Lecture Notes in Networks and Systems 1004

Xin-She Yang
Simon Sherratt
Nilanjan Dey
Amit Joshi *Editors*

Proceedings of Ninth International Congress on Information and Communication Technology

ICICT 2024, London, Volume 8

Springer

Lecture Notes in Networks and Systems

Volume 1004

The series "Lecture Notes in Networks and Systems" publishes the latest developments in Networks and Systems—quickly, informally and with high quality. Original research reported in proceedings and post-proceedings represents the core of LNNS.

Volumes published in LNNS embrace all aspects and subfields of, as well as new challenges in, Networks and Systems.

The series contains proceedings and edited volumes in systems and networks, spanning the areas of Cyber-Physical Systems, Autonomous Systems, Sensor Networks, Control Systems, Energy Systems, Automotive Systems, Biological Systems, Vehicular Networking and Connected Vehicles, Aerospace Systems, Automation, Manufacturing, Smart Grids, Nonlinear Systems, Power Systems, Robotics, Social Systems, Economic Systems and other. Of particular value to both the contributors and the readership are the short publication timeframe and the world-wide distribution and exposure which enable both a wide and rapid dissemination of research output.

The series covers the theory, applications, and perspectives on the state of the art and future developments relevant to systems and networks, decision making, control, complex processes and related areas, as embedded in the fields of interdisciplinary and applied sciences, engineering, computer science, physics, economics, social, and life sciences, as well as the paradigms and methodologies behind them.

Indexed by SCOPUS, INSPEC, WTI Frankfurt eG, zbMATH, SCImago.

All books published in the series are submitted for consideration in Web of Science.

For proposals from Asia please contact Aninda Bose (aninda.bose@springer.com).

Xin-She Yang · Simon Sherratt · Nilanjan Dey · Amit Joshi
Editors

Proceedings of Ninth International Congress on Information and Communication Technology

ICICT 2024, London, Volume 8

Springer

Editors
Xin-She Yang
Middlesex University
London, UK

Simon Sherratt
University of Reading
Reading, UK

Nilanjan Dey
Techno India College of Technology
Kolkata, West Bengal, India

Amit Joshi
Global Knowledge Research Foundation
Ahmedabad, Gujarat, India

ISSN 2367-3370 ISSN 2367-3389 (electronic)
Lecture Notes in Networks and Systems
ISBN 978-981-97-3304-0 ISBN 978-981-97-3305-7 (eBook)
https://doi.org/10.1007/978-981-97-3305-7

Preface

The Ninth International Congress on Information and Communication Technology will be held during February 19–22, 2024, in a hybrid mode, Physical at London, UK and Digital Platform : Zoom. ICICT 2024 organized by Global Knowledge Research Foundation and Managed by G. R. Scholastic LLP. The associated partners were Springer and Springer Nature. The conference will provide a useful and wide platform both for display of the latest research and for exchange of research results and thoughts. The participants of the conference will be from almost every part of the world, with backgrounds of either academia or industry, allowing a real multinational multicultural exchange of experiences and ideas.

A great pool of more than 2400 papers were received for this conference from across 129 countries among which around 485 papers were accepted and will be presented physically at London and Digital platform Zoom during the four days. Due to the overwhelming response, we had to drop many papers in the hierarchy of the quality. Total 70 technical sessions will be organized in parallel in 4 days along with a few keynotes and panel discussions in hybrid mode. The conference will be involved in deep discussion and issues which will be intended to solve at global levels. New technologies will be proposed, experiences will be shared, and future solutions for design infrastructure for ICT will also be discussed. The final papers will be published in ten volumes of proceedings by Springer LNNS Series. Over the years. this congress has been organized and conceptualized with collective efforts of a large number of individuals. I would like to thank each of the committee members and the reviewers for their excellent work in reviewing the papers. Grateful acknowledgements are extended to the team of Global Knowledge Research Foundation for their valuable efforts and support.

I look forward to welcoming you to the 10th Edition of this ICICT Congress 2025.

Amit Joshi, Ph.D.
Organising Secretary, ICICT 2024
Director—Global Knowledge Research Foundation
Ahmedabad, India

Contents

Editors and Contributors

About the Editors

Xin-She Yang obtained his D.Phil. in Applied Mathematics from the University of Oxford and subsequently worked at the Cambridge University and the National Physical Laboratory (UK) as a Senior Research Scientist. He is currently Reader in Modeling and Optimization at Middlesex University London and Adjunct Prof. at Reykjavik University (Iceland). He is also elected Bye-Fellow at Cambridge University and the IEEE CIS Chair for the Task Force on Business Intelligence and Knowledge Management. He was included in the "2016 Thomson Reuters Highly Cited Researchers" list.

Simon Sherratt was born near Liverpool, England, in 1969. He is currently Prof. of Biosensors at the Department of Biomedical Engineering, University of Reading, UK. His main research area is signal processing and personal communications in consumer devices, focusing on wearable devices and health care. He received the first place IEEE Chester Sall Memorial Award in 2006, the second place in 2016, and the third place in 2017.

