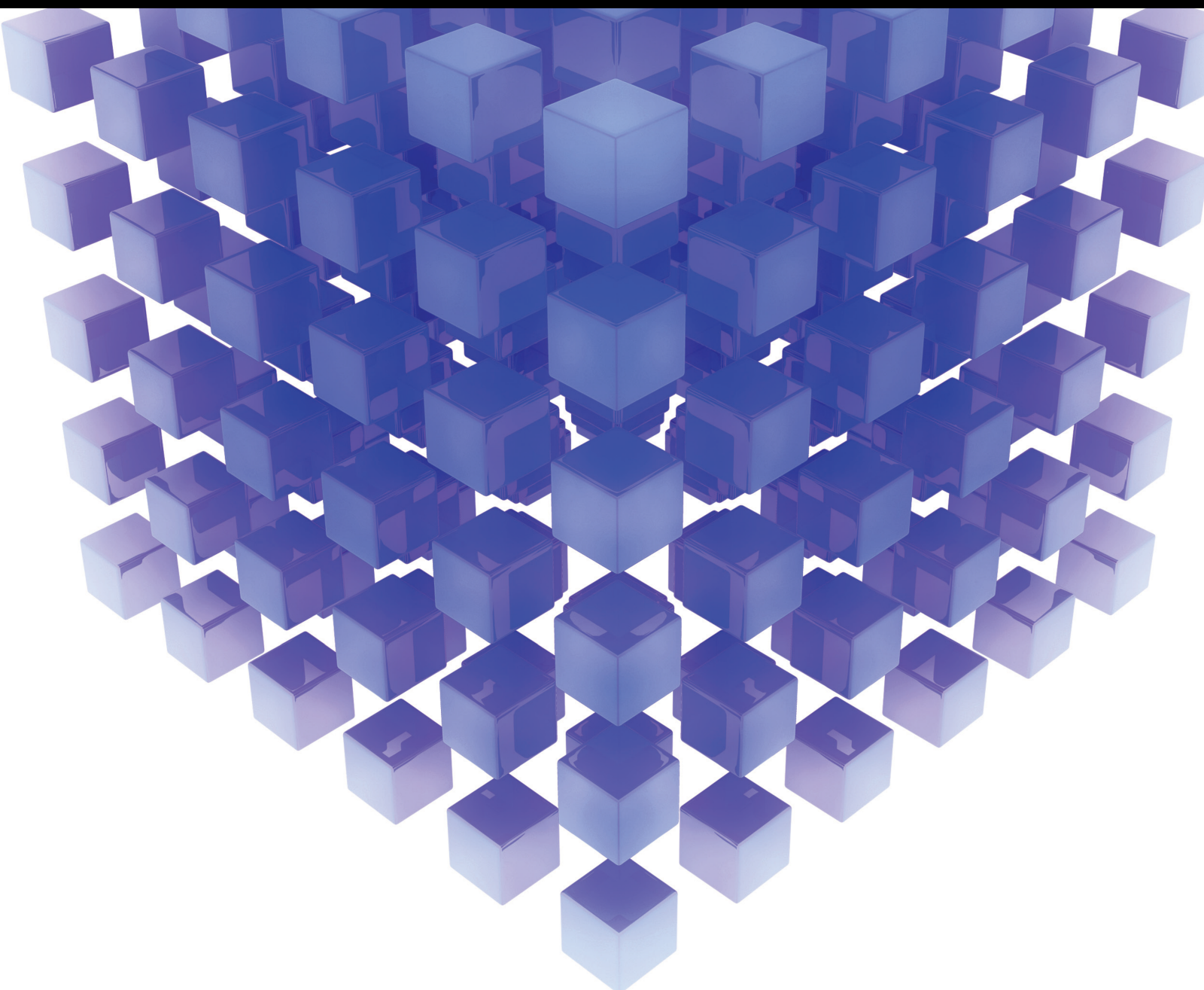


# Internet of Things and Big Data Analytics for a Green Environment

Lead Guest Editor: Yousef Farhaoui

Guest Editors: Badraddine Aghoutane, Mohammed Fattah, and Bharat Bhushan





---

# **Internet of Things and Big Data Analytics for a Green Environment**

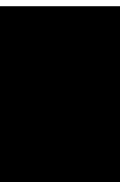
Mathematical Problems in Engineering

---

**Internet of Things and Big Data  
Analytics for a Green Environment**

Lead Guest Editor: Yousef Farhaoui

Guest Editors: Badraddine Aghoutane, Mohammed  
Fattah, and Bharat Bhushan




---

Copyright © 2021 Hindawi Limited. All rights reserved.

