese, Greece)
- Dr. Kuntal Deka (IIT Goa, India)
- Dr. Lei Cao (The University of Mississippi, USA)
- Dr. Lei Mo (INRIA, France)
- Dr. Lexi Xu (China Unicom Network Technology Research Institute, China)
- Dr. Lifeng Lai (University of California, Davis, USA)
- Dr. Linawati Linawati (Universitas Udayana, Indonesia)
- Dr. Luca Cavaglione (National Research Council (CNR), Italy)
- Dr. Luca Reggiani (Politecnico di Milano, Italy)
- Dr. M Sabarimalai Manikandan (Indian Institute of Technology Bhubaneswar, India)
- Dr. M Arif Khan (Charles Sturt University, Australia)
- Dr. Maggie Mashaly (German University in Cairo, Egypt)
- Dr. Majed Haddad (University of Avignon, France)
- Dr. Marcin Piotr Pawlowski (Expeditus, Poland)
- Dr. Marco Baldi (Università Politecnica delle Marche, Italy)
- Dr. Mardeni Roslee (MMU, Malaysia)
- Dr. Marie-Jose Montpetit (Concordia University, Canada)
- Dr. Mariusz Zal (Poznan University of Technology, Poland)
- Dr. Mauro Fonseca (UTFPR, Brazil)
- Dr. Máximo Morales-Céspedes (Universidad Carlos III de Madrid, Spain)
- Dr. Michele Albano (Aalborg University, Denmark)
- Dr. Mingzhe Chen (Princeton University, USA)

- Dr. Minoru Okada (Nara Institute of Science and Technology, Japan)
- Dr. Mohamed Moustafa (Egyptian Russian University, Egypt)
- Dr. Montree Kumngern (King Mongkut's Institute of Technology Ladkrabang, Thailand)
- Dr. Muhammad Reza Kahar Aziz (Institut Teknologi Sumatera, Indonesia)
- Dr. Mukesh Singhal (University of California at Merced, USA)
- Dr. Mustafa Akbaş (Embry-Riddle Aeronautical University, USA)
- Dr. N Nasimuddin (Institute for Infocomm Research, Singapore)
- Dr. Nanda Kishore Chavali (Mathworks India Pvt Ltd., India)
- Dr. Natarajan Meghanathan (Jackson State University, USA)
- Dr. Nicola Calabretta (COBRA Research Institute, The Netherlands)
- Dr. Nur Abdul Razak (Universiti Teknologi MARA, Malaysia)
- Dr. Oluwakayode Onireti (University of Glasgow, United Kingdom (Great Britain))
- Dr. Omar Al saif (Northern Technical University, Iraq)
- Dr. Paolo Crippa (Università Politecnica delle Marche, Italy)
- Dr. Pasquale Dottorato (Lab ID, Italy)
- Dr. Paul Mitchell (University of York, United Kingdom (Great Britain))
- Dr. Paula Fraga-Lamas (University of A Coruña, Spain)
- Dr. Pavel Loskot (ZJU-UIUC Institute, China)
- Dr. Peiyong Zhang (China University of Petroleum (East China), China)
- Dr. Peng-Yong Kong (Khalifa University, United Arab Emirates)
- Dr. Petros Bithas (National and Kapodistrian University of Athens, Greece)
- Dr. Philippe Owezarski (LAAS-CNRS, France)
- Dr. Pietro Cassarà (National Research Council (CNR) at Pisa, Italy)
- Dr. Ping Zhou (Apple, USA)
- Dr. Prima Kristalina (Politeknik Elektronika Negeri Surabaya (PENS), Indonesia)
- Dr. Punnarumol Temdee (Mae Fah Luang University, Thailand)
- Dr. Pushpendu Kar (University of Nottingham Ningbo China, China)
- Dr. Qasim Ahmed (University of Huddersfield, United Kingdom (Great Britain))
- Dr. Qin Hu (IUPUI, USA)
- Dr. R Prasad (Delft University of Technology, The Netherlands)
- Dr. Rafael Asorey-Cacheda (Technical University of Cartagena, Spain)
- Dr. Rakesh T (Monash University, Australia)
- Dr. Rallis Papademetriou (University of Portsmouth, United Kingdom (Great Britain))
- Dr. Ram Bilas Pachori (Indian Institute of Technology Indore, India)
- Dr. Ramiz Sabbagh (University of Kent, United Kingdom (Great Britain))

- Dr. Ramzi Adriman (Universitas Syiah Kuala, Indonesia)
- Dr. Rashmi Chaudhry (International Institute of Information Technology, Italy)
- Dr. Ratul Baruah (Tezpur University, India)
- Dr. Ravi Hegde (IIT Gandhinagar, India)
- Dr. Ravikant Saini (Indian Institute of Technology Jammu, India)
- Dr. Riadh Dhaou (IRIT/ENSEEIH, University of Toulouse, France)
- Dr. Riccardo Colella (University of Salento, Italy)
- Dr. Roberto Di Pietro (Hamad Bin Khalifa University, Qatar)
- Dr. Rodrigo Campos Bortoletto (Instituto Federal de São Paulo, Brazil)
- Dr. Rosdiadee Nordin (Universiti Kebangsaan Malaysia, Malaysia)
- Dr. Samir Medjiah (LAAS-CNRS, France)
- Dr. Sanjay Dhar Roy (National Institute of Technology Durgapur, India)
- Dr. Sanjay Singh (Manipal Institute of Technology, India)
- Dr. Sanjeev Gurugopinath (PES University, India)
- Dr. Sanya Anees (Indian Institute of Information Technology – Guwahati, India)
- Dr. Scabin Kumar (Amity University Lucknow Campus (UP) India, India)
- Dr. Seemanti Saha (National Institute of Technology Patna, India)
- Dr. Sherali Zeadally (University of Kentucky, USA)
- Dr. Shuai Zhao (Tencent America LLC, USA)
- Dr. Sirikan Chucherd (Mae Fah Luang University, Thailand)
- Dr. Sonali Chouhan (Indian Institute of Technology Guwahati, India)
- Dr. Song Xing (California State University, Los Angeles, USA)
- Dr. Stylianos Basagiannis (United Technologies Research Centre, Ireland)
- Dr. Sudhir Kumar (Indian Institute of Technology Patna, India)
- Dr. Sumiko Miyata (Shibaura Institute of Technology, Japan)
- Dr. Sunantha Sodsee (King Mongkut's University of Technology North Bangkok, Thailand)
- Dr. Surapong Uttama (Mae Fah Luang University, Thailand)
- Dr. Taeshik Shon (Ajou University, Korea (South))
- Dr. Tariq Umer (COMSATS University Islamabad Lahore Campus, Pakistan)
- Dr. Theofilos Chrysikos (University of Patras, Greece)
- Dr. Thomas Lagkas (International Hellenic University, Kavala Campus, Greece)
- Dr. Thumrongrat Amornraksa (King Mongkut's University of Technology Thonburi, Thailand)
- Dr. Tianhua Xu (Tianjin University, China)
- Dr. Tomoki Yoshihisa (Osaka University, Japan)
- Dr. Trong-Minh Hoang (Posts and Telecommunications Institute of Technology, Vietnam)

- Dr. Vandana Rohokale (SPPU Pune, Maharashtra, India)
- Dr. Vanlin Sathya (University of Chicago, USA)
- Dr. Vasilis Friderikos (King's College London, United Kingdom (Great Britain))
- Dr. Vladimir Dyo (University of Bedfordshire, United Kingdom (Great Britain))
- Dr. Wael Jaafar (Carleton University, Canada)
- Dr. Watcharapan Suwansantisuk (King Mongkut's University of Technology Thonburi, Thailand)
- Dr. Wei Feng (Tsinghua University, China)
- Dr. Weili (lily) Wu (University of Texas at Dallas, USA)
- Dr. Weiwen Zhang (Guangdong University of Technology, China)
- Dr. Wenjun Xu (Beijing University of Posts and Telecommunications, China)
- Dr. Worasak Rueangsirarak (School of Information Technology, Mae Fah Luang University, Thailand)
- Dr. Xianbin Yu (Zhejiang University, China)
- Dr. Xiang Gui (Massey University, New Zealand)
- Dr. Xianliang Jiang (Ningbo University, China)
- Dr. Xiao Zhang (South-Central University for Nationalities, China)
- Dr. Xiaohua (Edward) Li (State University of New York at Binghamton, USA)
- Dr. Xiaoyu Tang (Zhejiang University, China)
- Dr. Yafei Hou (Okayama University, Japan)
- Dr. Yang Wang (La Salle University, USA)
- Dr. Yangyang Li (China Academy of Electronics and Information Technology, China)
- Dr. Yasin Kabalci (Nigde Omer Halisdemir University, Turkey)
- Dr. Yatish Joshi (Cisco Systems, USA)
- Dr. Yee-Jin Cheon (Korea Aerospace Research Institute, Korea (South))
- Dr. Ying Mao (Fordham University, USA)
- Dr. Yong Guan (Iowa State University, USA)
- Dr. Yongxu Zhu (South Bank University, United Kingdom (Great Britain))
- Dr. Yu Zhang (Zhejiang University of Technology, China)
- Dr. Yuansong Qiao (Athlone Institute of Technology, Ireland)
- Dr. Yun-Wei Lin (National Chiao Tung University, Taiwan)
- Dr. Yusuf Nur Wijayanto (Indonesian Institute of Sciences (LIPI), Indonesia)
- Dr. Yvon Gourhant (Orange Labs, France)
- Dr. Zeeshan Kaleem (COMSATS University Islamabad, Wah Campus, Pakistan)
- Dr. Zengpeng Li (Lancaster University, United Kingdom (Great Britain))
- Dr. Zheng Chu (University of Surrey, United Kingdom (Great Britain))
- Dr. Zhi Lin (Army Engineering University of PLA, China)

Dr. Zhiyuan Zheng (Pinterest, USA)

Dr. Zongyang Zhang (Beihang University, China)

Table of Contents

Title Page
 Welcome Message from General Chair
 Committee
 Program Schedule
 Table of Contents

Keynote Speech

Keynote 1

Network slicing: from definition to evolution towards 6G

Carla Raffaelli, M.Sc., Ph.D

Keynote 2

Robotic Aerial Small Cells for Efficient 6G Network Densification

Dr. Vasilis Frederikos

Keynote 3

Artificial Intelligence for Autonomous Vehicle

Dr. Nolang Fanani, B.Eng., M.Sc

Keynote 4

New Generation Microwave Synthesizer Key Design Technologies and Advanced Testing Trend

Shashiv Phadnis

1570812289	Design and Analysis of Optical Fiber Network Jakarta - Singapore - Nusantara via Karimata Strait	1
	Muhammad Rendra Perdana Kusuma Djaka, Fajar Aulia Rachman, Herry Tony Andhyka and Catur Apriono (Universitas Indonesia, Indonesia)	
1570846760	Terahertz Antenna-coupled Microbolometer: Impact of High Heater Resistance	9
	Arie Pangesti Aji (Universitas Indonesia, Indonesia); Hiroaki Satoh (Shizuoka University, Japan); Catur Apriono and Eko Tjipto Rahardjo (Universitas Indonesia, Indonesia); Hiroshi Inokawa (Shizuoka University, Japan)	
1570849139	Modeling of Multiplexing Indoor Light Fidelity (Li-Fi) Technology Using Movable LED Panel	14
	I Wayan Mustika (Universitas Gadjah Mada, Indonesia); Fauza Khair and Anggun Fitriani Isnawati (Institut Teknologi Telkom Purwokerto, Indonesia); Arrizky Ayu Faradila Purnama (Institute of Technology Telkom Surabaya & Faculty of Electrical Technology and Intelligent Industry, Indonesia); Dwi Edi Setyawan (Institut Teknologi Telkom Surabaya, Indonesia)	

1570825645	Energy Efficient Cooperative Strategy over LEO Satellite Internet of Things	21
	Kaiwei Wang (No 38 Research Institute, China Electronics Technology Group Corporation, China)	
1570826871	Link Budget Analysis for a 3U Nanosatellite Operating At S-band	27
	Habib Idmouida (Mohammed V University in Rabat, Morocco & University Center for Research in Space Technologies, Mohammedia School of Ingeniers, Morocco)	
1570806826	Reversible Data Hiding using Pixel-Value-Ordering and Difference Expansion in Digital Images	33
	Ntivuguruzwa Jean De La Croix and Chaidir Islamy (Institut Teknologi Sepuluh Nopember, Indonesia); Tohari Ahmad (Institut Teknologi Sepuluh Nopember (ITS), Indonesia)	
1570816873	A Review Paper: Accuracy of Machine Learning for Depression Detection in Social Media	39
	Alya Melati Putri, Kevin Wijaya and Owen Salomo (Binus University, Indonesia); Anderies Anderies (BINUS University, Indonesia); Alexander Agung Santoso Gunawan (Bina Nusantara University & University of Indonesia, Indonesia)	
1570817330	Click Bait Detection for Internet News Title with Deep Learning Feed Forward	46
	Berlian Al Kindhi (Institut Teknologi Sepuluh Nopember, Indonesia); Sean John Rawlings (Cardiff Metropolitan University, United Kingdom (Great Britain))	
1570849653	A Decision Tree Knowledge-based System for Reviewing of Research Ethics Protocol	50
	Ratih Nur Esti Anggraini (Intelligent Systems Lab, University of Bristol, United Kingdom (Great Britain) & Institut Teknologi Sepuluh Nopember, Indonesia); Nurul Fajrin Ariyani, Abdullah Faqih Septiyanto, Zahra Meilani and Riyanarto Sarno (Institut Teknologi Sepuluh Nopember, Indonesia)	
1570825403	Systematic Literature Review: Collaborative Filtering Algorithms for Recommendation Systems	56
	Michael The Hadinata, Hans Andika, William Huang and Anderies Anderies (BINUS University, Indonesia); Irene Anindaputri Iswanto (Bina Nusantara University, Indonesia)	
1570825606	Intrusion Detection using Support Vector Machine on Internet of Things Dataset	62
	Rifky Aditya, Hilal H. Nuha and Sidik Prabowo (Telkom University, Indonesia)	
1570825636	Flood Identification with Fuzzy Logic Based on Rainfall and Weather for Smart City Implementation	67

Berlian Al Kindhi (Institut Teknologi Sepuluh Nopember, Indonesia)