Nilanjan Dey is Assistant Prof. at the Department of Information Technology, Techno India College of Technology, India. He has authored/edited more than 75 books with Springer, Elsevier, Wiley, CRC Press and published more than 300 peer-reviewed research papers. He is Editor-in-Chief of the International *Journal of Ambient Computing and Intelligence*; Series Co-editor of *Springer Tracts in Nature-Inspired Computing* (STNIC); and Series Co-editor of *Advances in Ubiquitous Sensing Applications for Healthcare*, Elsevier.

Amit Joshi is Director of Global Knowledge Research Foundation, also Entrepreneur and Researcher who has completed his masters' and research in the areas of cloud computing and cryptography in medical imaging. He has an experience of around ten years in academic and industry in prestigious organizations. He is Active Member

of ACM, IEEE, CSI, AMIE, IACSIT-Singapore, IDES, ACEEE, NPA, and many other professional societies. He is International Chair of InterYIT at International Federation of Information Processing. He has presented and published more than 50 papers in national and international journals/conferences of IEEE and ACM. He has also edited more than 40 books which are published by Springer, ACM, and other reputed publishers. He has also organized more than 50 national and international conferences and programs in association with ACM, Springer, and IEEE to name a few across different countries including India, UK, Europe, USA, Canada, Thailand, Egypt, and many more.

Contributors

Hafiza Abas Centre of Research for Fiqh Science and Technology (CFiRST), Ibnu Sina Institute for Scientific and Industrial Research (ISI-ISIR), Universiti Teknologi Malaysia (UTM), Skudai, Malaysia

Mohamed Abdel El Ghany German University in Cairo (GUC), Cairo, Egypt

Rosl A. Abdul Jabbar Department of Communication Engineering, College of Electronics Engineering, Ninevah University, Mosul, Iraq

Dilman S. Abdulla Computer Department, College of Science, University of Halabja-Halabja, Halabja, Iraq

C. Abingabiye University of Madras, Chennai, India

Muhamad Fazil Ahmad Universiti Sultan Zainal Abidin, Kuala, Malaysia

M. J. Akshay Department of Information Science and Engineering, Jawaharlal Nehru New College of Engineering, Shivamogga, India

Sharmin Akther Noakhali Science and Technology University, Noakhali, Bangladesh

Abdul Halim Ali Faculty of Languages and Communications, Universiti Pendidikan Sultan Idris Tanjong Malim, Tanjong Malim, Malaysia

Karl Andersson Pervasive and Mobile Computing Laboratory, Luleå University of Technology, Skellefteå, Sweden

Bassou Aouijil Faculty of Science and Technology, Moulay Ismail University of Meknes, Errachidia, Morocco

Miguel Arcos-Argudo Salesian Polytechnic University, Cuenca, Ecuador

P. Ashok Symbiosis Institute of Digital and Telecom Management (SIDTM), Symbiosis International (Deemed University), Pune, Maharashtra, India

Mariel Avalos The University of Oklahoma, Norman, OK, USA

Kardo O. Aziz Computer Department, College of Science, Charmo University, Sulaymaniyah, Iraq

Mohammad Tarek Aziz Rangamati Science and Technology University, Rangamati, Bangladesh

G. Bisetsa Jururyishya College of Science and Technology, African of Center of Excellence in Internet of Things, University of Rwanda, Kigali, Rwanda

Rodolfo Bojorque Salesian Polytechnic University, Cuenca, Ecuador

Filip Cák Faculty of Informatics and Information Technologies, Institute of Informatics, Information Systems and Software Engineering, Slovak University of Technology in Bratislava, Bratislava, Slovakia

Diego Cabezas Salesian Polytechnic University, Cuenca, Ecuador

Philippe Canalda University of Franche Comte (UFC), Montbeliard, France

Nicole Alexandra Argote Carrasco Universidad Privada del Norte, Lima, Peru

Mario Casillo DiSPAC, University of Salerno, Fisciano, SA, Italy;
DIIn, University of Salerno, Fisciano, SA, Italy

Liliana Cecere DIIn, University of Salerno, Fisciano, SA, Italy

Heyul Chavez Research and Development Laboratory in Emerging Technologies, Universidad Peruana de Ciencias Aplicadas, Lima, Peru

Lin Chen Zhejiang University of Technology, Hangzhou, China;
Zhejiang University of Technology, Hangzhou, China

J. Claude Habimana College of Science and Technology, African of Center of Excellence in Internet of Things, University of Rwanda, Kigali, Rwanda

Francesco Colace DIIn, University of Salerno, Fisciano, SA, Italy

Cesar Cruz Research and Development Laboratory in Emerging Technologies, Universidad Peruana de Ciencias Aplicadas, Lima, Peru