This is a special issue published in “Mathematical Problems in Engineering.” All articles are open access articles distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.




# Chief Editor

Guangming Xie , China

## Academic Editors

Kumaravel A , India  
Waqas Abbasi, Pakistan  
Mohamed Abd El Aziz , Egypt  
Mahmoud Abdel-Aty , Egypt  
Mohammed S. Abdo, Yemen  
Mohammad Yaghoub Abdollahzadeh  
Jamalabadi , Republic of Korea  
Rahib Abiyev , Turkey  
Leonardo Acho , Spain  
Daniela Adnessi , Italy  
Arooj Adeel , Pakistan  
Waleed Adel , Egypt  
Ramesh Agarwal , USA  
Francesco Aggogeri , Italy  
Ricardo Aguilar-Lopez , Mexico  
Afaq Ahmad , Pakistan  
Naveed Ahmed , Pakistan  
Elias Aifantis , USA  
Akif Akgul , Turkey  
Tareq Al-shami , Yemen  
Guido Ala, Italy  
Andrea Alaimo , Italy  
Reza Alam, USA  
Osamah Albahri , Malaysia  
Nicholas Alexander , United Kingdom  
Salvatore Alfonzetti, Italy  
Ghous Ali , Pakistan  
Nouman Ali , Pakistan  
Mohammad D. Aliyu , Canada  
Juan A. Almendral , Spain  
A.K. Alomari, Jordan  
José Domingo Álvarez , Spain  
Cláudio Alves , Portugal  
Juan P. Amezcua-Sanchez, Mexico  
Mukherjee Amitava, India  
Lionel Amodeo, France  
Sebastian Anita, Romania  
Costanza Arico , Italy  
Sabri Arik, Turkey  
Fausto Arpino , Italy  
Rashad Asharabi , Saudi Arabia  
Farhad Aslani , Australia  
Mohsen Asle Zaem , USA

Andrea Avanzini , Italy  
Richard I. Avery , USA  
Viktor Avrutin , Germany  
Mohammed A. Awadallah , Malaysia  
Francesco Aymerich , Italy  
Sajad Azizi , Belgium  
Michele Baccocchi , Italy  
Seungik Baek , USA  
Khaled Bahlali, France  
M.V.A Raju Bahubalendruni, India  
Pedro Balaguer , Spain  
P. Balasubramaniam, India  
Stefan Balint , Romania  
Ines Tejado Balsera , Spain  
Alfonso Banos , Spain  
Jerzy Baranowski , Poland  
Tudor Barbu , Romania  
Andrzej Bartoszewicz , Poland  
Sergio Baselga , Spain  
S. Caglar Baslamisli , Turkey  
David Bassir , France  
Chiara Bedon , Italy  
Azeddine Beghdadi, France  
Andriette Bekker , South Africa  
Francisco Beltran-Carbajal , Mexico  
Abdellatif Ben Makhlof , Saudi Arabia  
Denis Benasciutti , Italy  
Ivano Benedetti , Italy  
Rosa M. Benito , Spain  
Elena Benvenuti , Italy  
Giovanni Berselli, Italy  
Michele Betti , Italy  
Pietro Bia , Italy  
Carlo Bianca , France  
Simone Bianco , Italy  
Vincenzo Bianco, Italy  
Vittorio Bianco, Italy  
David Bigaud , France  
Sardar Muhammad Bilal , Pakistan  
Antonio Bilotta , Italy  
Sylvio R. Bistafa, Brazil  
Chiara Boccaletti , Italy  
Rodolfo Bontempo , Italy  
Alberto Borboni , Italy  
Marco Bortolini, Italy