1570827576	Performance Comparison of Machine Learning Algorithms for Student Personality Classification	73
	Didi Supriyadi (Diponegoro University, Indonesia & Institut Teknologi Telkom Purwokerto, Indonesia); Purwanto Purwanto (Universitas Diponegoro, Indonesia); Budi Warsito (Diponegoro University, Indonesia)	
1570829856	Improvement Object Detection Algorithm Based on YoloV5 with BottleneckCSP	79
	Aria Hendrawan (Information System School of Postgraduate Universitas Diponegoro, Indonesia & Universitas Semarang, Indonesia); Rahmat Gernowo, Oky Nurhayati, Budi Warsito and Adi Wibowo (Information System School of Postgraduate Diponegoro University, Indonesia)	
1570836276	Intrusion Detection using Deep Neural Network Algorithm on the Internet of Things	84
	Syariful Ikhwan (Institut Teknologi Telkom Purwokerto, Indonesia); Adi Wibowo and Budi Warsito (Diponegoro University, Indonesia)	
1570836614	Integration of Decision Tree-Fuzzy Algorithm for Decision Support System in Air Force Operation	88
	Hendri Himawan Triharminto (Indonesian Air Force Academy, Indonesia); Lenny Iryani (Politeknik Negeri Bandung, Indonesia)	
1570808247	Design and Implementation of On-Body Textile Antenna for Bird Tracking at 2.4 GHz	94
	Hasri Ainun Harris, Levy Olivia Nur and Radial Anwar (Telkom University, Indonesia)	
1570816865	Outage Analysis of UAV-assisted Co-operative communication system with imperfect SIC	100
	Anju Rs (National Institute of Technology, Trichy, India); Anandpushparaj J (National Institute of Technology, Trichirappalli, India); Muthu Palanivel Chidambara Nathan (National Institute of Technology, India)	
1570825046	HPA Rapp Model Nonlinear Distortion Effect Mitigation Technique on GFDM System	107
	Ari Endang Jayati (Institut Teknologi Sepuluh Nopember & Universitas Semarang, Indonesia)	
1570825607	System Usability Scale Analysis of Infusion Fluid Level Monitoring And Notification System Using IoT	112
	Handika Jaladara, Rizka Reza Pahlevi and Hilal H. Nuha (Telkom University, Indonesia)	
1570805131	The Performance Analysis of Hybrid SDN-IP Reactive Routing on ONOS Controller in Tree Topologies	118

Bongga Arifwidodo (Telkom Institute of Technology Purwokerto, Indonesia);
Donny Arief Oktavian and Jafaruddin Gusti Amri Ginting (IT Telkom
Purwokerto, Indonesia)

- | | | |
|-------------------|---|------------|
| 1570812204 | Auto Discover Virtual Private Network Using Border Gateway Protocol Route Reflector | 123 |
| | Setiyo Budiyo, Ch Aprihansah, Lukman Silalahi and Imelda Simanjuntak (Universitas Mercu Buana, Indonesia); Freddy Artadima Silaban (Universitas Mercu Buana & Indones, Indonesia); Agus Rochendi (Badan Riset dan Inovasi Nasional, Indonesia) | |
| 1570812251 | QoS Analysis on VoIP with VPN Using SSL and L2TP IPsec Method | 130 |
| | Erryc Darmawan, Setiyo Budiyo and Lukman Silalahi (Universitas Mercu Buana, Indonesia) | |
| 1570812259 | Secret Image Sharing and Steganography based on Fuzzy Logic and Prediction Error | 137 |
| | Chaidir Islamy (Institut Teknologi Sepuluh Nopember, Indonesia); Tohari Ahmad (Institut Teknologi Sepuluh Nopember (ITS), Indonesia); Royyana Ijtihadie (Institut Teknologi Sepuluh Nopember, Indonesia) | |
| 1570817172 | Adapting ISO 17025 to Enrich QoS as Quality Measurement on Internet of Medical Things | 143 |
| | Muhammad Yusro, Nor Safira Azlyn and Sevia Purnama (Institut Teknologi Telkom Purwokerto, Indonesia) | |
| 1570849890 | Marine Vessels Detection on Very High-Resolution Remote Sensing Optical Satellites | 149 |
| | Bill Van Ricardo Zalukhu and Arie Wahyu Wijayanto (Politeknik Statistika STIS, Indonesia); Muhammad Iqbal Habibie (National and Research Innovation Agency (BRIN), Indonesia) | |
| 1570839448 | An Implementation of Large Scale Hate Speech Detection System for Streaming Social Media Data | 155 |
| | Doan Long An (University of Information Technology, Vietnam); Thao Phuong Nguyen (University Information Technology, Vietnam); Trong-Hop Do (University of Information Technology, Ho Chi Minh City & Vietnam National University, Ho Chi Minh City, Vietnam) | |
| 1570839816 | A Practical Real-Time Flight Delay Prediction System using Big Data Technology | 160 |
| | Tri Minh Vo and Vu Tran Trieu (University of Information Technology, Vietnam); The Duc Pham (University Information of Technology, Vietnam); Trong-Hop Do (University of Information Technology, Ho Chi Minh City & Vietnam National University, Ho Chi Minh City, Vietnam) | |
| 1570841530 | Design and Testing on Migration of Remiss-Supply in Banking System to Microservice Architecture | 168 |

Alwi Maulana (Institut Teknologi Telkom Purwokerto, Indonesia); Pradana Ananda Raharja (Institut Teknologi Telkom Purwokerto, Indonesia & Fakultas Informatika, Indonesia)

- | | | |
|-------------------|---|------------|
| 1570843900 | School Zoning System for Student Admission using Constrained K-Means Algorithms | 174 |
| | Andi Alviadi Nur Risal (Hasanuddin University, Indonesia); Zahir Zainuddin (University of Hasanuddin, Indonesia); Muhammad Niswar (Universitas Hasanuddin, Indonesia) | |
| 1570844448 | Classifying Leaf Types using the Artificial Neural Network Method by Optimizing Parameter Iteration | 179 |
| | M Alfian Dzikri, S Ayu Septianingrum, Nova Rijati and Pujiono Pujiono (Universitas Dian Nuswantoro, Indonesia) | |
| 1570844565 | Ensemble of the Distance Correlation-Based and Entropy-Based Sensor Selection for Damage Detection | 183 |
| | Jimmy Tjen, Genrawan Hoendarto and Tony Darmanto (Universitas Widya Dharma Pontianak, Indonesia) | |
| 1570844733 | Mandibular segmentation on panoramic radiographs with CNN Transfer Learning | 190 |
| | Nur Nafi'iyah, Chastine Fatichah and Darlis Herumurti (Institut Teknologi Sepuluh Nopember, Indonesia); Eha Renwi Astuti (Universitas Airlangga, Indonesia); Esa Prakasa (BRIN, Indonesia) | |
| 1570845477 | Clustering Stress Reactivity based on Heart Rate Variability during Acute Mental Stress Task | 195 |
| | Auditya Purwandini Sutarto, Nailul Izzah and Mohamad H Hariyadi (Universitas Qomaruddin, Indonesia) | |
| 1570846522 | GRU-MF: A Novel Appliance Classification Method for Non-Intrusive Load Monitoring Data | 200 |
| | Aji Gautama Putrada, Nur Alamsyah, Syafrial Fachri Pane and Mohamad Nurkamal Fauzan (Telkom University, Indonesia) | |
| 1570849999 | DCGAN-based Medical Image Augmentation to Improve ELM Classification Performance | 206 |
| | Rando Rando, Noor Akhmad Setiawan and Adhistya Erna Permanasari (Universitas Gadjah Mada, Indonesia); Riries Rulaningtyas (Airlangga University, Indonesia); Andriyan B. Suksmono (Bandung Institute of Technology, Indonesia); Imas Sukaesih Sitanggang (Bogor Agricultural University, Indonesia) | |
| 1570847133 | n-Mating Effect on Genetic Algorithm-Based Clustering Performance for Hotspots Data | 212 |
| | Rani Rotul Muhima (Institut Teknologi Adhi Tama Surabaya, Indonesia) | |

1570850157	A study of Convolution Neural Network Based Cataract Detection with Image Segmentation Nina Sevani, Hendrik Tampubolon, Jeremy Wijaya, Lukas Cuvianto and Albert Salomo (Krida Wacana Christian University, Indonesia)	216
1570848940	A Novel License Plate Image Reconstruction System using Generative Adversarial Network Vy-Hao Phan and Minh-Quan Ha (University of Information Technology, Vietnam); Trong-Hop Do (University of Information Technology, Ho Chi Minh City & Vietnam National University, Ho Chi Minh City, Vietnam)	222
1570848944	A Small-Scale Temperature Forecasting System using Time Series Models Applied in Ho Chi Minh City Nam Quoc Nguyen, Thang Chau Phan, Khanh Phuoc Bao Truong, Hong Thi Thuy Dang and Trong-Hop Do (University of Information Technology, Ho Chi Minh City & Vietnam National University, Ho Chi Minh City, Vietnam)	229
1570825685	Linear Filter Design for FBMC-OQAM Transceiver Davide Mattera (Università degli Studi di Napoli Federico II, Italy); Mario Tanda (Università di Napoli Federico II, Italy)	235
1570825687	Triangular Patch Antenna Using Coplanar Waveguide and DGS Techniques for 5G Communications Nurhayati Nurhayati, Mohammad Iyo Agus Setyono and Alga Mardhiarta Yundha Tama (Universitas Negeri Surabaya, Indonesia)	241
1570825701	Coplanar Vivaldi Antenna with wave slot structure for RADAR application Nurhayati Nurhayati (Universitas Negeri Surabaya, Indonesia); Eko Setijadi (Institut Teknologi Sepuluh Nopember, Indonesia)	247
1570826885	Performance Evaluation of LoRa 915 MHz for Health Monitoring with Adaptive Data Rate Puput Dani Prasetyo Adi (National Research and Innovation Agency (BRIN-RI), Indonesia)	252
1570832619	Network Planning and Performance Analysis for 5G mmWave in Urban Areas Nasaruddin Nasaruddin (Syiah Kuala University, Indonesia); Nuzuar Rafli and Yunida Yunida (Universitas Syiah Kuala, Indonesia); Rusdha Muharrar (Syiah Kuala University, Indonesia)	258
1570833435	Performance analysis of FBMC-PAM systems in frequency-selective Rayleigh fading channels in the pres Davide Mattera (Università degli Studi di Napoli Federico II, Italy); Mario Tanda (Università di Napoli Federico II, Italy)	264
1570836452	A 4x4 Microstrip Feeder Antenna Design using Dolph-Chebyshev for Receiving Himawari-8 Satellite Data	270

	Muhammad Riza Darmawan and Catur Apriono (Universitas Indonesia, Indonesia)	
1570836864	LEO Satellite Authentication using Physical Layer Features with Support Vector Machine	277
	Mohammed Hammouda and T. Aaron Gulliver (University of Victoria, Canada)	
1570841692	Designing QPSK Modulator Using LTspice-Based Discrete Components	283
	Andicho Haryus Wirasapta (Gadjah Mada University, Indonesia); Prpto Nugroho (Universitas Gadjah Mada, Indonesia); Sigit Basuki Wibowo (Gadjah Mada University, Indonesia)	
1570843986	Threshold-Based Physical Layer Authentication for Space Information Networks	289
	Mohammed Hammouda and T. Aaron Gulliver (University of Victoria, Canada)	
1570844609	FER Polar Codes Performances Using 5G Broadband Channel with CP-OFDM Techniques at 2.3 GHz Frequency	294
	Reni Dyah Wahyuningrum (Institut Teknologi Telkom Purwokerto, Indonesia); Khoirun Ni'amah (Institut Teknologi Telkom Purwokerto & Telkom University, Indonesia); Solichah Larasati and Shinta Romadhona (Institut Teknologi Telkom Purwokerto, Indonesia)	
1570846100	Recent Trends in the Reconfigurable Intelligent Surfaces (RIS): Active RIS to Brain-controlled RIS	299
	Muhammad Miftahul Amri (Sungkyunkwan University, Korea (South))	
1570846106	Indoor Positioning System for Campus Building Based on WLAN Fingerprint	305
	Mohammad Edar Paradise Wibowo, Mohammad Raudya Hananditya and Firdaus Firdaus (Universitas Islam Indonesia, Indonesia); Noor Azurati Ahmad and Azlan Adi (Universiti Teknologi Malaysia, Malaysia)	
1570846640	Techno-Regulation Analysis of Micro Operator in Industrial Area	310
	Melati Sabila Putri, Bambang Setia Nugroho and Helni Jumhur (Telkom University, Indonesia)	
1570851068	Private 5G Network Capacity and Coverage Deployment for Vertical Industries: Case Study in Indonesia	317
	Asri Wulandari Asri (Politeknik Negeri Jakarta, Indonesia); Alfin Hikmaturokhman (Institut Teknologi Telkom Purwokerto & Universitas Indonesia, Indonesia); Marfani Marfani (PT Telkomsel, Indonesia)	
1570822994	Performance Comparison of Web Server Application on Single Board Computer	323
	Mega Pranata (Institut Teknologi Telkom Purwokerto); Aditya Wijayanto and Muhammad Fajar Sidiq (Institut Teknologi Telkom Purwokerto, Indonesia)	

1570825051	Tracking Device for The Mountaineers Using GPS Ari Endang Jayati (Institut Teknologi Sepuluh Nopember & Universitas Semarang, Indonesia)	328
1570825635	Sybil Attack Detection on ITS-V2X System using a Realistic Traffic Model-based Approach Afdhal Afdhal, Ahmadiar Ahmadiar and Ramzi Adriman (Universitas Syiah Kuala, Indonesia)	333
1570825665	Deep Feature Selection for Machine Learning based Attack Detection Systems Minh-Tri Huynh, Hoang-Trung Le, Xuan-Ha Nguyen and Le Kim-Hung (University of Information Technology, Vietnam)	339
1570846225	LoRA Gateway Coverage and Capacity Analysis in Urban Area For IoT Smart Gas Meter Demand Kalam Adhiansyah Lutfie (University of Indonesia, Indonesia); Prima Dewi Purnamasari and Dadang Gunawan (Universitas Indonesia, Indonesia); I Ketut Agung Enriko (Institut Teknologi Telkom Purwokerto & PT Telkom Indonesia, Indonesia)	345
1570829674	Feasibility Evaluation of Compact Flow Features for Real-time DDoS Attacks Classifications Muhammad Fajar Sidiq and Nanda Iryani (Institut Teknologi Telkom Purwokerto, Indonesia); Akbari Indra Basuki (National Research and Innovation Agency (BRIN), Indonesia); Arief Indriarto Haris and Rd Angga Ferianda (BRIN, Indonesia)	350
1570836485	An IoT-Based System for Water Quality Monitoring and Notification System of Aquaculture Prawn Pond Ramzi Adriman, Maya Fitria and Afdhal Afdhal (Universitas Syiah Kuala, Indonesia)	356
1570846836	Design of Spectrum analyzer Android-based Instructional Media for Vocational High School Student Assa K Rohana and Adythia E Nugraha (SMK TELKOM JAKARTA, Indonesia); Rohani Cristyn (Penabur Christian Senior High School Kota Wisata, Indonesia); Kukuh Harsanto and Garrison Lee (SMK TELKOM JAKARTA, Indonesia)	361
1570853669	Portable Air Quality Monitoring System in ANN Using Combination Hidden Layer Hyperparameters Haniah Mahmudah, Cindy Ulan Purwanti, Rahardhita Sudibyo, Ilham Dwi Pratama and Nur Menik Rohmawati (Politeknik Elektronika Negeri Surabaya, Indonesia)	368