Pavle Dakić Faculty of Informatics and Information Technologies, Institute of Informatics, Information Systems and Software Engineering, Slovak University of Technology in Bratislava, Bratislava, Slovakia;
Faculty of Informatics and Computing, Singidunum University, Belgrade, Serbia

Nippon Datta Rangamati Science and Technology University, Rangamati, Bangladesh

Guy Degla Institute of Mathematics and Sciences Physics, Porto-Novo, Benin

Simon Pierre Dembele Institute of Computer Science, University of Tartu, Tartu, Estonia

Idy Diop Cheikh Anta Diop University of Dakar (UCAD), Dakar, Senegal

Ibra Dioum Cheikh Anta Diop University of Dakar (UCAD), Dakar, Senegal

Zhelyana Doneva University of Plovdiv Paisii Hilendarski, Plovdiv, Bulgaria

Marie-Louise Dossou-Yovo Institute of Mathematics and Sciences Physics, Porto-Novo, Benin

Bana Shekh Faraj Blackburn College, Blackburn, UK;
Blackburn College, Blackburn, UK

Maskanatul Fiqiyah Faculty of Languages and Communications, Universiti Pendidikan Sultan Idris Tanjong Malim, Tanjong Malim, Malaysia

Mohammed Z. Mohammed Fwzi College of Electronics Engineering, Ninevah University, Mosul, Iraq

Silvia Gaftandzhieva University of Plovdiv Paisii Hilendarski, Plovdiv, Bulgaria

Joaquín Gairín Center for Research and Studies for Organizational Development (CRiEDO), Universitat Autònoma de Barcelona, Bellaterra, Spain

Tsend Ganbat University of Otgontenger, Ulaanbaatar, Mongolia

Norma Inés Caldas Gayoso Universidad Privada del Norte, Lima, Peru

Wan Rohila Ganti Wan Abdul Ghapar Universiti Sultan Zainal Abidin, Kuala, Malaysia

Tomáš Golis Faculty of Informatics and Information Technologies, Institute of Informatics, Information Systems and Software Engineering, Slovak University of Technology in Bratislava, Bratislava, Slovakia

Valeria Alexandra Solano Guevara Universidad Privada del Norte, Lima, Peru

Samsuddin Abd Hamid Faculty of Human Sciences, Universiti Pendidikan Sultan Idris, Tanjong Malim, Malaysia

Zulkiflee Haron Centre of Research for Fiqh Science and Technology (CFiRST), Ibnu Sina Institute for Scientific and Industrial Research (ISI-ISIR), Universiti Teknologi Malaysia (UTM), Skudai, Malaysia

Seema B. Hegde Department of Electronics and Communication, Siddaganga Institute of Technology, Tumakuru, India

Aminudin Bin Hehsan Centre of Research for Fiqh Science and Technology (CFiRST), Ibnu Sina Institute for Scientific and Industrial Research (ISI-ISIR), Universiti Teknologi Malaysia (UTM), Skudai, Malaysia

Carlos Herrera Research and Development Laboratory in Emerging Technologies, Universidad Peruana de Ciencias Aplicadas, Lima, Peru

Angie Dayhanna Ramos Hidalgo Universidad Privada del Norte, Lima, Peru

Abhishek C. Hooli Department of Master of Computer Applications, Siddaganga Institute of Technology, Tumakuru, India

Mohammad Shahadat Hossain University of Chittagong, Chittagong, Bangladesh

Samien Naif Hossain University of Greenwich, London, UK

Miftachul Huda Faculty of Human Sciences, Universiti Pendidikan Sultan Idris Tanjong Malim, Tanjong Malim, Malaysia;
Faculty of Human Sciences, Universiti Pendidikan Sultan Idris Tanjong Malim, Tanjong Malim, Malaysia

Mohd Fauzi Abu Hussin Centre of Research for Fiqh Science and Technology (CFiRST), Ibnu Sina Institute for Scientific and Industrial Research (ISI-ISIR), Universiti Teknologi Malaysia (UTM), Skudai, Malaysia

Azman Ismail National Academy of Arts, Culture and Heritage, Kuala Lumpur, Malaysia

Panabergenova Jamilya Karakalpak State University Named After Berdakh, Nukus, Uzbekistan

Muhammad Talhah Ajmain Jima'ain Faculty of Social Science and Humanities, Universiti Teknologi Malaysia, Skudai, Malaysia

Juhazren Junaidi Centre of Research for Fiqh Science and Technology (CFiRST), Ibnu Sina Institute for Scientific and Industrial Research (ISI-ISIR), Universiti Teknologi Malaysia (UTM), Skudai, Malaysia

S. Kannadhasan Department of Electronics and Communication Engineering, Study World College of Engineering, Coimbatore, Tamilnadu, India

Summrina Kanwal Center for Applied Intelligent Systems Research, Halmstad University, Halmstad, Sweden

Harem Karem Pasewan Organization, Sulaymaniyah, Iraq

Umarova Karligash Karakalpak State University Named After Berdakh, Nukus, Uzbekistan