Paolo Boscariol, Italy  
Daniela Boso , Italy  
Guillermo Botella-Juan, Spain  
Abdesselem Boulkroune , Algeria  
Boulaïd Boulkroune, Belgium  
Fabio Bovenga , Italy  
Francesco Braghin , Italy  
Ricardo Branco, Portugal  
Julien Bruchon , France  
Matteo Bruggi , Italy  
Michele Brun , Italy  
Maria Elena Bruni, Italy  
Maria Angela Butturi , Italy  
Bartłomiej Błachowski , Poland  
Dhanamjayulu C , India  
Raquel Caballero-Águila , Spain  
Filippo Cacace , Italy  
Salvatore Caddemi , Italy  
Zuowei Cai , China  
Roberto Caldelli , Italy  
Francesco Cannizzaro , Italy  
Maosen Cao , China  
Ana Carpio, Spain  
Rodrigo Carvajal , Chile  
Caterina Casavola, Italy  
Sara Casciati, Italy  
Federica Caselli , Italy  
Carmen Castillo , Spain  
Inmaculada T. Castro , Spain  
Miguel Castro , Portugal  
Giuseppe Catalanotti , United Kingdom  
Alberto Cavallo , Italy  
Gabriele Cazzulani , Italy  
Fatih Vehbi Celebi, Turkey  
Miguel Cerrolaza , Venezuela  
Gregory Chagnon , France  
Ching-Ter Chang , Taiwan  
Kuei-Lun Chang , Taiwan  
Qing Chang , USA  
Xiaoheng Chang , China  
Prasenjit Chatterjee , Lithuania  
Kacem Chehdi, France  
Peter N. Cheimets, USA  
Chih-Chiang Chen , Taiwan  
He Chen , China

Kebing Chen , China  
Mengxin Chen , China  
Shyi-Ming Chen , Taiwan  
Xizhong Chen , Ireland  
Xue-Bo Chen , China  
Zhiwen Chen , China  
Qiang Cheng, USA  
Zeyang Cheng, China  
Luca Chiapponi , Italy  
Francisco Chicano , Spain  
Tirivanhu Chinyoka , South Africa  
Adrian Chmielewski , Poland  
Seongim Choi , USA  
Gautam Choubey , India  
Hung-Yuan Chung , Taiwan  
Yusheng Ci, China  
Simone Cinquemani , Italy  
Roberto G. Citarella , Italy  
Joaquim Ciurana , Spain  
John D. Clayton , USA  
Piero Colajanni , Italy  
Giuseppina Colicchio, Italy  
Vassilios Constantoudis , Greece  
Enrico Conte, Italy  
Alessandro Contento , USA  
Mario Cools , Belgium  
Gino Cortellessa, Italy  
Carlo Cosentino , Italy  
Paolo Crippa , Italy  
Erik Cuevas , Mexico  
Guozeng Cui , China  
Mehmet Cunkas , Turkey  
Giuseppe D'Aniello , Italy  
Peter Dabnichki, Australia  
Weizhong Dai , USA  
Zhifeng Dai , China  
Purushothaman Damodaran , USA  
Sergey Dashkovskiy, Germany  
Adiel T. De Almeida-Filho , Brazil  
Fabio De Angelis , Italy  
Samuele De Bartolo , Italy  
Stefano De Miranda , Italy  
Filippo De Monte , Italy

José António Fonseca De Oliveira  
Correia , Portugal  
Jose Renato De Sousa , Brazil  
Michael Defoort, France  
Alessandro Della Corte, Italy  
Laurent Dewasme , Belgium  
Sanku Dey , India  
Gianpaolo Di Bona , Italy  
Roberta Di Pace , Italy  
Francesca Di Puccio , Italy  
Ramón I. Diego , Spain  
Yannis Dimakopoulos , Greece  
Hasan Dinçer , Turkey  
José M. Domínguez , Spain  
Georgios Dounias, Greece  
Bo Du , China  
Emil Dumic, Croatia  
Madalina Dumitriu , United Kingdom  
Premraj Durairaj , India  
Saeed Eftekhari Azam, USA  
Said El Kafhali , Morocco  
Antonio Elipse , Spain  
R. Emre Erkmen, Canada  
John Escobar , Colombia  
Leandro F. F. Miguel , Brazil  
FRANCESCO FOTI , Italy  
Andrea L. Facci , Italy  
Shahla Faisal , Pakistan  
Giovanni Falsone , Italy  
Hua Fan, China  
Jianguang Fang, Australia  
Nicholas Fantuzzi , Italy  
Muhammad Shahid Farid , Pakistan  
Hamed Faruqi, Iran  
Yann Favennec, France  
Fiorenzo A. Fazzolari , United Kingdom  
Giuseppe Fedele , Italy  
Roberto Fedele , Italy  
Baowei Feng , China  
Mohammad Ferdows , Bangladesh  
Arturo J. Fernández , Spain  
Jesus M. Fernandez Oro, Spain  
Francesco Ferrise, Italy  
Eric Feulvarch , France  
Thierry Floquet, France