- 1570853744 Performance of Deep Learning Benchmark Models on Thermal Imagery of Pain through Facial Expressions 374**
- Raihan Islamadina (Universitas Islam Negeri Ar Raniry, Indonesia); Khairun Saddami (Universitas Syiah Kuala, Indonesia); Maulisa Oktiana (Syiah Kuala University, Indonesia); Taufik F. Abidin (Universitas Syiah Kuala, Indonesia); Rusdha Muharar (Syiah Kuala University, Indonesia); Fitri Arnia (Universitas Syiah Kuala, Indonesia)
- 1570854233 Sliding Mode Control of Angular Speed DC Motor System with Parameter Uncertainty 380**
- Alfian Ma'arif (Universitas Ahmad Dahlan, Indonesia); Iswanto Iswanto, Is (Universitas Muhammadiyah Yogyakarta, Indonesia); Aninditya Anggari Nuryono, Aan (Mulia University, Indonesia); Nia Maharani Raharja (Universitas Gadjah Mada, Indonesia); Hari Maghfiroh (Universitas Gadjah Mada & IEEE SB UGM, Indonesia)
- 1570855991 Oil Palm Leaf Disease Detection on Natural Background Using Convolutional Neural Networks 388**
- Anindita Septiarini and Hamdani Hamdani (Universitas Mulawarman, Indonesia); Eko Junirianto (Politeknik Pertanian Negeri Samarinda, Indonesia); Mohammad Sofyan S Thayf (STMIK KHARISMA Makassar, Indonesia); Gandung Triyono (Universitas Gadjah Mada, Indonesia); Henderi Henderi (University of Raharja, Indonesia)
- 1570846652 Decision Making via Game Theory for Autonomous Vehicles in the Presence of a Moving Obstacle 393**
- Marina Vicini, Sercan Albut and Elvina Gindullina (University of Padova, Italy); Leonardo Badia (Università degli Studi di Padova, Italy)
- 1570849331 Hiding Document Format Files Using Video Steganography Techniques With Least Significant Bit Method 399**
- Tufail Akhmad Satrio, Wahyu Adi Prabowo and Trihastuti Yuniati (Institut Teknologi Telkom Purwokerto, Indonesia)
- 1570850000 Error Rate Performance of Equatorial HF Skywave MIMO Packet Radio 407**
- Elsa Lolita Anggraini, Gamantyo Hendrantoro and Titiek Suryani (Institut Teknologi Sepuluh Nopember, Indonesia)
- 1570850070 Analysis of Microwave Absorber Using Sugarcane Bagasse for 27 - 29 GHz Frequency 411**
- Yougha Budi Prahmana, Ayu Mika Sherila and Umairah Umairah (Universitas Mercu Buana, Indonesia); Erfan Handoko (Universitas Negeri Jakarta, Indonesia); Mudrik Alaydrus (Universitas Mercu Buana, Indonesia)

1570848572	Trajectory and Power Optimization for Buffer-Assisted Amplify-and-Forward UAV Relay Naga manoj Makkena (International Institute of Information of Technology, Hyderabad, India); P Ubaidulla (International Institute of Information Technology, India)	415
1570851329	Robustness Analysis of 5-Element Overlapped Linear Subarrays for Wide Angular Scanning Applications Titus Cahya Pertiwi (Institut Teknologi Sepuluh Nopember, Indonesia); Fannush Shofi Akbar (Institut Teknologi Telkom Surabaya, Indonesia); Gamantyo Hendranto (Institut Teknologi Sepuluh Nopember, Indonesia); Leo P. Ligthart (em. prof. Delft University of Technology & Universitas Indonesia, Beijing Institute of Technology, ITS Surabaya, The Netherlands)	422
1570843062	Implementation of the Internet of Things for Flood Mitigation and Environmental Sustainability Muhamad Azrino Gustalika (Institut Teknologi Telkom Purwokerto, Indonesia); Sudianto Sudianto (Telkom Institute of Technology Purwokerto, Indonesia); Diandra Chika Fransisca, Fahrudin Mukti Wibowo, Mas Aly Afandi and Reni Dyah Wahyuningrum (Institut Teknologi Telkom Purwokerto, Indonesia)	426
1570843781	DRL-Based Secure Beamforming for Hybrid-RIS Aided Satellite Downlink Communications Quynh Tu Ngo, Khoa Tran Phan, Abdun Mahmood and Wei Xiang (La Trobe University, Australia)	432
1570854156	Investigated insider and outsider attacks on the federated learning system Ibraim Ahmed (University of Mosul, Iraq & College of Science, Iraq); Manar Kashmoola (Mosul University, Iraq)	438
1570849141	Analysis of Transmitter Half Angle and FOV Variations on Multiplexing Indoor Li-Fi Communication I Wayan Mustika (Universitas Gadjah Mada, Indonesia); Fauza Khair and Anggun Fitriani Isnawati (Institut Teknologi Telkom Purwokerto, Indonesia); Dwi Edi Setyawan (Institut Teknologi Telkom Surabaya, Indonesia); Arrizky Ayu Faradila Purnama (Institute of Technology Telkom Surabaya & Faculty of Electrical Technology and Intelligent Industry, Indonesia)	444
1570847645	Performance Analysis of Eigenface Method for detecting organic and non organic waste type Aditya Wijayanto (Institut Teknologi Telkom Purwokerto, Indonesia); Afifah Dwi Ramadhani (Politeknik Elektronika Negeri Surabaya, Indonesia); Muhamad Azrino Gustalika and Alon Jala Tirta Segara (Institut Teknologi Telkom Purwokerto, Indonesia)	451

1570850150	Soft FFR Scheme for Distributed D2D Communication in Multicell of Cellular Communication Networks	456
	Soraida Sabella, Misfa Susanto, Fx Arinto Setyawan and Fadil Hamdani (University of Lampung, Indonesia)	
1570851744	New Approach of Ensemble Method to Improve Performance of IDS using S-SDN Classifier	463
	Amarudin Amarudin (Universitas Gadjah Mada & Universitas Teknokrat Indonesia, Indonesia); Ridi Ferdiana (Universitas Gadjah Mada, Indonesia); Widy Widyawan (Gadjah Mada University, Indonesia)	
1570853516	Security Analysis and Improvement for Satellite and Mobile Network Integration	469
	Meiling Chen (CMRI, China)	
1570843844	Quality Control Through Game Theory of a Cascading Multi-robot Machine Vision System	475
	Samuele Benfatti, Ivano Donadi and Elvina Gindullina (University of Padova, Italy); Leonardo Badia (Università degli Studi di Padova, Italy)	

Hiding Document Format Files Using Video Steganography Techniques With Least Significant Bit Method

Tufail Akhmad Satrio
Department of Informatics Engineering
Institut Teknologi Telkom Purwokerto
Purwokerto, Indonesia
tufailas040@gmail.com

Wahyu Adi Prabowo*
Department of Informatics Engineering
Institut Teknologi Telkom Purwokerto
Purwokerto, Indonesia
wahyuadi@ittelkom-pwt.ac.id

Trihastuti Yuniati
Department of Informatics Engineering
Institut Teknologi Telkom Purwokerto
Purwokerto, Indonesia
trihastuti@ittelkom-pwt.ac.id

Abstract—Video Steganography is one type that can use to hide secret messages. Video Steganography is a technique to hide messages in video media by inserting messages into one of the video frames. Cryptography can be combined with the Steganography technique to secure hidden messages in video files. This research was conducted to analyze the LSB (Least Significant Bit) steganography test combined with the Fernet cryptographic process. This study investigates the file insertion process, the test extraction process, the speed of system implementation, the visual attack, the Peak Signal Noise Ratio (PSNR) value, and the audio comparison between original video and video with embedded files. The results of this test indicate that the embedding process in the video is directly proportional to the results received. The larger the original video size, the larger the embedded video size will be.

Keywords—video steganography, cryptography, Least Significant Bit, LSB, Fernet

I. INTRODUCTION

Advances in technology and the internet are currently making various kinds of breakthroughs in the field of data communication. Communication is one of the essential needs in human life to relate to each other [1], [2]. When communicating, there will be an exchange of information between the two parties [3] and often there is essential information that is confidential [4]. Security and confidentiality of data or information are critical in information systems and data communication [5].

The major problem in the digital world, important information or data, is that data is an asset vulnerable to being stolen by others [6]. Recently, there has been renewed interest in data security. One way that is generally used to secure the data is to use a combination of steganography and cryptography [7], [8]. Steganography is one way to hide a message or personal data into data or other messages that appear to contain nothing except for people who know the key [5]. The purpose of steganography is to hide messages and make them invisible to attackers [9] and can even allow someone not to detect a message or data in the file [10]. Cryptography is the art of maintaining the security or confidentiality of data. Cryptography will convert data into specific codes and is only intended for parties with only a key to convert the code back into data [11]. The key is not an object but a secret code known by the party who exchanges information or data and will later be used to encrypt or decrypt data [12]. *Encryption* is a process carried out to secure a

message (plaintext) into a hidden message (ciphertext), while decryption is the process of converting ciphertext into plaintext [13].

Studies on steganography and cryptography show the importance of data security. Several researchers have attempted to combine the concepts of steganography and cryptography. Steganography with LSB (Least Significant Bit) method and Hill Chipper cryptography can be combined in securing messages [14]–[16]. In some of these studies, image media is used, so the steganography technique can be called Image Steganography. From the results of this study, the process of hiding messages in digital images is safe and unknown to the naked eye because the size of the bitmap resulting from steganography does not change after the process of inserting binary text into a binary bitmap. Using the Least Significant Bit (LSB) method, which replaces the last bit so that the bitmap capacity before and after steganography does not experience significant changes, cryptographic testing can be done encode and decode. Another study combines LSB steganography and RSA cryptography (Rivest-Shamir-Adleman) through video media [17], [18]. The results of this study indicate that this high-level system's performance and methodology have succeeded in performing embedded files compared to other systems using the same methodology [19].

In this study, researchers built an application combining LSB steganography and fernet cryptography on video media. The advantage of this LSB steganography method is that the quality and size of the image after the message is inserted do not look much different [19]. The least significant bit is the part of the binary data sequence (base two) with the most negligible significant/smallest value. It is located on the far right of the bit sequence [20]. In the arrangement of bits in a byte (1 byte = 8 bits), there are the most significant bits (the most significant bit or MSB) and the least significant bit (the least significant bit or LSB) [21]. Fernet is an implementation of symmetric cryptography (also known as “secret key”) authentication [22]. Fernet is a cryptographic method that provides a simple authentication and encryption method using HMAC (Hash-based Message Authentication Code) with SHA256 for authentication and symmetric AES-128 in CBC (Cipher Block Chaining) mode using PKCS7 padding, which offers 128 bits (16 bytes) in length [23], [24].

For this reason, in this study, the researchers built an application that was built using the Python language to insert a file that has been encrypted using cryptography into a video

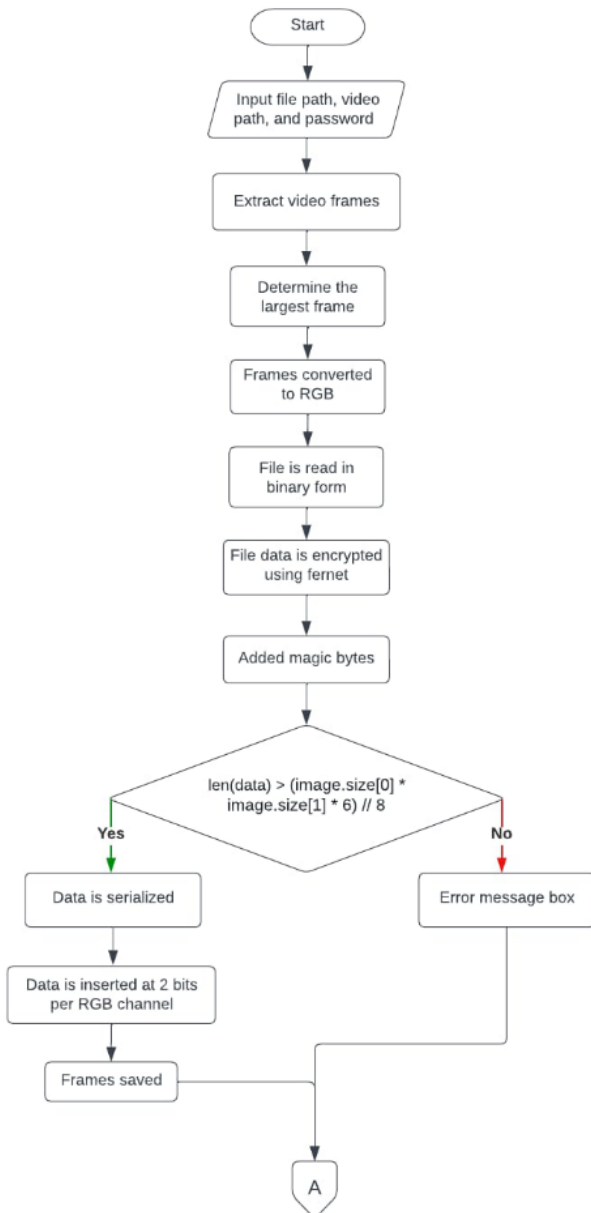


Fig. 1. Flowchart encryption process

that has been determined using steganography techniques, better known as Video Steganography. Video steganography is a technique of hiding or inserting data into a video [25]. In a video, some frames can be inserted into secret messages [26], so if someone wants to extract the message, they must check every frame in the video. The video used is a video in MP4 format. This format was chosen because it is often used by many people and is easy to find on the internet [27]. The files used in inserting messages into videos are files with .docx and .pdf formats. The choice of file with this format is because it can accommodate many messages/data compared to the .txt format, which can only be filled with text messages. Test Analysis of the results of steganography and encryption includes investigating the file insertion process, the test extraction process, the speed of system implementation, the visual attack, the Peak Signal Noise Ratio (PSNR) value, and the audio comparison between original video and video with embedded files. The results of this test indicate that the embedding process in the video is directly proportional to the results received. The larger the original video size, the larger the embedded video size will be.