Khairul Ghufran Kaspin Faculty of Human Sciences, Universiti Pendidikan Sultan Idris Tanjong Malim, Tanjong Malim, Malaysia

Soki Kawashima Nagoya Institute of Technology, Nagoya, Aichi, Japan

Guillermo Kemper Research and Development Laboratory in Emerging Technologies, Universidad Peruana de Ciencias Aplicadas, Lima, Peru

Faiza Khan School of Electrical Engineering and Computer Science, NUST, Islamabad, Pakistan

Ryosuke Kinoshita Nagoya Institute of Technology, Nagoya, Aichi, Japan

Aarya V. Kulkarni Pune, Maharashtra, India

Ovee V. Kulkarni Pune, Maharashtra, India

S. N. Kumar Department of Electrical and Electronics Engineering, Amal Jyothi College of Engineering, Koovappally, Kerala, India

Yulia Kumar Department of Computer Science and Technology, Kean University, Union, NJ, USA

J. Jenny Li Department of Computer Science and Technology, Kean University, Union, NJ, USA

Marco Lombardi DiSPAC, University of Salerno, Fisciano, SA, Italy

Angelo Lorusso DIIn, University of Salerno, Fisciano, SA, Italy

Gabriela Lucas Salesian Polytechnic University, Cuenca, Ecuador

Kimberly Milena Morales Luna Universidad Privada del Norte, Lima, Peru

Jens Lundström Center for Applied Intelligent Systems Research, Halmstad University, Halmstad, Sweden

Tanjim Mahmud Rangamati Science and Technology University, Rangamati, Bangladesh

Maryam M. Al Dabel Department of Computer Science and Engineering, College of Computer Science and Engineering, University of Hafr Al Batin, Hafr Al Batin, Saudi Arabia

Abduljabar M. Maroof Kurdish Department, College of Languages, University of Sulaimani, Sulaymaniyah, Iraq

Koki Matsuno Ritsumeikan University, Kusatsu, Shiga, Japan

Alessandra Micalizzi Pegaso University, Naples, Italy;
SAE Institute, Milan, Italy

Mohsina Mishra Electrical and Electronics Engineering Department, Global College of Engineering and Technology, Muscat, Oman

Takeshi Mizumoto Hylable Inc, Toshima-City, Tokyo, Japan

Kebashnee Moodley University of Witwatersrand, Braamfontein, Johannesburg, South Africa

Pilar Morquecho-Yunga Salesian Polytechnic University, Cuenca, Ecuador

Alfonso R. Vargas Murillo Universidad Privada del Norte, Lima, Peru

R. Musabe College of Science and Technology, African of Center of Excellence in Internet of Things, University of Rwanda, Kigali, Rwanda

Mukhamad Hadi Musolin Universiti Islam Antarabangsa Sultan Abdul Halim Mu'adzam Shah, Kuala Ketil, Malaysia

Jamyandorj Narantuya Mongolian Academy of Sciences, Brain and Mind Research Institute, Ulaanbaatar, Mongolia

Munkhjargal Narantuya National University of Mongolia, Ulaanbaatar, Mongolia

Massa Ndong Cheikh Anta Diop University of Dakar (UCAD), Dakar, Senegal

Mariame Niang Cheikh Anta Diop University of Dakar (UCAD), Dakar, Senegal

K. Nithish Kumar Chennai, Tamilnadu, India

Slawomir Nowaczyk Center for Applied Intelligent Systems Research, Halmstad University, Halmstad, Sweden

F. Nzanywayingoma College of Science and Technology, African of Center of Excellence in Internet of Things, University of Rwanda, Kigali, Rwanda

Daniel Ogwok University of Johannesburg, Johannesburg, South Africa

Lizeth Aracelly López Orosco Universidad Privada del Norte, Lima, Peru

Acheampong Owusu Business School, University of Ghana, Legon, Accra, Ghana

Francisco Carlos Paletta Universidade de São Paulo, São Paulo, Brazil

S. Parameswari Department of Electronics and Communication Engineering, Sri Sairam Institute of Technology, Chennai Tamilnadu, India

Heng Peng Dongguan Polytechnic, Dongguan, China

Jackson Phiri University of Zambia (UNZA), Lusaka, Zambia

Andrea Plaza-Cordero Salesian Polytechnic University, Cuenca, Ecuador

B. G. Premasudha Department of Master of Computer Applications, Siddaganga Institute of Technology, Tumakuru, India

Sari Laelatul Qodriah Universitas Muhammadiyah Cirebon, Cirebon, Jawa Barat, Indonesia

Mahmoud Rahat Center for Applied Intelligent Systems Research, Halmstad University, Halmstad, Sweden

K. Ramachandran Department of Mechanical Engineering, Study World College of Engineering, Coimbatore, Tamilnadu, India

Jhoanna Steffanny Serratti Ramos Universidad Privada del Norte, Lima, Peru

Firend Al. Rasch American University of Malta, Cospicua, Malta

Carlos Raymundo Research and Development Laboratory in Emerging Technologies, Universidad Peruana de Ciencias Aplicadas, Lima, Peru