Eric Florentin , France  
Gerardo Flores, Mexico  
Antonio Forcina , Italy  
Alessandro Formisano, Italy  
Francesco Franco , Italy  
Elisa Francomano , Italy  
Juan Frausto-Solis, Mexico  
Shujun Fu , China  
Juan C. G. Prada , Spain  
HECTOR GOMEZ , Chile  
Matteo Gaeta , Italy  
Mauro Gaggero , Italy  
Zoran Gajic , USA  
Jaime Gallardo-Alvarado , Mexico  
Mosè Gallo , Italy  
Akemi Gálvez , Spain  
Maria L. Gandarias , Spain  
Hao Gao , Hong Kong  
Xingbao Gao , China  
Yan Gao , China  
Zhiwei Gao , United Kingdom  
Giovanni Garcea , Italy  
José García , Chile  
Harish Garg , India  
Alessandro Gasparetto , Italy  
Stylianos Georgantzinou, Greece  
Fotios Georgiades , India  
Parviz Ghadimi , Iran  
Ştefan Cristian Gherghina , Romania  
Georgios I. Giannopoulos , Greece  
Agathoklis Giaralis , United Kingdom  
Anna M. Gil-Lafuente , Spain  
Ivan Giorgio , Italy  
Gaetano Giunta , Luxembourg  
Jefferson L.M.A. Gomes , United Kingdom  
Emilio Gómez-Déniz , Spain  
Antonio M. Gonçalves de Lima , Brazil  
Qunxi Gong , China  
Chris Goodrich, USA  
Rama S. R. Gorla, USA  
Veena Goswami , India  
Xunjie Gou , Spain  
Jakub Grabski , Poland

Antoine Grall , France  
George A. Gravvanis , Greece  
Fabrizio Greco , Italy  
David Greiner , Spain  
Jason Gu , Canada  
Federico Guarracino , Italy  
Michele Guida , Italy  
Muhammet Gul , Turkey  
Dong-Sheng Guo , China  
Hu Guo , China  
Zhaoxia Guo, China  
Yusuf Gurefe, Turkey  
Salim HEDDAM , Algeria  
ABID HUSSANAN, China  
Quang Phuc Ha, Australia  
Li Haitao , China  
Petr Hájek , Czech Republic  
Mohamed Hamdy , Egypt  
Muhammad Hamid , United Kingdom  
Renke Han , United Kingdom  
Weimin Han , USA  
Xingsi Han, China  
Zhen-Lai Han , China  
Thomas Hanne , Switzerland  
Xinan Hao , China  
Mohammad A. Hariri-Ardebili , USA  
Khalid Hattaf , Morocco  
Defeng He , China  
Xiao-Qiao He, China  
Yanchao He, China  
Yu-Ling He , China  
Ramdane Hedjar , Saudi Arabia  
Jude Hemanth , India  
Reza Hemmati, Iran  
Nicolae Herisanu , Romania  
Alfredo G. Hernández-Díaz , Spain  
M.I. Herreros , Spain  
Eckhard Hitzer , Japan  
Paul Honeine , France  
Jaromir Horacek , Czech Republic  
Lei Hou , China  
Yingkun Hou , China  
Yu-Chen Hu , Taiwan  
Yunfeng Hu, China  
Can Huang , China  
Gordon Huang , Canada  
Linsheng Huo , China  
Sajid Hussain, Canada  
Asier Ibeas , Spain  
Orest V. Iftime , The Netherlands  
Przemyslaw Ignaciuk , Poland  
Giacomo Innocenti , Italy  
Emilio Insfran Pelozo , Spain  
Azeem Irshad, Pakistan  
Alessio Ishizaka, France  
Benjamin Ivorra , Spain  
Breno Jacob , Brazil  
Reema Jain , India  
Tushar Jain , India  
Amin Jajarmi , Iran  
Chiranjibe Jana , India  
Łukasz Jankowski , Poland  
Samuel N. Jator , USA  
Juan Carlos Jáuregui-Correa , Mexico  
Kandasamy Jayakrishna, India  
Reza Jazar, Australia  
Khalide Jbilou, France  
Isabel S. Jesus , Portugal  
Chao Ji , China  
Qing-Chao Jiang , China  
Peng-fei Jiao , China  
Ricardo Fabricio Escobar Jiménez , Mexico  
Emilio Jiménez Macías , Spain  
Maolin Jin, Republic of Korea  
Zhuo Jin, Australia  
Ramash Kumar K , India  
BHABEN KALITA , USA  
MOHAMMAD REZA KHEDMATI , Iran  
Viacheslav Kalashnikov , Mexico  
Mathiyalagan Kalidass , India  
Tamas Kalmar-Nagy , Hungary  
Rajesh Kaluri , India  
Jyottheswara Reddy Kalvakurthi, India  
Zhao Kang , China  
Ramani Kannan , Malaysia  
Tomasz Kapitaniak , Poland  
Julius Kaplunov, United Kingdom  
Konstantinos Karamanos, Belgium  
Michal Kawulok, Poland