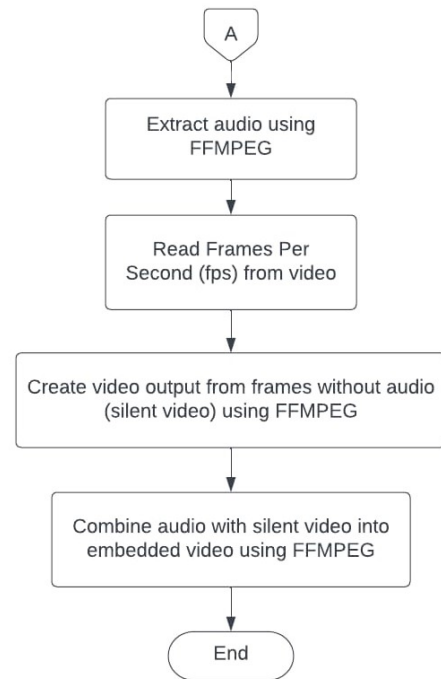


Fig. 2. Flowchart steganography process

II. SYSTEM IMPLEMENTATION

This stage involves applying the methods and techniques used to create application programs. The application implementation uses the python language, which is used to combine LSB steganography and fernet cryptography. The way the first video steganography application works is the insertion of files into the video. This first step aims to enter the file location, video location, and password. Then the inputted video will be extracted frame and audio using FFMPEG, and the frame will be used as a medium for message insertion. The frame selection is based on the largest frame size from a set of extracted frames. The next step is to insert the file into the frame using the LSB method. The file to be inserted is first opened using a binary format, then encrypted using the fernet algorithm to increase the level of data security. Then, the file will be given a unique mark (magic bytes) so that the file is detected in the frame that is the cover object when extracting the video file. After successfully inserting the file, the next step is to unify the frame and audio into a video output containing the secret file. The working process of the video steganography application can be seen in Fig. 1.

Next, the first step in extracting the file is to enter *the path of the Embedded Video* or video that is inserted the message and enter *the password*. Next, the video will be extracted its frames to retrieve hidden file data, this process can be seen in Fig. 2.

The next process is *extract Data File* in Fig. 3, in that process the frames that have been extracted will be selected with the largest size because it contains file data that has been hidden. The frames that have been obtained will be checked for LSB bits, if there are special marks (magic bytes) then the data will be taken from the LSB bits of the frame. Furthermore, the data will be decrypted first to get the original data. Once encrypted, the data will be converted into a *file* again using *binary writing mode*. After *the file* is successfully retrieved, the *extract Data File* completes.

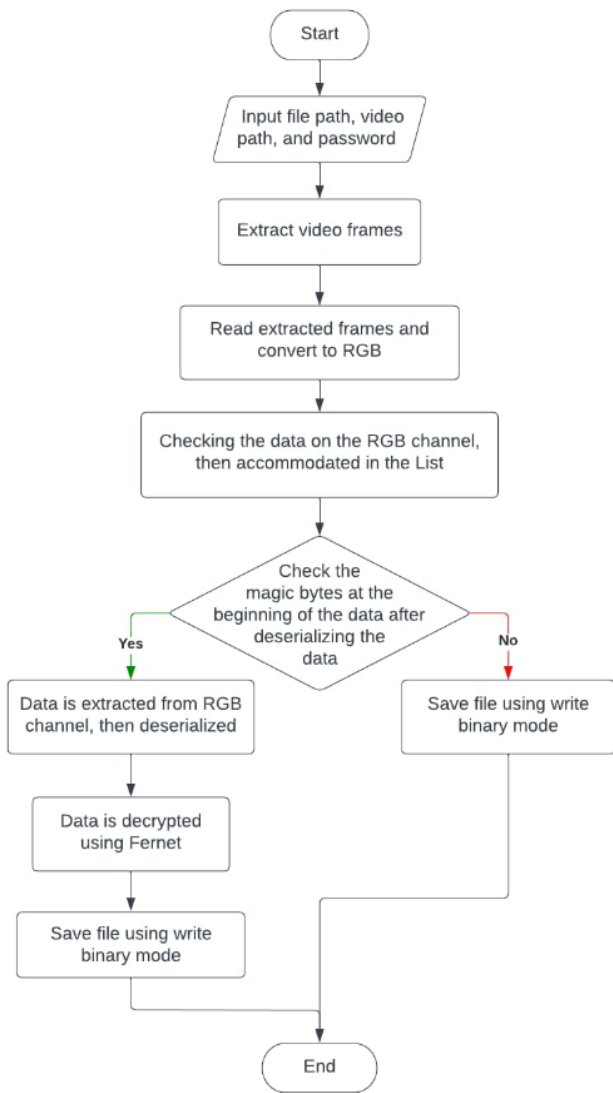


Fig. 3. Flowchart extraction process

The image below in Fig. 4 is the main window of the application. In the main window, there are two buttons, namely the "Hide File" and "Extract Files." The "Hide File" button inserts files into the video. The "Extract File" button is to retrieve files that have been inserted into the video.

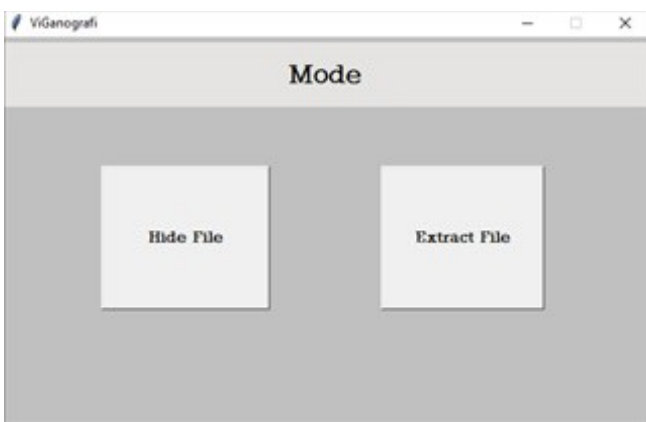


Fig. 4. Main window of the application

When the "Hide File" and "Extract File" button is pressed, then the user will be redirected to a new window as below in Fig. 5.

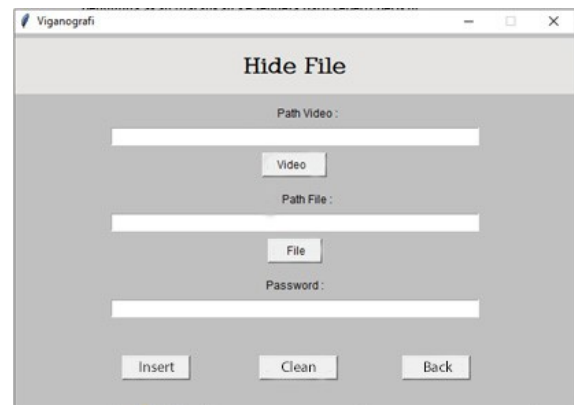


Fig. 5. "Hide File" menu window

In Fig. 5, contains three fields that must be filled in; the three columns are the video path, file path, and password fields. The three columns are inputs or variables used for file insertion into the video. In the "Extract File" menu in Fig. 6, there are two inputs or variables: the video path and password. Both variables must be filled so that the file extraction process runs smoothly.

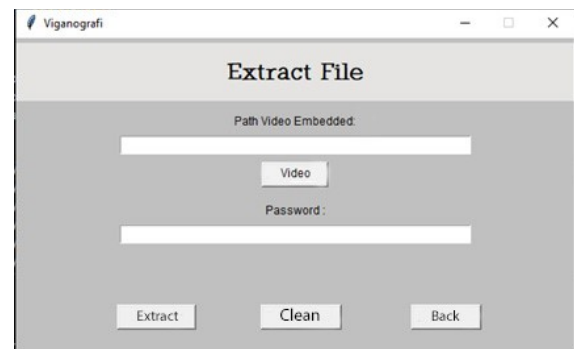


Fig. 6. "Extract File" menu window

III. RESULT AND DISCUSSION

Every process on this system was tested to find out that the system in the application was running well and analyzed the results of the output files received in each running process.

A. Process of Hiding Files Into Videos

In this hiding testing process, four videos and three files are used. The first three videos are similar with a duration of 29 seconds. The first three videos have differences in quality, namely 144p, 360p, and 720p. The video tests the success of the file-hiding process on a 2-bit data frame. Then the last video is used to test the visual attack on the given results. In the last video, the bits used in file hiding are 2 bits, 4 bits, and 6 bits. Then the three files used, both "docx" and "pdf" formats, have different sizes. The difference is applied to find out how big the maximum size of the data file that can be inserted into the video frame.

TABLE 1. FILE HIDING TEST RESULT

No	Original Video Name	Original Video Size	File Name	File Size	Password	Embedded Video Name	Embedded Video Size	Average Hiding Time (s)	Success or Failed
1.	144.mp4	633 KB	file.docx	20 KB	doc123	Embedded_Video_144p.mp4	45.933 KB	6,113	Success
2			file1.docx	112 KB		-	-	-	Failed
3			file2.docx	379 KB		-	-	-	Failed
4			file.pdf	13 KB	pdf123	Embedded_Video_144p1.mp4	45.927 KB	6,295	Success
5			file1.pdf	105 KB		-	-	-	Failed
6			file2.pdf	350 KB		-	-	-	Failed
7	360p.mp4	1.575 KB	file.docx	20 KB	doc123	Embedded_Video_360p.mp4	209.286 KB	16,620	Success
8			file1.docx	112 KB		Embedded_Video_360p1.mp4	209.378 KB	18,533	Success
9			file2.docx	379 KB		-	-	-	Failed
10			file.pdf	13 KB	pdf123	Embedded_Video_360p2.mp4	209.279 KB	16,319	Success
11			file.pdf	105 KB		Embedded_Video_360p3.mp4	209.370 KB	17,738	Success
12			file2.pdf	350 KB		-	-	-	Failed
13	720p.mp4	4.401 KB	file.docx	20 KB	doc123	Embedded_Video_720p.mp4	585.612 KB	43,403	Success
14			file1.docx	112 KB		Embedded_Video_720p1.mp4	585.729 KB	48,954	Success
15			file2.docx	379 KB		Embedded_Video_720p2.mp4	586.060 KB	46,912	Success
16			file.pdf	13 KB	pdf123	Embedded_Video_720p3.mp4	585.604 KB	43,622	Success
17			file1.pdf	105 KB		Embedded_Video_720p4.mp4	585.720 KB	42,001	Success
18			file2.pdf	350 KB		Embedded_Video_720p5.mp4	586.024 KB	45,805	Success

Based on Table 1. above, it can be seen that hiding files in videos with low-quality 144p can only be inserted with files with the smallest size, both "docx" and "pdf" files. The other four files cannot be inserted because they exceed the size limit that a 144p.mp4 video frame can store. Then the video with 360p quality can be inserted into two "docx" files and two "pdf" files because the frame is larger than the 144p quality video. Then on the video with the highest quality, which is 720p, all files can be inserted; this is because the video frame has a larger size than the two previous videos, so the maximum limit of the data size that can be inserted is getting bigger.

In the Table 1, it can be seen that there is an apparent difference between the original video and the embedded video, which lies in its size. Embedded video has a considerable size, and this is because the process of making video after file insertion does not use an encoding. Encoding serves to compress the video so that it can reduce its size of the video. However, in video steganography using this LSB method, the encoding process can cause the loss of file data inserted into the frame so that when the file extraction process is run, the file data is not found. In addition, the size of the embedded video is also affected by Frame Per Second (FPS). FPS will

determine the number of frames contained in a video. The greater the number of FPS of a video, the larger the size of the embedded video produced.

Videos with the same content but different video quality, namely 144p, 360p, and 720p, significantly differ in file hiding time. The higher the video quality, the longer the file hiding time will be. From these results it can be seen that the large number of FPS and the larger frame size will affect the process of extracting frames and making embedded videos, thus making the file insertion time longer.

B. Testing the Process of Extracting Files From Embedded Video

This test determines the smooth process of extracting files from embedded video. This test has a frame extraction process and file data decryption. The frame extraction process takes the frames contained in the embedded video and then checks each frame to determine whether there is a secret data file in it. If the data file is found, the data will be decrypted using Fernet; after successfully decrypting, the data will be made into a file according to the extension.

TABLE 2. FILE EXTRACTING TEST RESULT

No.	Embedded Video Name	Embedded Video Size	Extraction File Name	Extraction File Size	Average Extraction Time	Success or Failed
1	Embedded_Video_cat144p.mp4	45.933 KB	extracted_data.docx	20 KB	4,493	Success
2	Embedded_Video_cat144p1.mp4	45.927 KB	extracted_data.pdf	13 KB	4,354	Success
3	Embedded_Video_cat360p.mp4	209.286 KB	extracted_data1.docx	20 KB	11,451	Success
4	Embedded_Video_cat360p1.mp4	209.378 KB	extracted_data2.docx	112 KB	11,579	Success
5	Embedded_Video_cat360p2.mp4	209.279 KB	extracted_data1.pdf	13 KB	11,136	Success
6	Embedded_Video_cat360p3.mp4	209.370 KB	extracted_data2.pdf	105 KB	11,628	Success
7	Embedded_Video_cat720p.mp4	585.612 KB	extracted_data3.docx	20 KB	29,080	Success
8	Embedded_Video_cat720p1.mp4	585.729 KB	extracted_data4.docx	112 KB	27,376	Success
9	Embedded_Video_cat720p2.mp4	586.060 KB	extracted_data5.docx	379 KB	28,752	Success
10	Embedded_Video_cat720p3.mp4	585.604 KB	extracted_data3.pdf	13 KB	26,928	Success
11	Embedded_Video_cat720p4.mp4	585.720 KB	extracted_data4.pdf	105 KB	30,145	Success
12	Embedded_Video_cat720p5.mp4	586.024 KB	extracted_data5.pdf	350 KB	29,816	Success
13	Embedded_Video_cam2bit.mp4	28.162 KB	extracted_data6.docx	112 KB	3,130	Success
14	Embedded_Video_cam4bit.mp4	28.131 KB	extracted_data7.docx		3,097	Success
15	Embedded_Video_cam6bit.mp4	28.110 KB	extracted_data8.docx		3,135	Success

Based on Table 2. above, it can be seen that the file extraction process from all embedded videos was successfully carried out. All files inserted in both "docx" and "pdf" formats have been successfully extracted into a complete file. Files on insertion with different bits were also recovered. File extraction speed is affected by FPS; the higher the quality of a video, the longer the file hiding time will be.

C. Visual Attack Test

Visual attack testing is a test that is carried out by looking for visible differences in the embedded video with the naked eye. If a difference is visible to the naked eye when the embedded video is played, then it indicates that the frame inserted by the message is not of decent quality. Because the purpose of steganography is to keep the data secret so that others do not readily know it, the results of this study can be seen in the Fig 7 and 8.