Moh Abdul Rohim Faculty of Human Sciences, Universiti Pendidikan Sultan Idris Tanjong Malim, Tanjong Malim, Malaysia

Julio Ronceros Research and Development Laboratory in Emerging Technologies, Universidad Peruana de Ciencias Aplicadas, Lima, Peru

Mohammed Sabiri Faculty of Science and Technology, Moulay Ismail University of Meknes, Errachidia, Morocco

V. C. Sai Santhosh Chennai, Tamilnadu, India

Takayoshi Sakurai Nagoya Institute of Technology, Nagoya, Aichi, Japan

Jorge Salazar The University of Oklahoma, Norman, OK, USA

Domenico Santaniello DiSPaC, University of Salerno, Fisciano, SA, Italy

Alfonso Santoriello DiSPAC, University of Salerno, Fisciano, SA, Italy

Fabián Santos Centro de Investigación para el Territorio y el Hábitat Sostenible (CITEHS), Universidad Indoamérica, Quito, Ecuador

Judhi Santoso School of Electrical Engineering and Informatics, Institut Teknologi Bandung, Bandung, Indonesia

Haryadi Sarjono BINUS University, Jakarta, Indonesia;
BINUS University, Jakarta, Indonesia

Khalil H. Sayidmarie Department of Communication Engineering, College of Electronics Engineering, Ninevah University, Mosul, Iraq;
College of Engineering, AUK, Duhok, Iraq

Neo Segoete University of Witwatersrand, Braamfontein, Johannesburg, South Africa

Reda Owis Hassan Serour Universiti Islam Antarabangsa Sultan Abdul Halim Mu'adzam Shah, Kuala Ketil, Malaysia

Hiromitsu Shimakawa Ritsumeikan University, Kusatsu-shi, Shiga-ken, Japan

Shun Shiramatsu Nagoya Institute of Technology, Nagoya, Aichi, Japan

Abdulrahman Siddiq Blackburn College, Blackburn, UK

Ine Silviya BINUS University, Jakarta, Indonesia

Azwel Simwinga University of Zambia (UNZA), Lusaka, Zambia;
University of Zambia (UNZA), Lusaka, Zambia

Maragustam Siregar Universitas Islam Negeri Sunan Kalijaga, Yogyakarta, Indonesia

Mohammad Raihan Soleiman BINUS University, Jakarta, Indonesia

François Spies University of Franche Comte (UFC), Montbeliard, France

Fernanda Suárez Centro de Investigación para el Territorio y el Hábitat Sostenible (CITEHS), Universidad Indoamérica, Quito, Ecuador

Gerald Sugi BINUS University, Jakarta, Indonesia

Kridanto Surendro School of Electrical Engineering and Informatics, Institut Teknologi Bandung, Bandung, Indonesia

Ramyar A. Teimoor IT Department, Kurdistan Technical Institute, Sulaymaniyah, Iraq

Tofiq A. Tofiq Computer Department, College of Science, University of Sulaimani-Sulaymaniyah, Sulaymaniyah, Iraq

Farshad Ghassemi Toosi Computer Science Department at Munster Technological University, Cork, Ireland

Agung Trisetyarso School of Computer Science, Department of Mathematics, Bina Nusantara University, Jakarta, Indonesia

Carlos Silvestre Herrera Trujillo Research and Development Laboratory in Emerging Technologies, Universidad Peruana de Ciencias Aplicadas, Lima, Peru

Adriana Margarita Turriate-Guzmán Universidad Privada del Norte, Lima, Peru

Mohammad Kamal Uddin University of Chittagong, Chittagong, Bangladesh

Kohei Urayama Ritsumeikan University, Kusatsu-shi, Shiga-ken, Japan

Carmine Valentino DIIn, University of Salerno, Fisciano, SA, Italy

Wilbert Villalobos Department of Computer Science and Technology, Kean University, Union, NJ, USA

Francois Volschenk University of Johannesburg, Johannesburg, South Africa

Azhar Wahid Faculty of Languages and Communications, Universiti Pendidikan Sultan Idris Tanjong Malim, Tanjong Malim, Malaysia

Fangya Xu University of Reading, Reading, UK

Heppy Yohanes Teology Bethel the Way Institute, Jakarta, Indonesia

Lenny Putri Yulianti School of Electrical Engineering and Informatics, Institut Teknologi Bandung, Bandung, Indonesia

Farahwahida Mohd Yusof Centre of Research for Fiqh Science and Technology (CFiRST), Ibnu Sina Institute for Scientific and Industrial Research (ISI-ISIR), Universiti Teknologi Malaysia (UTM), Skudai, Malaysia

Gianpierre Zapata Research and Development Laboratory in Emerging Technologies, Universidad Peruana de Ciencias Aplicadas, Lima, Peru

A Review on Image Steganography

Bana Shekh Faraj and Abdulrahman Siddiq

Abstract This paper is concerned with an important aspect of data security, known as steganography. In steganography, a secret message is hidden into another data file such as image, video, audio, or text file. The advantage of steganography over cryptography is that the intended secret message does not attract attention to itself as an object of scrutiny. In this paper, the different steganography techniques and related security issues are reviewed. The main focus is made on the most widely used technique called the Least Significant Bit (LSB) approach. The details of the LSB algorithm are presented, and it is implemented by using a MATLAB code. Text data has been embedded into a cover image, after the embedding process the stego image is generated that seems to be the same as the original cover image with only slight changes that Human Visual System cannot detect.