Irfan Kaymaz , Turkey  
Vahid Kayvanfar , Qatar  
Krzysztof Kecik , Poland  
Mohamed Khader , Egypt  
Chaudry M. Khalique , South Africa  
Mukhtaj Khan , Pakistan  
Shahid Khan , Pakistan  
Nam-Il Kim, Republic of Korea  
Philipp V. Kiryukhantsev-Korneev ,  
Russia  
P.V.V Kishore , India  
Jan Koci , Czech Republic  
Ioannis Kostavelis , Greece  
Sotiris B. Kotsiantis , Greece  
Frederic Kratz , France  
Vamsi Krishna , India  
Edyta Kucharska, Poland  
Krzysztof S. Kulpa , Poland  
Kamal Kumar, India  
Prof. Ashwani Kumar , India  
Michal Kunicki , Poland  
Cedrick A. K. Kwuimy , USA  
Kyandoghere Kyamakya, Austria  
Ivan Kyrchei , Ukraine  
Márcio J. Lacerda , Brazil  
Eduardo Lalla , The Netherlands  
Giovanni Lancioni , Italy  
Jaroslaw Latalski , Poland  
Hervé Laurent , France  
Agostino Lauria , Italy  
Aimé Lay-Ekuakille , Italy  
Nicolas J. Leconte , France  
Kun-Chou Lee , Taiwan  
Dimitri Lefebvre , France  
Eric Lefevre , France  
Marek Lefik, Poland  
Yaguo Lei , China  
Kauko Leiviskä , Finland  
Ervin Lenzi , Brazil  
ChenFeng Li , China  
Jian Li , USA  
Jun Li , China  
Yueyang Li , China  
Zhao Li , China

Zhen Li , China  
En-Qiang Lin, USA  
Jian Lin , China  
Qibin Lin, China  
Yao-Jin Lin, China  
Zhiyun Lin , China  
Bin Liu , China  
Bo Liu , China  
Heng Liu , China  
Jianxu Liu , Thailand  
Lei Liu , China  
Sixin Liu , China  
Wanquan Liu , China  
Yu Liu , China  
Yuanchang Liu , United Kingdom  
Bonifacio Llamazares , Spain  
Alessandro Lo Schiavo , Italy  
Jean Jacques Loiseau , France  
Francesco Lolli , Italy  
Paolo Lonetti , Italy  
António M. Lopes , Portugal  
Sebastian López, Spain  
Luis M. López-Ochoa , Spain  
Vassilios C. Loukopoulos, Greece  
Gabriele Maria Lozito , Italy  
Zhiguo Luo , China  
Gabriel Luque , Spain  
Valentin Lychagin, Norway  
YUE MEI, China  
Junwei Ma , China  
Xuanlong Ma , China  
Antonio Madeo , Italy  
Alessandro Magnani , Belgium  
Toqeer Mahmood , Pakistan  
Fazal M. Mahomed , South Africa  
Arunava Majumder , India  
Sarfranz Nawaz Malik, Pakistan  
Paolo Manfredi , Italy  
Adnan Maqsood , Pakistan  
Muazzam Maqsood, Pakistan  
Giuseppe Carlo Marano , Italy  
Damijan Markovic, France  
Filipe J. Marques , Portugal  
Luca Martinelli , Italy  
Denizar Cruz Martins, Brazil






