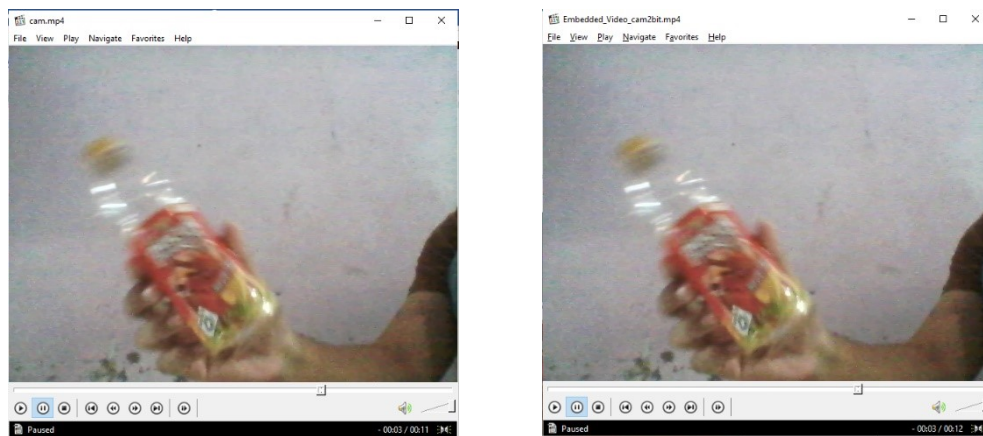


Fig. 7. Before & after video 2bit embedded video footage at 8th seconds

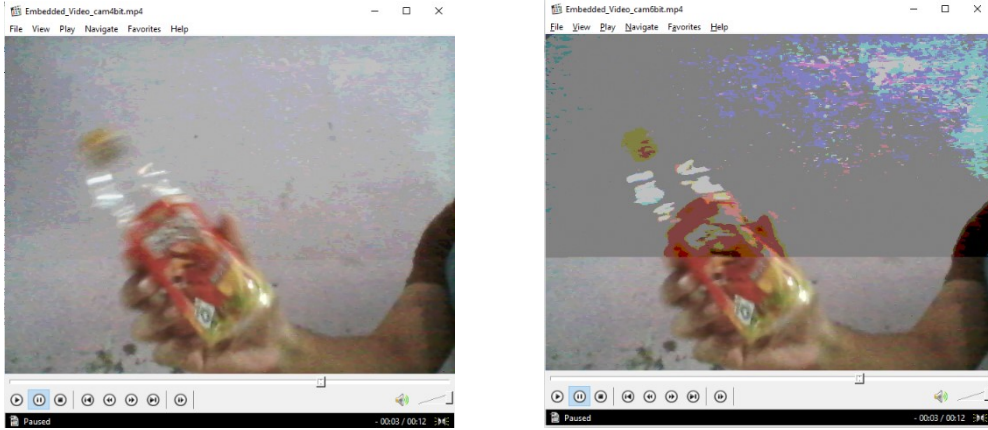


Fig. 8. Before & after video 6bit embedded video footage at 8th seconds

Based on the results above, it can be concluded that the frame inserted by the file at 2 bits of data does not show any visible difference compared to the hidden file at 4 bits and 6 bits of data. Therefore, in this video steganography application, 2 bits of data are used in hiding files.

is more than 30 decibels (> 30 dB), then the image quality after hiding can be said to be good, whereas if the PSNR value is less than 30 decibels (< 30 dB), then the image quality can be said to be poor [28].

D. Peak Signal Noise Ratio (PSNR) Test

PSNR testing is carried out to determine the difference in the quality of the frame, which is the object of hiding the secret file after the process is carried out. If the resulting PSNR value

TABLE 3. PSNR VALUE TEST RESULTS

No.	Original Video Name	File Name	File Size	Order Of Frames (.png)	Frame Size Before Hiding	Frame Size After Hiding	PSNR Value(dB)
1.	144p. mp4	file.docx	20 KB	101	67,8 KB	92,7 KB	44,661
2.		file.Pdf	13 KB			83,9 KB	46,471
3.	360p. mp4	file.docx	20 KB	235	315 KB	351 KB	52,623
4.		file1.docx	112 KB			517 KB	44,984
5.		file.pdf	13 KB			339 KB	54,478
6.		file1.pdf	105 KB			504 KB	45,301
7.	720. mp4	file.docx	20 KB	237	907 KB	952 KB	58,751
8.		file1.docx	112 KB			1.169 KB	51,016
9.		file2.docx	379 KB			1.774 KB	45,732
10.		file.pdf	13 KB			938 KB	60,607
11.		file1.pdf	105 KB			1.150 KB	51,329
12.		file2.pdf	350 KB			1.710 KB	46,080

Based on table 3. above, it can be concluded that the frame inserted in the data file changes significantly in size. If the

inserted file is getting more significant (up to the specified frame size limit), then the frame inserted by the file will be

more oversized. This is inversely proportional to the resulting PSNR value. The larger the file inserted into the frame, the smaller the PSNR value will be. A smaller PSNR value indicates a decrease in the resulting image quality.

In this study, the frame inserted by the file can still be categorized as decent quality because the resulting PSNR value is above 30 dB. However, when inserting files into different bit frames (2 bits, 4 bits, and 6 bits), apart from changing the size, there is also a decrease in frame quality which can be seen from the smaller PSNR value. Based on Table 3, it can be seen that the insertion of a 2-bit frame produces a larger frame size than the insertion of a 4-bit and 6-bit frame. Insertion of 4-bit and 6-bit frames results in a smaller frame size than the original. So it can be concluded that the insertion of files in 4-bit and 6-bit frames is not recommended because the quality of the resulting frame is not feasible to use.

E. Audio Comparison Test

In this study, the audio Bit Rate value and the audio Sample Rate value in the embedded video are the same as the original audio. Therefore, it can be concluded that the audio quality of the embedded video does not change even though the video has been regenerated through frames, one of which contains a secret data file. So in this insertion, the audio quality is maintained, and the audio playback timing follows the original video.

F. Comparison Of The Original File With The Extracted File

Based on the tests that have been carried out, the original file with the extracted file has the same contents, the exact details, and also the same size. So it can be concluded that every file inserted into the video can be entirely recovered without any difference. The following is a table and some pictures that contain a comparison between the original file and the extracted file, all files used in this study can be hidden in the video.

TABLE 4. FILE EXTRACTING TEST RESULT

No.	Original File Name	Original File Size	Extraction File Name	Extraction File Size
1.	file.docx	20 KB	extracted_data3.docx	20 KB
2.	file1.docx	112 KB	extracted_data4.docx	112 KB
3.	file2.docx	379 KB	extracted_data5.docx	379 KB
4.	file.pdf	13 KB	extracted_data3.pdf	13 KB
5.	file1.pdf	105 KB	extracted_data4.pdf	105 KB
6.	file2.pdf	350 KB	extracted_data5.pdf	350 KB

Based on Table 4 above, it can be concluded that the size of the file that has been hidden into the video and then extracted again, both files in .docx or .pdf formats have the same size as the original file without any changes.

IV. CONCLUSSION

The results found that the embedded video's size was huge due to the .png format and the process of merging frames into video without encoding. The use of encoding during video creation will lead to the loss of file data that has been inserted.

Files extracted from embedded videos have not changed, either in the content or in size. Factors that affect embedded video size are the frame format, video quality, Frame Per Second (FPS), file size, and data bits used for file insertion. Hiding files at 2 bits of data results in better frame quality, and there is no visible difference with the original frame, compared to inserting files at 4 bits of data and 6 bits of data which produces steganography frames with noise that is visible to the naked eye. Hiding files at 2 bits of data results in better frame quality, no visible difference with the original frame, and has a PSNR value between 40 dB to 61 dB so that it can be categorized as a decent frame. Hiding files at 4 bits of data and 6 bits of data produces steganography frames with visible noise and have a PSNR value below 40 dB, so it is not feasible to use.

REFERENCES

- [1] N. Roztocki, P. Soja, and H. R. Weistroffer, "The role of information and communication technologies in socioeconomic development: towards a multi-dimensional framework*," *Information Technology for Development*, vol. 25, no. 2, 2019, pp.171–183.
- [2] M. A. Ruben, M. D. Stosic, J. Correale, and D. Blanch-Hartigan, "Is Technology Enhancing or Hindering Interpersonal Communication? A Framework and Preliminary Results to Examine the Relationship Between Technology Use and Nonverbal Decoding Skill," *Front Psychol*, vol. 11, 2021, pp.1-10.
- [3] J. Li *et al.*, "Semantic multi-agent system to assist business integration: An application on supplier selection for shipbuilding yards," *Comput Ind*, vol. 96, 2018, pp.10-26.
- [4] J. Rauh, "Secret sharing and shared information," *Entropy*, vol. 19, no. 11, 2017, pp.2-12.
- [5] N. Sohrabi Safa, R. von Solms, and S. Furnell, "Information security policy compliance model in organizations," *Comput Secur*, vol. 56, pp. 70–82, Feb. 2016, pp.70-82.
- [6] "Steganographic Method of Data Hiding using JPEG Images," *International Journal of Science and Research (IJSR)*, vol. 4, no. 11, pp. 1175–1178, Nov. 2015, doi: 10.21275/v4i11.nov151370.
- [7] S. Basuki and R. Anugrah, "Transaction Document Security Protection In The Form Of Image File, Jpg or Tif Interbank Transfer Using Steganography And Cryptography," *IAIC Transactions on Sustainable Digital Innovation (ITSDI)*, vol. 1, no. 1, 2021, pp.42-48.
- [8] . K., "Image Security using Steganography and Cryptography," *Int J Res Appl Sci Eng Technol*, vol. 9, no. VII, 2021, pp.366-371.
- [9] V. Varuikhin and A. Levina, "Continuous Wavelet Transform Applications in Steganography," in *Procedia Computer Science*, 2021, vol. 186, pp. 580–587. doi: 10.1016/j.procs.2021.04.179.
- [10] A. H. S. Saad, M. S. Mohamed, and E. H. Hafez, "Coverless Image Steganography Based on Optical Mark Recognition and Machine Learning," *IEEE Access*, vol. 9, 2021, pp.16522-16531.
- [11] F. Thabit, A. P. S. Alhomdy, A. H. A. Al-Ahdal, and P. D. S. Jagtap, "A new lightweight cryptographic algorithm for enhancing data security in cloud computing," *Global Transitions Proceedings*, vol. 2, no. 1, pp. 91–99, 2021, doi: 10.1016/j.gltp.2021.01.013.
- [12] V. B. Kirubanad and M. Kumari, "Data encryption and decryption using graph plotting," *International Journal of Civil Engineering and Technology*, vol. 9, no. 2, 2018, pp.36-46.
- [13] N. M. Zamri, S. M. H. Asraf, and S. Z. S. Idrus, "Two Level Security in Delivering Message Using Encryption and Steganography Techniques," in *Journal of Physics: Conference Series*, 2020, vol. 1529, no. 3. pp.1-9.
- [14] Win junaidi, "Algoritma Hill Cipher untuk Enkripsi Data Teks yang digunakan untuk Steganografi gambar dengan Metode LSB (Least Significant Bit)," *Pelita Informatika Budi Darma*, vol. 9, no. 3, 2015. pp.92-99.
- [15] W. Junaidi, "ALGORITMA HILL CHIPER UNTUK ENKRIPSI DATA TEKS YANG DIGUNAKAN UNTUK STEGANOGRAFI GAMBAR DENGAN METODE LSB (LEAST SIGNIFICANT BIT)," *Pelita Informatika Budi Darma*, no. 3, 2015. pp.92-99.
- [16] D. Laoli, B. Sinaga, and A. S. R. M. Sinaga, "Penerapan Algoritma Hill Cipher Dan Least Significant Bit (LSB) Untuk Pengamanan Pesan Pada Citra Digital," *JISKA (Jurnal Informatika Sunan Kalijaga)*, vol. 4, no. 3, 2020, pp.138-148.

- [17] S. G. Supratman, "STEGANOGRAFI DENGAN MENGGUNAKAN METODE LSB DAN ALGORITMA HILL CIPHER," *Buffer Informatika*, vol. 1, no. 1, 2017, pp.38-48.
- [18] O. F. A. Wahab, A. A. M. Khalaf, A. I. Hussein, and H. F. A. Hamed, "Hiding data using efficient combination of RSA cryptography, and compression steganography techniques," *IEEE Access*, vol. 9, 2021, pp.31805-31815
- [19] M. Kaur and A. Kaur, "Improved Security Mechanism of Text in Video using Steganographic Technique: A Review," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 7782, no. 5, 2014. Pp.44-51.
- [20] K. Vyas and B. L. Pal, "a Proposed Method in Image Steganography To Improve Image Quality With Lsb Technique," *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 3, no. 1, 2014. pp.5246-5251.
- [21] T. Barhoom and W. Saqer, "Steganography algorithm within 2-LSBs with indicators-based randomness," *International Journal of Computing and Digital Systems*, vol. 6, no. 5, 2017, pp.272.276.
- [22] D. Rawat and V. Bhandari, "A Steganography Technique for Hiding Image in an Image using LSB Method for 24 Bit Color Image," *Int J Comput Appl*, vol. 64, no. 20, 2013, pp.1-4.
- [23] S. Tripathi, R. K. Tiwari, R. Nigam, N. K. Gupta, and B. Verma, "The hybrid cryptography for enhancing the data security in fog computing," in *Proceedings - 2021 IEEE 10th International Conference on Communication Systems and Network Technologies, CSNT 2021*, 2021. pp. 766-771.
- [24] Pronika and S. S. Tyagi, "Enhancing security of cloud data through encryption with AES and fernet algorithm through Convolutional-Neural-Networks (CNN)," *International Journal of Computer Networks and Applications*, vol. 8, no. 4, 2021, pp.288-299.
- [25] D. P., S. S. Babu, and Y. Vijayalakshmi, "Enhancement of e-commerce security through asymmetric key algorithm," *Comput Commun*, vol. 153, 2020, pp.125-134.
- [26] E. J. Baker *et al.*, "Video steganography using 3D distance calculator based on YCbCr color components," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 24, no. 2, 2021, doi: 10.11591/ijeecs.v24.i2.pp831-842.
- [27] J. Vivek and B. Gadgay, "Video Steganography Using Chaos Encryption Algorithm with High Efficiency Video Coding for Data Hiding," *International Journal of Intelligent Engineering and Systems*, vol. 14, no. 5, 2021, pp.15-24.
- [28] R. L. Oxford and C. Y. Lin, "Autonomous learners in digital realms: Exploring strategies for effective digital language learning," in *Independent Language Learning: Building on Experience, Seeking New Perspectives*, Hong Kong University Press, 2011. pp.157-172.
- [29] Hemanth, *Intelligent Data Analysis for Biomedical Applications*. Elsevier, 2019.

PAPER NAME

Hiding Document Format Files Using Video Steganography Techniques With Least Significant Bit Method.

WORD COUNT

4918 Words

CHARACTER COUNT

24503 Characters

PAGE COUNT

8 Pages

FILE SIZE

810.4KB

SUBMISSION DATE

Jan 31, 2023 12:48 PM GMT+7

REPORT DATE

Jan 31, 2023 12:49 PM GMT+7

● **11% Overall Similarity**

The combined total of all matches, including overlapping sources, for each database.