Keywords Steganography · Cryptography · Watermarking · LSB steganography · Stego image

1 Introduction

The evolution of wireless communication has also launched new security problems specified for the wireless environment. Some of the existing security technologies are useful for particular problems, while for others new solution technologies in the security concept must be added in a sophisticated manner [1].

At the present time, the protection of data in order to make it confidential when transmitting it through a public medium is demanded. Mainly the data had been processed before being transmitted which would reform the data into a formation that is not readable. Only the authorized people could manage to reverse the formation and make it in the normal form so that they could read and understand the data. Cryptography is the science that deals with such techniques; nowadays, a different

B. S. Faraj (✉) · A. Siddiq
Blackburn College, Blackburn, UK
e-mail: bana.shekh@blackburn.ac.uk

X.-S. Yang et al. (eds.), *Proceedings of Ninth International Congress on Information and Communication Technology*, Lecture Notes in Networks and Systems 1004,
https://doi.org/10.1007/978-981-97-3305-7_1

technique is available to protect the data, which is steganography [2]. Steganography has come from the Greek word "Protected Writing" [3]. Steganography is the science of concealing information into a safe object in a way that is unnoticeable to an intruder. The safe object is known as the cover, and the hidden information is the payload; the cover can be in the form of text, images, audio, and video files. The most common cover type is the image because of the widespread use for this type of file in everyday life and its plenty of repetitions [4].

The rest of this paper is ordered as literature review that compares related work in terms of the used methodology in the second section. A methodology is to show the method of concealing information using a specific approach called Least Significant Bit (LSB) regarding image steganography technique in the third section. An implementation for the design of steganography is provided in the fourth section, a discussion on the resulted data from the implementation has been presented in the fifth section, the sixth section is a conclusion of the whole review paper, and finally, the references are cited.

2 Literature Review

In this section, related work regarding the methodology of using steganography is reviewed. Steganography includes different disciplines for hiding information such as image, video, audio, text, DNA, and protocol [5, 6]. In addition, two other techniques are commonly used for securing data transmission, which are cryptography and watermarking. Table 1 shows a comparison between the three techniques [7, 8].

Every steganography technique contains three main elements; a cover object, serves as a surface to transfer the original message, message object, which is the original message needs to be transmitted without been exposed, and resulting steganography object, which is the combination of the two first elements and it is the exposed object while being transmitting [9].

A popular technique for hiding secret information is the image steganography, because it can easily spread out through the World Wide Web or in newsgroups. The cover source that is in the format of image is altered in noisy areas with many color variations. So that the appearance of the overall cover is not affected so as not to attract attention. The common methods for achieving this type is the LSB, masking, filtering, and the transformations on the cover image [10, 11]. Other techniques regarding the image steganography had been studied, such as spatial domain, transform domain,

Table 1 Comparison between steganography, cryptography, and watermarking

Techniques	Purpose	Carrier
Steganography	Hiding data from intruders	Needs a carrier
Cryptography	Encrypting data to be unreadable format for intruders	Does not need a carrier
Watermarking	Protecting the content of the carrier (data)	Needs a carrier

and model-based steganography. While each technique evolves many different types for achieving the goal, among them is the LSB that is explained in the previous literature which is a branch of spatial domain steganography [12].

A different technique for image steganography had been proposed, which is the Mid Position Value (MPV). In the transmitter side the cover image is scrambled by applying Arnold Transformation, "Arnold scrambling algorithm is based on square digital image in most literature, and these images are mostly N × N pixels of the digital image" [13], resulting in a randomized cover image that is secure because the pixels of the image had changed their position before been embedded. After that, bits of the secret image had been inserted to the modified cover image, for this purpose the MPV had been integrated, using the idea of middle position and its respective values for the existing pixels, additionally, basing the other pixels on the ground level, the computation of key values was gained. Last but not least, a specific insertion method had been considered, so that to embed the private bits.

For getting back the original stego image, Inverse Arnold Transformation had to be executed. Furthermore, in the receiver side, the same steps, as in the transmitter, would lead to retrieve the secret image [14].

Another method for embedding and extracting data rather than MPV had been proposed, which was Overlapping of Three Pixel Block of Image. The embedding process was executed by passing through the image in a raster scan arrangement, splitting the image into blocks of a sequential size of three pixels, after that mathematical explanations for the two processes had been presented for further explaining the method, the result of the technique showed quite small difference between the cover image and the modified cover image; thus, secure steganographic with a high capacity method was achieved throughout the study [2].