Francisco J. Martos , Spain  
Elio Masciari , Italy  
Paolo Massioni , France  
Alessandro Mauro , Italy  
Jonathan Mayo-Maldonado , Mexico  
Pier Luigi Mazzeo , Italy  
Laura Mazzola, Italy  
Driss Mehdi , France  
Zahid Mehmood , Pakistan  
Roderick Melnik , Canada  
Xiangyu Meng , USA  
Jose Merodio , Spain  
Alessio Merola , Italy  
Mahmoud Mesbah , Iran  
Luciano Mescia , Italy  
Laurent Mevel , France  
Constantine Michailides , Cyprus  
Mariusz Michta , Poland  
Prankul Middha, Norway  
Aki Mikkola , Finland  
Giovanni Minafò , Italy  
Edmondo Minisci , United Kingdom  
Hiroyuki Mino , Japan  
Dimitrios Mitsotakis , New Zealand  
Ardashir Mohammadzadeh , Iran  
Francisco J. Montáns , Spain  
Francesco Montefusco , Italy  
Gisele Mophou , France  
Rafael Morales , Spain  
Marco Morandini , Italy  
Javier Moreno-Valenzuela , Mexico  
Simone Morganti , Italy  
Caroline Mota , Brazil  
Aziz Moukrim , France  
Shen Mouquan , China  
Dimitris Mourtzis , Greece  
Emiliano Mucchi , Italy  
Taseer Muhammad, Saudi Arabia  
Ghulam Muhiuddin, Saudi Arabia  
Amitava Mukherjee , India  
Josefa Mula , Spain  
Jose J. Muñoz , Spain  
Giuseppe Muscolino, Italy  
Marco Mussetta , Italy

Hariharan Muthusamy, India  
Alessandro Naddeo , Italy  
Raj Nandkeolyar, India  
Keivan Navaie , United Kingdom  
Soumya Nayak, India  
Adrian Neagu , USA  
Erivelton Geraldo Nepomuceno , Brazil  
AMA Neves, Portugal  
Ha Quang Thinh Ngo , Vietnam  
Nhon Nguyen-Thanh, Singapore  
Papakostas Nikolaos , Ireland  
Jelena Nikolic , Serbia  
Tatsushi Nishi, Japan  
Shanzhou Niu , China  
Ben T. Nohara , Japan  
Mohammed Nouari , France  
Mustapha Nourelfath, Canada  
Kazem Nouri , Iran  
Ciro Núñez-Gutiérrez , Mexico  
Włodzimierz Ogryczak, Poland  
Roger Ohayon, France  
Krzysztof Okarma , Poland  
Mitsuhiro Okayasu, Japan  
Murat Olgun , Turkey  
Diego Oliva, Mexico  
Alberto Olivares , Spain  
Enrique Onieva , Spain  
Calogero Orlando , Italy  
Susana Ortega-Cisneros , Mexico  
Sergio Ortobelli, Italy  
Naohisa Otsuka , Japan  
Sid Ahmed Ould Ahmed Mahmoud , Saudi Arabia  
Taoreed Owolabi , Nigeria  
EUGENIA PETROPOULOU , Greece  
Arturo Pagano, Italy  
Madhumangal Pal, India  
Pasquale Palumbo , Italy  
Dragan Pamučar, Serbia  
Weifeng Pan , China  
Chandan Pandey, India  
Rui Pang, United Kingdom  
Jürgen Pannek , Germany  
Elena Panteley, France  
Achille Paolone, Italy