- 7% Internet database
- 6% Publications database
- Crossref database
- Crossref Posted Content database
- 5% Submitted Works database

● **Excluded from Similarity Report**

- Manually excluded sources
- Manually excluded text blocks

Hiding Document Format Files Using Video Steganography Techniques With Least Significant Bit Method

Tufail Akhmad Satrio
Department of Informatics Engineering
Institut Teknologi Telkom Purwokerto
Purwokerto, Indonesia
tufailas040@gmail.com

Wahyu Adi Prabowo*
Department of Informatics Engineering
Institut Teknologi Telkom Purwokerto
Purwokerto, Indonesia
wahyuadi@ittelkom-pwt.ac.id

Trihastuti Yuniati
Department of Informatics Engineering
Institut Teknologi Telkom Purwokerto
Purwokerto, Indonesia
trihastuti@ittelkom-pwt.ac.id

Abstract—Video Steganography is one type that can use to hide secret messages. Video Steganography is a technique to hide messages in video media by inserting messages into one of the video frames. Cryptography can be combined with the Steganography technique to secure hidden messages in video files. This research was conducted to analyze the LSB (Least Significant Bit) steganography test combined with the Fernet cryptographic process. This study investigates the file insertion process, the test extraction process, the speed of system implementation, the visual attack, the Peak Signal Noise Ratio (PSNR) value, and the audio comparison between original video and video with embedded files. The results of this test indicate that the embedding process in the video is directly proportional to the results received. The larger the original video size, the larger the embedded video size will be.

Keywords—video steganography, cryptography, Least Significant Bit, LSB, Fernet

I. INTRODUCTION

Advances in technology and the internet are currently making various kinds of breakthroughs in the field of data communication. Communication is one of the essential needs in human life to relate to each other [1], [2]. When communicating, there will be an exchange of information between the two parties [3] and often there is essential information that is confidential [4]. Security and confidentiality of data or information are critical in information systems and data communication [5].

The major problem in the digital world, important information or data, is that data is an asset vulnerable to being stolen by others [6]. Recently, there has been renewed interest in data security. One way that is generally used to secure the data is to use a combination of steganography and cryptography [7], [8]. Steganography is one way to hide a message or personal data into data or other messages that appear to contain nothing except for people who know the key [5]. The purpose of steganography is to hide messages and make them invisible to attackers [9] and can even allow someone not to detect a message or data in the file [10]. Cryptography is the art of maintaining the security or confidentiality of data. Cryptography will convert data into specific codes and is only intended for parties with only a key to convert the code back into data [11]. The key is not an object but a secret code known by the party who exchanges information or data and will later be used to encrypt or decrypt data [12]. Encryption is a process carried out to secure a

message (plaintext) into a hidden message (ciphertext), while decryption is the process of converting ciphertext into plaintext [13].

Studies on steganography and cryptography show the importance of data security. Several researchers have attempted to combine the concepts of steganography and cryptography. Steganography with LSB (Least Significant Bit) method and Hill Chipper cryptography can be combined in securing messages [14]–[16]. In some of these studies, image media is used, so the steganography technique can be called Image Steganography. From the results of this study, the process of hiding messages in digital images is safe and unknown to the naked eye because the size of the bitmap resulting from steganography does not change after the process of inserting binary text into a binary bitmap. Using the Least Significant Bit (LSB) method, which replaces the last bit so that the bitmap capacity before and after steganography does not experience significant changes, cryptographic testing can be done encode and decode. Another study combines LSB steganography and RSA cryptography (Rivest-Shamir-Adleman) through video media [17], [18]. The results of this study indicate that this high-level system's performance and methodology have succeeded in performing embedded files compared to other systems using the same methodology [19].

In this study, researchers built an application combining LSB steganography and fernet cryptography on video media. The advantage of this LSB steganography method is that the quality and size of the image after the message is inserted do not look much different [19]. The least significant bit is the part of the binary data sequence (base two) with the most negligible significant/smallest value. It is located on the far right of the bit sequence [20]. In the arrangement of bits in a byte (1 byte = 8 bits), there are the most significant bits (the most significant bit or MSB) and the least significant bit (the least significant bit or LSB) [21]. Fernet is an implementation of symmetric cryptography (also known as “secret key”) authentication [22]. Fernet is a cryptographic method that provides a simple authentication and encryption method using HMAC (Hash-based Message Authentication Code) with SHA256 for authentication and symmetric AES-128 in CBC (Cipher Block Chaining) mode using PKCS7 padding, which offers 128 bits (16 bytes) in length [23], [24].

For this reason, in this study, the researchers built an application that was built using the Python language to insert a file that has been encrypted using cryptography into a video

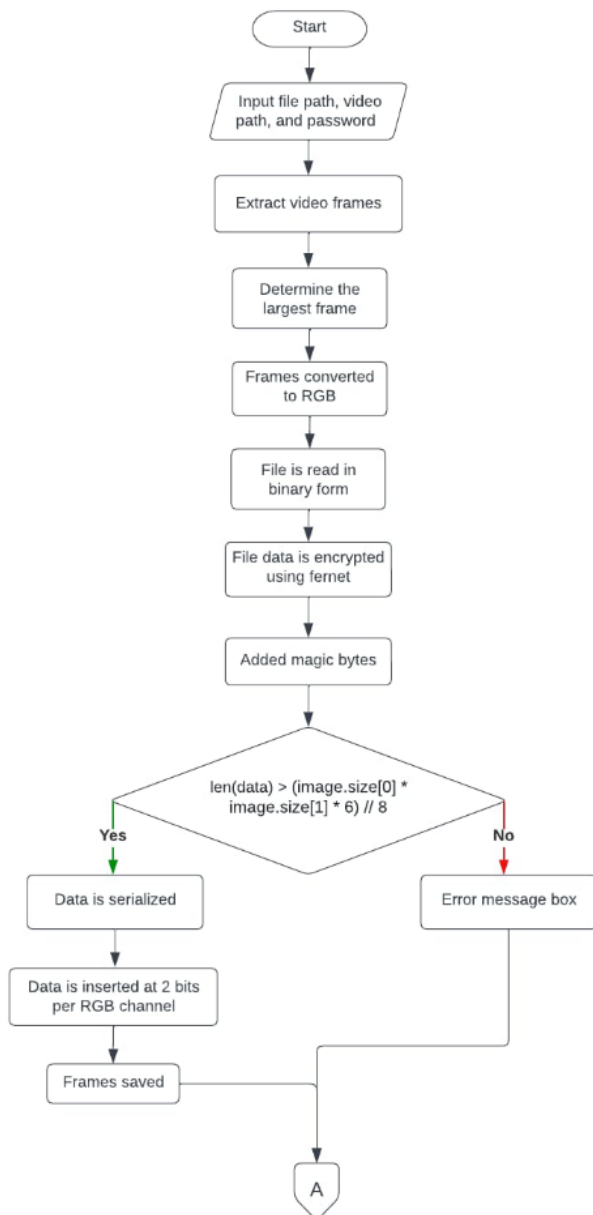


Fig. 1. Flowchart encryption process

that has been determined using steganography techniques, better known as Video Steganography. Video steganography is a technique of hiding or inserting data into a video [25]. In a video, some frames can be inserted into secret messages [26], so if someone wants to extract the message, they must check every frame in the video. The video used is a video in MP4 format. This format was chosen because it is often used by many people and is easy to find on the internet [27]. The files used in inserting messages into videos are files with .docx and .pdf formats. The choice of file with this format is because it can accommodate many messages/data compared to the .txt format, which can only be filled with text messages. Test Analysis of the results of steganography and encryption includes investigating the file insertion process, the test extraction process, the speed of system implementation, the visual attack, the Peak Signal Noise Ratio (PSNR) value, and the audio comparison between original video and video with embedded files. The results of this test indicate that the embedding process in the video is directly proportional to the results received. The larger the original video size, the larger the embedded video size will be.

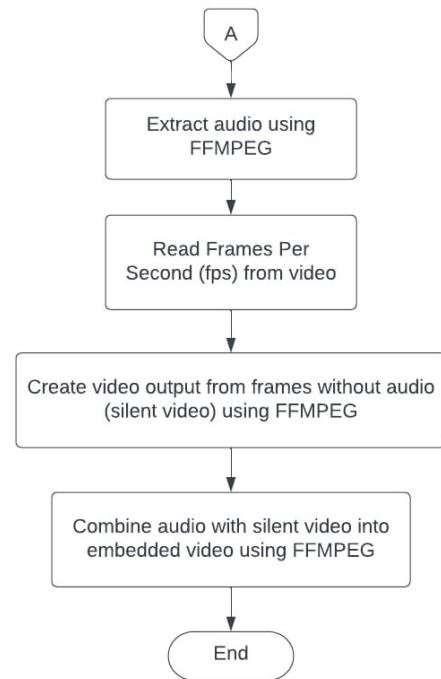


Fig. 2. Flowchart steganography process

II. SYSTEM IMPLEMENTATION

This stage involves applying the methods and techniques used to create application programs. The application implementation uses the python language, which is used to combine LSB steganography and fernet cryptography. The way the first video steganography application works is the insertion of files into the video. This first step aims to enter the file location, video location, and password. Then the inputted video will be extracted frame and audio using FFMPEG, and the frame will be used as a medium for message insertion. The frame selection is based on the largest frame size from a set of extracted frames. The next step is to insert the file into the frame using the LSB method. The file to be inserted is first opened using a binary format, then encrypted using the fernet algorithm to increase the level of data security. Then, the file will be given a unique mark (magic bytes) so that the file is detected in the frame that is the cover object when extracting the video file. After successfully inserting the file, the next step is to unify the frame and audio into a video output containing the secret file. The working process of the video steganography application can be seen in Fig. 1.

Next, the first step in extracting the file is to enter the path of the Embedded Video or video that is inserted the message and enter the password. Next, the video will be extracted its frames to retrieve hidden file data, this process can be seen in Fig. 2.

The next process is extract Data File in Fig. 3, in that process the frames that have been extracted will be selected with the largest size because it contains file data that has been hidden. The frames that have been obtained will be checked for LSB bits, if there are special marks (magic bytes) then the data will be taken from the LSB bits of the frame. Furthermore, the data will be decrypted first to get the original data. Once encrypted, the data will be converted into a file again using binary writing mode. After the file is successfully retrieved, the extract Data File completes.

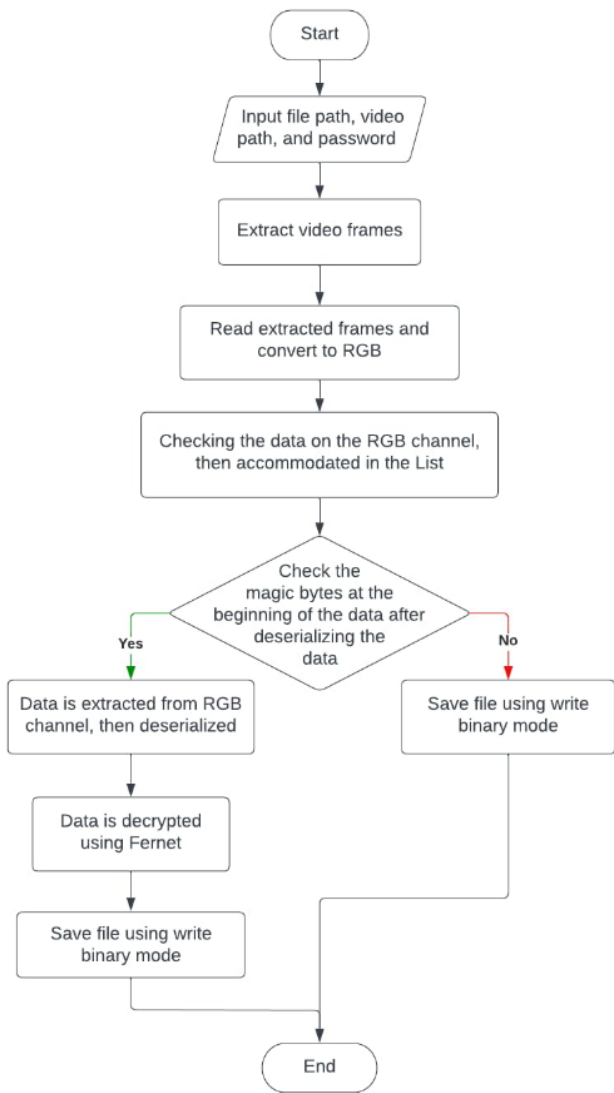


Fig. 3. Flowchart extraction process

The image below in Fig. 4 is the main window of the application. In the main window, there are two buttons, namely the "Hide File" and "Extract Files." The "Hide File" button inserts files into the video. The "Extract File" button is to retrieve files that have been inserted into the video.

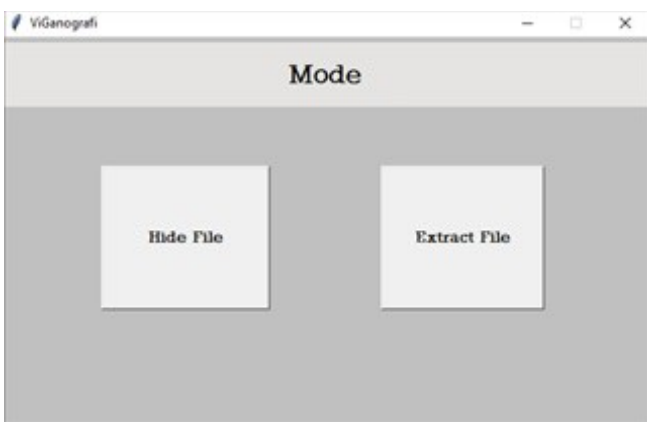


Fig. 4. Main window of the application

When the "Hide File" and "Extract File" button is pressed, then the user will be redirected to a new window as below in Fig. 5.

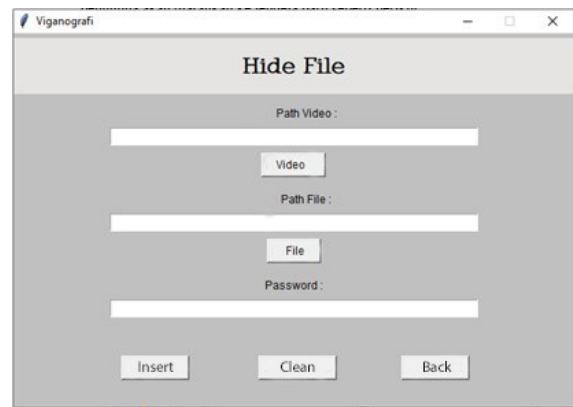


Fig. 5. "Hide File" menu window

In Fig. 5, contains three fields that must be filled in; the three columns are the video path, file path, and password fields. The three columns are inputs or variables used for file insertion into the video. In the "Extract File" menu in Fig. 6, there are two inputs or variables: the video path and password. Both variables must be filled so that the file extraction process runs smoothly.

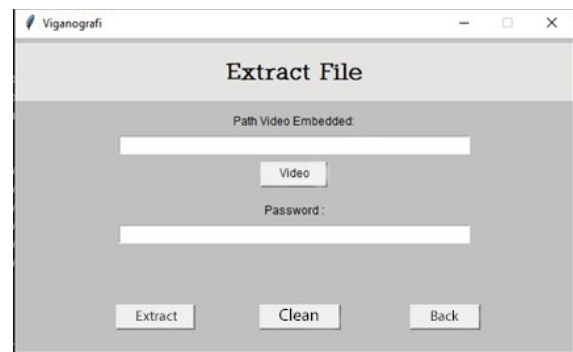


Fig. 6. "Extract File" menu window

III. RESULT AND DISCUSSION

Every process on this system was tested to find out that the system in the application was running well and analyzed the results of the output files received in each running process.