Another paper presents the use of LSB in image steganography, mentioning the weakness of this method for being vulnerable to attack due to its simplicity; therefore, the paper suggests adding a stego key for overcoming the issue.

A 24-bit color image is used as the cover to embed the secret image, a color combination of Red, Green, Blue (RGB) components, each pixel of the image contains 24-bitmap values for each of the three colors represented as bits; thus, a wide variety of colors can be achieved in this whole process can be achieved by LSB. Though embedding the secret image changes the color's intensity, it does not make a noticeable change in the carrier/cover image because of its huge size besides, human eyes cannot notice the small modifications of the pixels' intensity.

As stated earlier for overcoming the weakness of this method, a stego key must be added and encrypted into the carrier image. A password can be seen as an example for stego key, and it is also another secret information in the cover image [15].

Text steganography is another form of hiding information. Here, words have been selected based on how frequent they are used in everyday life and their popularity in social medias such as Facebook, WhatsApp, Hike, and Yahoo messenger. For instance, the word see is replaced by the letter C and you by U. this technique can manage to hide a large amount of data but it is a time consuming process [16]. A design of coding methods was proposed for the purpose of developing alterations that can be decoded reliably and in the same time highly unnoticeable to the reader, even

noise would not affect the designed method, the method is to alter text formatting or altering specific characteristics of textual elements known as text steganography.

The conflicting of being both reliable decoding and minimum visible changes makes the challenges to design document marking techniques. The format of a document file describes the content and page layout of a computer file, standard languages were used for the format description such as PostScript2, Tex, and @off, and the image viewed to the reader was generated from this format file. Three techniques had been used for this method, Line-Shift Coding, Word-Shift Coding, and Feature Coding [10].

Audio steganography conceals information in which a basic model for such type includes a carrier, cover file, to hide the secret information. A message contains the secret information that needs to be transmitted confidentially and a password/stego key to ensure the receiving of secret information to the authorized recipient The following techniques had been utilized for the method, LSB, parity coding, phase coding, spread spectrum, and echo hiding [17, 18].

A technique named substitution was used regarding audio steganography. It replaces either a bit or a few bits in the cover file that makes unnoticeable changes to human ear depending on the type of file. The technique has a high embedding capacity (41,000 bps); however, it is considered as the least robust against attacks attempting to reveal the secret information nevertheless, against distortion with high average power. Two solutions had been proposed to fix the problems. For the first problem, making discovering of which bits are embedded difficult through modifying other bits rather than the LSB, as in usual cases, additionally, selecting the samples for modification private not modifying all of the samples. Regarding the second problem, embedding the bits of the message in deeper layers and altering the other bits to decrease the amount of error [19].

In spite of the many techniques used for hiding information, in this review video steganography is provided as the final technique. It is a technique that is hiding secret messages into a video; here the video acts as the cover file, and it has become more popular nowadays because the security issue is becoming much more serious with the evolution of computer applications. Additionally, video is an electronic medium considered to be a powerful tool recently for sharing digital video contents and its size. The regarding algorithm can be divided into three categories in the terms of their embedding position, video steganography technique based on intra-embedding, pre-embedding, and post-embedding [20].

An effective method for hiding secret data into a video has been demonstrated. A video file is normally composed of several frames, in this method some of the frames (or images) were used for the hiding process. The secret data is hidden in random frames, using index helps to identify the frames containing the secret data referred to as index frames. The remaining frames are also going to the same process of steganography in order to provide further security to the data. The process can be managed through three steps sequentially which are analyzing the video, determining the index frame with its data, and determining frames for secret data [21].

3 LSB Steganography

A simple and common approach for embedding data in a cover file is the LSB substitution. Since the cover file for this type is an image, which contains RGB components, the pixel information is stored in encoded format in one byte. The first bit regarding each pixel can be modified in order to store the secret data. For this purpose, the preliminary condition must be applied, which states that in order to store a text in an image, the text size must be smaller or equal to the image size so that the image can hide the text.

LSB is a spatial domain method, making the secret data exposed to cropping and noise. In this method, the Most Significant Bit (MSB) of the secret message image is stored in the LSB of the cover image.

The pixels of an image are stored in the form of bits. In a grayscale image, the intensity of each pixel is stored in 8 bits (i.e., 1 byte), similarly, for color image (RGB) each pixel requires 24 bits (i.e., 3 bytes), 8 bits for each layer. When the LSB of an image is modified, the Human Visual System (HVS) cannot detect the modification regarding the color or intensity of a pixel. This has been taken as an advantage to store and hide information using the method, as the hidden information can be stored in the stated bit [9].

3.1 Steps Taken in LSB Steganography

At the sender in order to hide an image message into a cover image, the following steps must be taken:

1. Selecting a cover image with addition of noise for making the process of disguise easier.
2. Selecting the image message that needs to be hid.
3. Separating the bit planes for each of the images.