George A. Papakostas , Greece  
Xosé M. Pardo , Spain  
You-Jin Park, Taiwan  
Manuel Pastor, Spain  
Pubudu N. Pathirana , Australia  
Surajit Kumar Paul , India  
Luis Payá , Spain  
Igor Pažanin , Croatia  
Libor Pekař , Czech Republic  
Francesco Pellicano , Italy  
Marcello Pellicciari , Italy  
Jian Peng , China  
Mingshu Peng, China  
Xiang Peng , China  
Xindong Peng, China  
Yuexing Peng, China  
Marzio Pennisi , Italy  
Maria Patrizia Pera , Italy  
Matjaz Perc , Slovenia  
A. M. Bastos Pereira , Portugal  
Wesley Peres, Brazil  
F. Javier Pérez-Pinal , Mexico  
Michele Perrella, Italy  
Francesco Pesavento , Italy  
Francesco Petrini , Italy  
Hoang Vu Phan, Republic of Korea  
Lukasz Pieczonka , Poland  
Dario Piga , Switzerland  
Marco Pizzarelli , Italy  
Javier Plaza , Spain  
Goutam Pohit , India  
Dragan Poljak , Croatia  
Jorge Pomares , Spain  
Hiram Ponce , Mexico  
Sébastien Poncet , Canada  
Volodymyr Ponomaryov , Mexico  
Jean-Christophe Ponsart , France  
Mauro Pontani , Italy  
Sivakumar Poruran, India  
Francesc Pozo , Spain  
Aditya Rio Prabowo , Indonesia  
Anchasa Pramuanjaroenkij , Thailand  
Leonardo Primavera , Italy  
B Rajanarayan Prusty, India

Krzysztof Puszynski , Poland  
Chuan Qin , China  
Dongdong Qin, China  
Jianlong Qiu , China  
Giuseppe Quaranta , Italy  
DR. RITU RAJ , India  
Vitomir Racic , Italy  
Carlo Rainieri , Italy  
Kumbakonam Ramamani Rajagopal, USA  
Ali Ramazani , USA  
Angel Manuel Ramos , Spain  
Higinio Ramos , Spain  
Muhammad Afzal Rana , Pakistan  
Muhammad Rashid, Saudi Arabia  
Manoj Rastogi, India  
Alessandro Rasulo , Italy  
S.S. Ravindran , USA  
Abdolrahman Razani , Iran  
Alessandro Reali , Italy  
Jose A. Reinoso , Spain  
Oscar Reinoso , Spain  
Haijun Ren , China  
Carlo Renno , Italy  
Fabrizio Renno , Italy  
Shahram Rezapour , Iran  
Ricardo Rianza , Spain  
Francesco Riganti-Fulginei , Italy  
Gerasimos Rigatos , Greece  
Francesco Ripamonti , Italy  
Jorge Rivera , Mexico  
Eugenio Roanes-Lozano , Spain  
Ana Maria A. C. Rocha , Portugal  
Luigi Rodino , Italy  
Francisco Rodríguez , Spain  
Rosana Rodríguez López, Spain  
Francisco Rossomando , Argentina  
Jose de Jesus Rubio , Mexico  
Weiguo Rui , China  
Rubén Ruiz , Spain  
Ivan D. Rukhlenko , Australia  
Dr. Eswaramoorthi S. , India  
Weichao SHI , United Kingdom  
Chaman Lal Sabharwal , USA  
Andrés Sáez , Spain



Bekir Sahin, Turkey  
Laxminarayan Sahoo , India  
John S. Sakellariou , Greece  
Michael Sakellariou , Greece  
Salvatore Salamone, USA  
Jose Vicente Salcedo , Spain  
Alejandro Salcido , Mexico  
Alejandro Salcido, Mexico  
Nunzio Salerno , Italy  
Rohit Salgotra , India  
Miguel A. Salido , Spain  
Sinan Salih , Iraq  
Alessandro Salvini , Italy  
Abdus Samad , India  
Sovan Samanta, India  
Nikolaos Samaras , Greece  
Ramon Sancibrian , Spain  
Giuseppe Sanfilippo , Italy  
Omar-Jacobo Santos, Mexico  
J Santos-Reyes , Mexico  
José A. Sanz-Herrera , Spain  
Musavarah Sarwar, Pakistan  
Shahzad Sarwar, Saudi Arabia  
Marcelo A. Savi , Brazil  
Andrey V. Savkin, Australia  
Tadeusz Sawik , Poland  
Roberta Sburlati, Italy  
Gustavo Scaglia , Argentina  
Thomas Schuster , Germany  
Hamid M. Sedighi , Iran  
Mijanur Rahaman Seikh, India  
Tapan Senapati , China  
Lotfi Senhadji , France  
Junwon Seo, USA  
Michele Serpilli, Italy  
Silvestar Šesnić , Croatia  
Gerardo Severino, Italy  
Ruben Sevilla , United Kingdom  
Stefano Sfarra , Italy  
Dr. Ismail Shah , Pakistan  
Leonid Shaikhet , Israel  
Vimal Shanmuganathan , India  
Prayas Sharma, India  
Bo Shen , Germany  
Hang Shen, China