A. Process of Hiding Files Into Videos

In this hiding testing process, four videos and three files are used. The first three videos are similar with a duration of 29 seconds. The first three videos have differences in quality, namely 144p, 360p, and 720p. The video tests the success of the file-hiding process on a 2-bit data frame. Then the last video is used to test the visual attack on the given results. In the last video, the bits used in file hiding are 2 bits, 4 bits, and 6 bits. Then the three files used, both "docx" and "pdf" formats, have different sizes. The difference is applied to find out how big the maximum size of the data file that can be inserted into the video frame.

TABLE 1. FILE HIDING TEST RESULT

No	Original Video Name	Original Video Size	File Name	File Size	Password	Embedded Video Name	Embedded Video Size	Average Hiding Time (s)	Success or Failed
1.	144.mp4	633 KB	file.docx	20 KB	doc123	Embedded_Video_144p.mp4	45.933 KB	6,113	Success
2			file1.docx	112 KB		-	-	-	Failed
3			file2.docx	379 KB		-	-	-	Failed
4			file.pdf	13 KB	pdf123	Embedded_Video_144p1.mp4	45.927 KB	6,295	Success
5			file1.pdf	105 KB		-	-	-	Failed
6			file2.pdf	350 KB		-	-	-	Failed
7	360p.mp4	1.575 KB	file.docx	20 KB	doc123	Embedded_Video_360p.mp4	209.286 KB	16,620	Success
8			file1.docx	112 KB		Embedded_Video_360p1.mp4	209.378 KB	18,533	Success
9			file2.docx	379 KB		-	-	-	Failed
10			file.pdf	13 KB	pdf123	Embedded_Video_360p2.mp4	209.279 KB	16,319	Success
11			file.pdf	105 KB		Embedded_Video_360p3.mp4	209.370 KB	17,738	Success
12			file2.pdf	350 KB		-	-	-	Failed
13	720p.mp4	4.401 KB	file.docx	20 KB	doc123	Embedded_Video_720p.mp4	585.612 KB	43,403	Success
14			file1.docx	112 KB		Embedded_Video_720p1.mp4	585.729 KB	48,954	Success
15			file2.docx	379 KB		Embedded_Video_720p2.mp4	586.060 KB	46,912	Success
16			file.pdf	13 KB	pdf123	Embedded_Video_720p3.mp4	585.604 KB	43,622	Success
17			file1.pdf	105 KB		Embedded_Video_720p4.mp4	585.720 KB	42,001	Success
18			file2.pdf	350 KB		Embedded_Video_720p5.mp4	586.024 KB	45,805	Success

Based on Table 1. above, it can be seen that hiding files in videos with low-quality 144p can only be inserted with files with the smallest size, both "docx" and "pdf" files. The other four files cannot be inserted because they exceed the size limit that a 144p.mp4 video frame can store. Then the video with 360p quality can be inserted into two "docx" files and two "pdf" files because the frame is larger than the 144p quality video. Then on the video with the highest quality, which is 720p, all files can be inserted; this is because the video frame has a larger size than the two previous videos, so the maximum limit of the data size that can be inserted is getting bigger.

In the Table 1, it can be seen that there is an apparent difference between the original video and the embedded video, which lies in its size. Embedded video has a considerable size, and this is because the process of making video after file insertion does not use an encoding. Encoding serves to compress the video so that it can reduce its size of the video. However, in video steganography using this LSB method, the encoding process can cause the loss of file data inserted into the frame so that when the file extraction process is run, the file data is not found. In addition, the size of the embedded video is also affected by Frame Per Second (FPS). FPS will

determine the number of frames contained in a video. The greater the number of FPS of a video, the larger the size of the embedded video produced.

Videos with the same content but different video quality, namely 144p, 360p, and 720p, significantly differ in file hiding time. The higher the video quality, the longer the file hiding time will be. From these results it can be seen that the large number of FPS and the larger frame size will affect the process of extracting frames and making embedded videos, thus making the file insertion time longer.

B. Testing the Process of Extracting Files From Embedded Video

This test determines the smooth process of extracting files from embedded video. This test has a frame extraction process and file data decryption. The frame extraction process takes the frames contained in the embedded video and then checks each frame to determine whether there is a secret data file in it. If the data file is found, the data will be decrypted using Fernet; after successfully decrypting, the data will be made into a file according to the extension.

TABLE 2. FILE EXTRACTING TEST RESULT

No.	Embedded Video Name	Embedded Video Size	Extraction File Name	Extraction File Size	Average Extraction Time	Success or Failed
1	Embedded_Video_cat144p.mp4	45.933 KB	extracted_data.docx	20 KB	4,493	Success
2	Embedded_Video_cat144p1.mp4	45.927 KB	extracted_data.pdf	13 KB	4,354	Success
3	Embedded_Video_cat360p.mp4	209.286 KB	extracted_data1.docx	20 KB	11,451	Success
4	Embedded_Video_cat360p1.mp4	209.378 KB	extracted_data2.docx	112 KB	11,579	Success
5	Embedded_Video_cat360p2.mp4	209.279 KB	extracted_data1.pdf	13 KB	11,136	Success
6	Embedded_Video_cat360p3.mp4	209.370 KB	extracted_data2.pdf	105 KB	11,628	Success
7	Embedded_Video_cat720p.mp4	585.612 KB	extracted_data3.docx	20 KB	29,080	Success
8	Embedded_Video_cat720p1.mp4	585.729 KB	extracted_data4.docx	112 KB	27,376	Success
9	Embedded_Video_cat720p2.mp4	586.060 KB	extracted_data5.docx	379 KB	28,752	Success
10	Embedded_Video_cat720p3.mp4	585.604 KB	extracted_data3.pdf	13 KB	26,928	Success
11	Embedded_Video_cat720p4.mp4	585.720 KB	extracted_data4.pdf	105 KB	30,145	Success
12	Embedded_Video_cat720p5.mp4	586.024 KB	extracted_data5.pdf	350 KB	29,816	Success
13	Embedded_Video_cam2bit.mp4	28.162 KB	extracted_data6.docx	112 KB	3,130	Success
14	Embedded_Video_cam4bit.mp4	28.131 KB	extracted_data7.docx		3,097	Success
15	Embedded_Video_cam6bit.mp4	28.110 KB	extracted_data8.docx		3,135	Success

1 Based on Table 2. above, it can be seen that the file extraction process from all embedded videos was successfully carried out. All files inserted in both "docx" and "pdf" formats have been successfully extracted into a complete file. Files on insertion with different bits were also recovered. File extraction speed is affected by FPS; the higher the quality of a video, the longer the file hiding time will be.

C. Visual Attack Test

Visual attack testing is a test that is carried out by looking for visible differences in the embedded video with the naked eye. If a difference is visible to the naked eye when the embedded video is played, then it indicates that the frame inserted by the message is not of decent quality. Because the purpose of steganography is to keep the data secret so that others do not readily know it, the results of this study can be seen in the Fig 7 and 8.

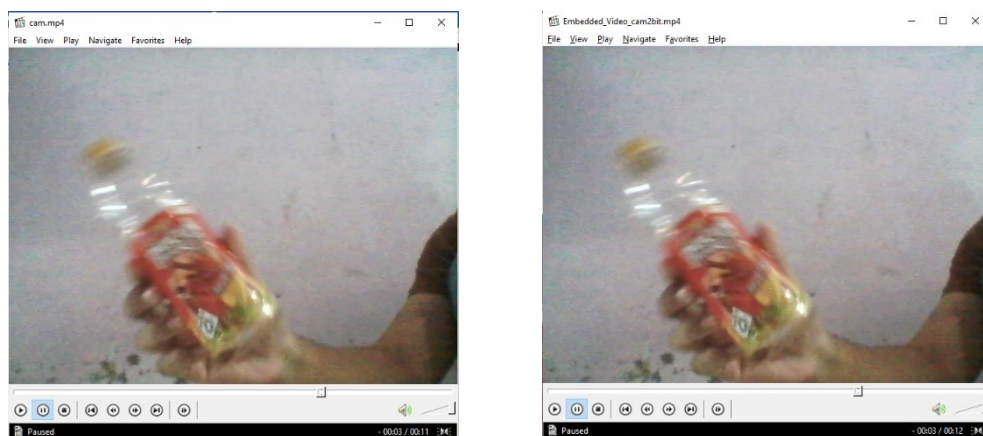


Fig. 7. Before & after video 2bit embedded video footage at 8th seconds

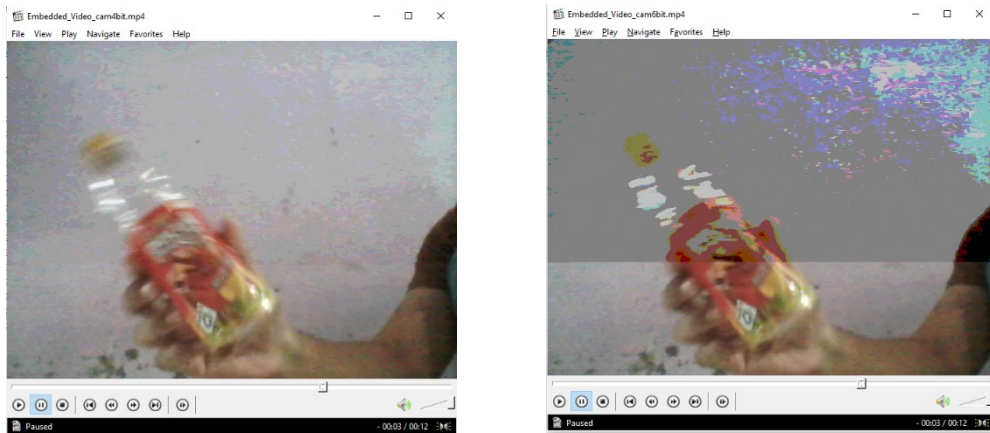


Fig. 8. Before & after video 6bit embedded video footage at 8th seconds

6 Based on the results above, it can be concluded that the frame inserted by the file at 2 bits of data does not show any visible difference compared to the hidden file at 4 bits and 6 bits of data. Therefore, in this video steganography application, 2 bits of data are used in hiding files.

16 is more than 30 decibels (> 30 dB), then the image quality after hiding can be said to be good, whereas if the PSNR value is less than 30 decibels (< 30 dB), then the image quality can be said to be poor [28].

D. Peak Signal Noise Ratio (PSNR) Test

PSNR testing is carried out to determine the difference in the quality of the frame, which is the object of hiding the secret file after the process is carried out. 23 If the resulting PSNR value

TABLE 3. PSNR VALUE TEST RESULTS

No.	Original Video Name	File Name	File Size	Order Of Frames (.png)	Frame Size Before Hiding	Frame Size After Hiding	PSNR Value(dB)
1.	144p. mp4	file.docx	20 KB	101	67,8 KB	92,7 KB	44,661
2.		file.Pdf	13 KB			83,9 KB	46,471
3.	360p. mp4	file.docx	20 KB	235	315 KB	351 KB	52,623
4.		file1.docx	112 KB			517 KB	44,984
5.		file.pdf	13 KB			339 KB	54,478
6.		file1.pdf	105 KB			504 KB	45,301
7.	720. mp4	file.docx	20 KB	237	907 KB	952 KB	58,751
8.		file1.docx	112 KB			1.169 KB	51,016
9.		file2.docx	379 KB			1.774 KB	45,732
10.		file.pdf	13 KB			938 KB	60,607
11.		file1.pdf	105 KB			1.150 KB	51,329
12.		file2.pdf	350 KB			1.710 KB	46,080

Based on table 3. above, it can be concluded that the frame inserted in the data file changes significantly in size. If the

inserted file is getting more significant (up to the specified frame size limit), then the frame inserted by the file will be

more oversized. This is inversely proportional to the resulting PSNR value. The larger the file inserted into the frame, the smaller the PSNR value will be. A smaller PSNR value indicates a decrease in the resulting image quality.

In this study, the frame inserted by the file can still be categorized as decent quality because the resulting PSNR value is above 30 dB. However, when inserting files into different bit frames (2 bits, 4 bits, and 6 bits), apart from changing the size, there is also a decrease in frame quality which can be seen from the smaller PSNR value. Based on Table 3, it can be seen that the insertion of a 2-bit frame produces a larger frame size than the insertion of a 4-bit and 6-bit frame. Insertion of 4-bit and 6-bit frames results in a smaller frame size than the original. So it can be concluded that the insertion of files in 4-bit and 6-bit frames is not recommended because the quality of the resulting frame is not feasible to use.

E. Audio Comparison Test

In this study, the audio Bit Rate value and the audio Sample Rate value in the embedded video are the same as the original audio. Therefore, it can be concluded that the audio quality of the embedded video does not change even though the video has been regenerated through frames, one of which contains a secret data file. So in this insertion, the audio quality is maintained, and the audio playback timing follows the original video.

F. Comparison Of The Original File With The Extracted File

Based on the tests that have been carried out, the original file with the extracted file has the same contents, the exact details, and also the same size. So it can be concluded that every file inserted into the video can be entirely recovered without any difference. The following is a table and some pictures that contain a comparison between the original file and the extracted file, all files used in this study can be hidden in the video.

TABLE 4. FILE EXTRACTING TEST RESULT

No.	Original File Name	Original File Size	Extraction File Name	Extraction File Size
1.	file.docx	20 KB	extracted_data3.docx	20 KB
2.	file1.docx	112 KB	extracted_data4.docx	112 KB
3.	file2.docx	379 KB	extracted_data5.docx	379 KB
4.	file.pdf	13 KB	extracted_data3.pdf	13 KB
5.	file1.pdf	105 KB	extracted_data4.pdf	105 KB
6.	file2.pdf	350 KB	extracted_data5.pdf	350 KB

Based on Table 4 above, it can be concluded that the size of the file that has been hidden into the video and then extracted again, both files in .docx or .pdf formats have the same size as the original file without any changes.

IV. CONCLUSSION

The results found that the embedded video's size was huge due to the .png format and the process of merging frames into video without encoding. The use of encoding during video creation will lead to the loss of file data that has been inserted.

Files extracted from embedded videos have not changed, either in the content or in size. Factors that affect embedded video size are the frame format, video quality, Frame Per Second (FPS), file size, and data bits used for file insertion. Hiding files at 2 bits of data results in better frame quality, and there is no visible difference with the original frame, compared to inserting files at 4 bits of data and 6 bits of data which produces steganography frames with noise that is visible to the naked eye. Hiding files at 2 bits of data results in better frame quality, no visible difference with the original frame, and has a PSNR value between 40 dB to 61 dB so that it can be categorized as a decent frame. Hiding files at 4 bits of data and 6 bits of data produces steganography frames with visible noise and have a PSNR value below 40 dB, so it is not feasible to use.