LSB has the least information regarding the image, while the MSB mostly contains the shape and color of the image. The ideal case for the separation step is to replace up to four bitplanes in regards to the cover image with the 4.

LSB of the message image results in a steganographic image pixel that does not reveal any change compared to the original message. Less number of bitplanes by the message image can be used but resulting in a distorted and loss of information in the corresponding image, further cleared by Fig. 1.

4. Replacing the 4 least bitplanes of the cover image by the 4 most bitplanes of the message image.
5. Combining the bitplanes results in the steganographic image. In the receiver sider to retrieve the hidden message image:

1. Getting the steganographic image.

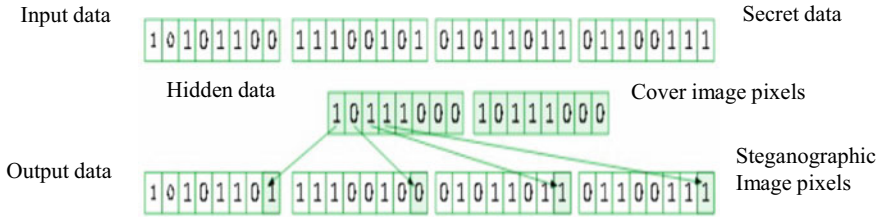

Fig. 1 LSB in image steganography

2. Extracting the amount of bitplanes of the image as needed.
3. Reversing the process by recombining the 4 least bit planes in order to retrieve the message image [9].

3.2 Implementation and Result

MATLAB program was used to carry out the result. A black and white image was chosen to be the cover image, as shown in Fig. 2a, the message to be hidden is (Communication Network Security). Figure 2 (b) shows the embedded message within the image. It is clear that human beings are unable to recognize the message because from the appearance only the size of the image is changed.

Detection of the hidden message/data can be through comparing the stego to the cover file, and detecting files of larger sizes and/or variations in statistical properties is most probably the file contains the hidden data. Analyzing the distribution of known characteristics often reveals the hidden message.

4 Steganalysis

Steganalysis is the study of detecting steganography and decoding the stego-message to regenerate the hidden message. Steganalysis is the integration of steganography similar to cryptography and cryptanalysis. According to knowing the actual message, the cover file, and the steganography algorithm, steganalysis can be divided into six parts (Table 2).

4.1 The Detection Processes

Detection of the hidden message/data can be through comparing the stego to the cover file, detecting files of larger sizes and/or variations in statistical properties is

(a) cover image

(b) the stego image

Fig. 2 LSB method for a black and white image

Table 2 Steganalysis types

Steganalysis types	Hidden message	Cover-file	Algorithm	Stego file
Stego only attack	Unknown	Unknown	Unknown	Known
Known cover attack	Unknown	Known	Unknown	Known
Known message attack	Known	Unknown	Unknown	Unknown
Chosen stego attack	Unknown	Unknown	Known	Known
Known stego attack	Known	Known	Known	Known

most probably the file contains the hidden data. Analyzing distribution of known characteristics often reveals the hidden message.

Furthermore, detecting and deciphering the original message are complicated, and it faces many challenges since it can be destroyed before reaching the destination. For instance, an image file that might be used as a cover for the original message can be altered in terms of changing file format, compression algorithms, and levels, while there would be no visible impact on the file image [8].

5 Discussion

The cover image has chosen to be black and white because it provides the clarity of the method in an easy way. It is clear that the resulted stego image is slightly changed to the original image in a way that HVS cannot detect the changes. This is because a greyscale or black and white image is a monochrome (one-color) image, just the brightness of the image changes. The level of the brightness is altered from 0 to 255 levels, since each pixel contains 8 bits that allow such levels of representation [22]. If the LSB for example 0 is black, converting it to 1 only makes it a little brighter. However, the size of the image has been changed due to the requirements of the MATLAB code program. Also, the input image was in the form of JFIF (JPEG File Interchange Format), while the program deals with other formats of images such as png and jpg; therefore, the image has been converted to png format. Furthermore, there are some factors that must be achieved throughout steganography to determine the effectiveness of each steganography technique. Such as the following;

Robustness defines the ability of a technique to remain the hidden data safe even if the stego file (i.e., stego image) endures modifications.

Imperceptibility refers to the invisibility of a steganography algorithm, which determines the strength of steganography. And it is considered as the main requirement in order to transmit data without being noticed to human eyes.

Bit Error Rate (BER) is the ratio of the error bits to the total number of bits sent over a communication channel. In order to recover a hidden data, this ratio must be in a very low amount.

Mean Square Error (MSE): computation is obtained by comparing byte by byte of the cover file to the generated stego file. It can be used to measure distortion.

Peak Signal-to-Noise Ratio (PSNR) is the ratio of maximum signal to noise corresponding to the stego file. It can be used as a measure of image quality. The higher the PSNR the less the distortion thus better quality image [23].