REFERENCES

- [1] N. Roztock, P. Soja, and H. R. Weist, "The role of information and communication technologies in socioeconomic development: towards a multi-dimensional framework*," *Information Technology for Development*, vol. 25, no. 2, 2019, pp.171-183.
- [2] M. A. Ruben, M. D. Stosic, J. Correale, and D. Blanch-Hartigan, "Is Technology Enhancing or Hindering Interpersonal Communication? A Framework and Preliminary Results to Examine the Relationship Between Technology Use and Nonverbal Decoding Skill," *Front Psychol*, vol. 11, 2021, pp.1-10.
- [3] J. Li *et al.*, "Semantic multi-agent system to assist business integration: An application on supplier selection for shipbuilding yards," *Comput Ind*, vol. 96, 2018, pp.10-26.
- [4] Rauh, "Secret sharing and shared information," *Entropy*, vol. 19, no. 11, 2017, pp.2-12.
- [5] N. Sohrabi Safa, R. von Solms, and S. Furnell, "Information security policy compliance model in organizations," *Comput Secur*, vol. 56, 70-82, Feb. 2016, pp.70-82.
- [6] "Steganographic Method of Data Hiding using JPEG Images," *International Journal of Science and Research (IJSR)*, vol. 4, no. 11, pp. 1175-1178, Nov. 2015, doi: 10.21275/v4i11.nov151370.
- [7] S. Basuki and R. Anugrah, "Transaction Document Security Protection In The Form Of Image File, Jpg or Tif Interbank Transfer Using Steganography And Cryptography," *IAIC Transactions on Sustainable Digital Innovation (ITSDI)*, vol. 1, no. 1, 2021, pp. 48.
- [8] . K., "Image Security using Steganography and Cryptography," *Int J Res Appl Sci Eng Technol*, vol. 9, no. VII, 2021, pp.366-371.
- [9] V. Varuikhin and A. Levina, "Continuous Wavelet Transform Applications in Steganography," *Procedia Computer Science*, 2021, vol. 186, pp. 580-587. doi: 10.1016/j.procs.2021.04.179.
- [10] A. H. S. Saad, M. S. Mohamed, and E. H. Hafez, "Coverless Image Steganography Based on Optical Mark Recognition and Machine Learning," *IEEE Access*, vol. 9, 2021, pp.16522-16531.
- [11] F. Thabit, A. P. S. Alhomdy, A. H. A. Al-Ahdal, and P. D. S. Jagtap, "A new lightweight cryptographic algorithm for enhancing data security in cloud computing," *Global Transitions Proceedings*, vol. 2, no. 1, pp. 91-99, 2021, doi: 10.1016/j.gltp.2021.01.013.
- [12] V. B. Kirubanad and M. Kumari, "Data encryption and decryption using graph plotting," *International Journal of Civil Engineering and Technology*, vol. 9, no. 2, 2018, pp.36-46.
- [13] N. M. Zamri, S. M. H. Asraf, and S. Z. S. Idrus, "Two Level Security in Delivering Message Using Encryption and Steganography Techniques," in *Journal of Physics: Conference Series*, 2020, vol. 1529, no. 3. pp.1-9.
- [14] Win junaidi, "Algoritma Hill Cipher untuk Enkripsi Data Teks yang digunakan untuk Steganografi gambar dengan Metode LSB (Least Significant Bit)," *Pelita Informatika Budi Darma*, vol. 9, no. 3, 2015. pp.92-99.
- [15] W. Junaidi, "ALGORITMA HILL CHIPER UNTUK ENKRIPSI DATA TEKS YANG DIGUNAKAN UNTUK STEGANOGRAFI GAMBAR DENGAN METODE LSB (LEAST SIGNIFICANT BIT)," *Pelita Informatika Budi Darma*, no. 3, 2015. pp.92-99.
- [16] D. Laoli, B. Sinaga, and A. S. R. M. Sinaga, "Penerapan Algoritma Hill Cipher Dan Least Significant Bit (LSB) Untuk Pengamanan Pesan Pada Citra Digital," *JISKA (Jurnal Informatika Sunan Kalijaga)*, vol. 4, no. 3, 2020, pp.138-148.

- [17] S. G. Supratman, "STEGANOGRAFI DENGAN MENGGUNAKAN METODE LSB DAN ALGORITMA HILL CIPHER," *Buffer Informatika*, vol. 1, no. 1, 2017, pp.38-48.
- [18] O. F. A. Wahab, A. A. M. Khalaf, A. I. Hussein, and H. F. A. Hamed, "Hiding data using efficient combination of RSA cryptography, and compression steganography techniques," *IEEE Access*, vol. 9, 2021, pp.31805-31815
- [19] M. Kaur and A. Kaur, "Improved Security Mechanism of Text in Video using Steganographic Technique: A Review," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 7782, no. 5, 2014. Pp.44-51.
- [20] K. Vyas and B. L. Pal, "a Proposed Method in Image Steganography To Improve Image Quality With Lsb Technique," *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 3, no. 1, 2014. pp.5246-5251.
- [21] T. Barhoom and W. Saqer, "Steganography Algorithm within 2-LSBs with indicators-based randomness," *International Journal of Computing and Digital Systems*, vol. 6, no. 5, 2017, pp.272.276.
- [22] R. Rawat and V. Bhandari, "A Steganography Technique for Hiding Image in an Image using LSB Method for 24 Bit Color Image," *Int J Comput Appl*, vol. 64, no. 20, 2013, pp.1-4.
- [23] S. Tripathi, R. K. Tiwari, R. Nigam, N. K. Gupta, and B. Verma, "The hybrid cryptography for enhancing the data security in fog computing," *Proceedings - 2021 IEEE 10th International Conference on Communication Systems and Network Technologies, CSNT 2021*, 2021. pp. 766-771.
- [24] Pronika and S. S. Tyagi, "Enhancing security of cloud data through encryption with AES and fernet algorithm through Convolutional-Neural-Networks (CNN)," *International Journal of Computer Networks and Applications*, vol. 8, no. 4, 2021, pp.288-299.
- [25] D. P., S. S. Babu, and Y. Vijayalakshmi, "Enhancement of e-commerce security through asymmetric key algorithm," *Comput Commun*, vol. 153, 2020, pp.125-134.
- [26] E. J. Baker et al., "Video steganography using 3D distance calculator based on YCbCr color components," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 24, no. 2, 2021, doi: 10.11591/ijeecs.v24.i2.pp831-842.
- [27] J. Vivek and B. Gadgay, "Video Steganography Using Chaos Encryption Algorithm with High Efficiency Video Coding for Data Hiding," *International Journal of Intelligent Engineering and Systems*, vol. 14, no. 5, 2021, pp.15-24.
- [28] R. L. Oxford and C. Y. Lin, "Autonomous learners in digital realms: Exploring strategies for effective digital language learning," in *Independent Language Learning: Building on Experience, Seeking New Perspectives*, Hong Kong University Press, 2011. pp.157-172.
- [29] Hemanth, *Intelligent Data Analysis for Biomedical Applications*. Elsevier, 2019.

● **11% Overall Similarity**

Top sources found in the following databases:

- 7% Internet database
- Crossref database
- 5% Submitted Works database
- 6% Publications database
- Crossref Posted Content database

TOP SOURCES

The sources with the highest number of matches within the submission. Overlapping sources will not be displayed.

1	ejournal.raharja.ac.id Internet	2%
2	semanticscholar.org Internet	1%
3	"Program Schedule", 2022 IEEE International Conference on Communic... Crossref	<1%
4	dergipark.org.tr Internet	<1%
5	I Wayan Mustika, Fauza Khair, Anggun Fitriani Isnawati, Annisa Nur Aini... Crossref	<1%
6	tnsroindia.org.in Internet	<1%
7	ijitee.org Internet	<1%
8	CSU Office of the Chancellor on 2022-04-26 Submitted works	<1%

9	Amrita Vishwa Vidyapeetham on 2022-06-29	<1%
	Submitted works	
10	link.springer.com	<1%
	Internet	
11	ijcaonline.org	<1%
	Internet	
12	Edge Hill University on 2019-03-26	<1%
	Submitted works	
13	Islamic University of Gaza on 2019-03-02	<1%
	Submitted works	
14	researchgate.net	<1%
	Internet	
15	ABV-Indian Institute of Information Technology and Management Gwal...	<1%
	Submitted works	
16	De Rosal Ignatius Moses Setiadi, Supriadi Rustad, Pulung Nurtantio An...	<1%
	Crossref	
17	Napier University on 2017-04-23	<1%
	Submitted works	
18	Elly Matul Imah, Ivan Kurnia Laksono, Karisma Karisma, Atik Wintarti. "...	<1%
	Crossref	
19	Khalid A. Al-Afandy, Osama S. Faragallah, Ahmed Elmhawwy, El-Sayed ...	<1%
	Crossref	
20	Methaq Talib Gaata, Mustafa Dhiaa Al-Hassani. "Underwater image co...	<1%
	Crossref	

21	Universiti Tenaga Nasional on 2021-05-10	<1%
	Submitted works	
22	University of Stirling on 2022-01-14	<1%
	Submitted works	
23	ijece.iaescore.com	<1%
	Internet	
24	Aditya Kotkar, Shreyas Khadapkar, Aniket Gupta, Smita Jangale. "Multi...	<1%
	Crossref	
25	Coventry University on 2022-08-12	<1%
	Submitted works	
26	Mustafa Munther Mashkour, Lahieb Mohammed Jawad. "Compressed ...	<1%
	Crossref	
27	University Tun Hussein Onn Malaysia on 2017-06-06	<1%
	Submitted works	
28	University of Durham on 2019-09-05	<1%
	Submitted works	
29	Xue-Hang Qian, Guang-Bao Xu, Hua-Kun Wang, Dong-Huan Jiang. "Thr...	<1%
	Crossref	
30	scholar.archive.org	<1%
	Internet	
31	neliti.com	<1%
	Internet	
32	"Proceedings of International Conference on Communication and Netw...	<1%
	Crossref	

33

emerald.com

Internet

<1%

● Excluded from Similarity Report

- Manually excluded sources
- Manually excluded text blocks

EXCLUDED SOURCES

Tufail Akhmad Satrio, Wahyu Adi Prabowo, Trihastuti Yuniati. "Hiding Docume... 78%
Crossref

EXCLUDED TEXT BLOCKS

2022 IEEE International Conference on Communication, Networks and Satellite (C...
I Wayan Mustika, Fauza Khair, Anggun Fitriani Isnawati, Annisa Nur Aini Maryadi, Dwi Edi Setyawan, Arrizky A...

Hiding Document Format Files Using VideoSteganography Techniques With Least ...
www.semanticscholar.org

EngineeringInstitut Teknologi Telkom PurwokertoPurwokerto, Indonesia
Ghina Fahira, Alfin Hikmaturokhman, Achamd Rizal Danisya. "5G NR Planning at mmWave Frequency : Study...

EngineeringInstitut Teknologi Telkom PurwokertoPurwokerto, Indonesia
I Wayan Mustika, Fauza Khair, Anggun Fitriani Isnawati, Annisa Nur Aini Maryadi, Dwi Edi Setyawan, Arrizky A...

2022 IEEE International Conference on Communication, Networks and Satellite (C...
I Wayan Mustika, Fauza Khair, Anggun Fitriani Isnawati, Annisa Nur Aini Maryadi, Dwi Edi Setyawan, Arrizky A...

2022 IEEE International Conference on Communication, Networks and Satellite (C...
I Wayan Mustika, Fauza Khair, Anggun Fitriani Isnawati, Annisa Nur Aini Maryadi, Dwi Edi Setyawan, Arrizky A...

Algoritma Hill
widuri.raharja.info

ALGORITMA HILL CHIPER UNTUK ENKRIPSIDATA TEKS YANG DIGUNAKAN UNTU...
widuri.raharja.info

REFERENCES[1]N. Roztocki, P. Soja, and H. R. Weistroffer, "The role of information...

Niranjan Rao Deevela, Farheen Chishti, Bhim Singh, Tara C. Kandpal. "NGK-LMS Control for Grid Connected ...

M. A. Ruben, M. D. Stosic, J. Correale, and D. Blanch-Hartigan, "IsTechnology Enha...

lersse-dl.ece.ubc.ca

J. Li et al., "Semantic multi-agent system to assist businessintegration: An applica...

ijstr.org

N. Sohrabi Safa, R. von Solms, and S. Furnell, "Information securitypolicy complian...

pdfs.semanticscholar.org

Basuki and R. Anugrah, "Transaction Document SecurityProtection In The Form Of ...

media.neliti.com

V. Varuikhin and A. Levina, "Continuous Wavelet TransformApplications in Stegan...

journal.unipdu.ac.id

A. H. S. Saad, M. S. Mohamed, and E. H. Hafez, "Coverless ImageSteganography B...

Lalit Negi, Lokesh Negi. "Hybrid approach for Data Security using Coverless Image Steganography with AES"...

11]F. Thabit, A. P. S. Alhomdy, A. H. A. Al-Ahdal, and P. D. S. Jagtap, "A new lightw...

downloads.hindawi.com

N. M

University of Northumbria at Newcastle on 2021-01-04

B. Sinaga, and A. S. R. M. Sinaga, "Penerapan AlgoritmaHill Cipher Dan Least Signi...

ejournal.uin-suka.ac.id

STEGANOGRAFI DENGAN MENGGUNAKANMETODE LSB DAN ALGORITMA HILL C...

Yati Nurhayati, Siti Maesyarah, Sherly Gina Supartman, Erlan Darmawan, Elin Herlina. "Implementation of the..."

18]O. F. A. Wahab, A. A. M. Khalaf, A. I. Hussein, and H. F. A. Hamed, "Hiding data u...

Estabraq Hussein Jasim Halboos, Abbas M. Albakry. "Improve steganography system using agents softwar..."

Kaur, "Improved Security Mechanism of Text inVideo using Steganographic Techni...

www.ijaerd.com

Vyas and B. L. Pal, "a Proposed Method in Image SteganographyTo Improve Image...

www.jatit.org

Tyagi, "Enhancing security of cloud data throughencryption with AES and fernet al...

ijettjournal.org

E. J. Baker et al., "Video steganography using 3D distance calculatorbased on YCb...

Methaq Talib Gaata, Mustafa Dhiaa Al-Hassani. "Underwater image copyright protection using robust water..."

J. Vivek and B. Gadgay, "Video Steganography Using ChaosEncryption Algorithm ...

inass.org

R. L. Oxford

Cheng, Gary, and Juliana Chau. "Exploring the relationship between students' self-regulated learning ability a..."

D. P., S. S. Babu, and Y. Vijayalakshmi, "Enhancement of e-commerce security thro...

Qixin Zhang. "An Overview and Analysis of Hybrid Encryption: The Combination of Symmetric Encryption an..."