Xin Pu Shen, China  
Dimitri O. Shepelsky, Ukraine  
Jian Shi , China  
Amin Shokrollahi, Australia  
Suzanne M. Shontz , USA  
Babak Shotorban , USA  
Zhan Shu , Canada  
Angelo Sifaleras , Greece  
Nuno Simões , Portugal  
Mehakpreet Singh , Ireland  
Piyush Pratap Singh , India  
Rajiv Singh, India  
Seralathan Sivamani , India  
S. Sivasankaran , Malaysia  
Christos H. Skiadas, Greece  
Konstantina Skouri , Greece  
Neale R. Smith , Mexico  
Bogdan Smolka, Poland  
Delfim Soares Jr. , Brazil  
Alba Sofi , Italy  
Francesco Soldovieri , Italy  
Raffaele Solimene , Italy  
Yang Song , Norway  
Jussi Sopanen , Finland  
Marco Spadini , Italy  
Paolo Spagnolo , Italy  
Ruben Specogna , Italy  
Vasilios Spitas , Greece  
Ivanka Stamova , USA  
Rafał Stanisławski , Poland  
Miladin Stefanović , Serbia  
Salvatore Strano , Italy  
Yakov Strelniker, Israel  
Kangkang Sun , China  
Qiuqin Sun , China  
Shuaishuai Sun, Australia  
Yanchao Sun , China  
Zong-Yao Sun , China  
Kumarasamy Suresh , India  
Sergey A. Suslov , Australia  
D.L. Suthar, Ethiopia  
D.L. Suthar , Ethiopia  
Andrzej Swierniak, Poland  
Andras Szekrenyes , Hungary  
Kumar K. Tamma, USA



Yong (Aaron) Tan, United Kingdom  
Marco Antonio Taneco-Hernández , Mexico  
Lu Tang , China  
Tianyou Tao, China  
Hafez Tari , USA  
Alessandro Tasora , Italy  
Sergio Teggi , Italy  
Adriana del Carmen Téllez-Anguiano , Mexico  
Ana C. Teodoro , Portugal  
Efstathios E. Theotokoglou , Greece  
Jing-Feng Tian, China  
Alexander Timokha , Norway  
Stefania Tomasiello , Italy  
Gisella Tomasini , Italy  
Isabella Torricollo , Italy  
Francesco Tornabene , Italy  
Mariano Torrisi , Italy  
Thang nguyen Trung, Vietnam  
George Tsiatas , Greece  
Le Anh Tuan , Vietnam  
Nerio Tullini , Italy  
Emilio Turco , Italy  
Ilhan Tuzcu , USA  
Efstratios Tzirtzilakis , Greece  
FRANCISCO UREÑA , Spain  
Filippo Ubertini , Italy  
Mohammad Uddin , Australia  
Mohammad Safi Ullah , Bangladesh  
Serdar Ulubeyli , Turkey  
Mati Ur Rahman , Pakistan  
Panayiotis Vafeas , Greece  
Giuseppe Vairo , Italy  
Jesus Valdez-Resendiz , Mexico  
Eusebio Valero, Spain  
Stefano Valvano , Italy  
Carlos-Renato Vázquez , Mexico  
Martin Velasco Villa , Mexico  
Franck J. Vernerey, USA  
Georgios Veronis , USA  
Vincenzo Vespri , Italy  
Renato Vidoni , Italy  
Venkatesh Vijayaraghavan, Australia


Anna Vila, Spain  
Francisco R. Villatoro , Spain  
Francesca Vipiana , Italy  
Stanislav Vitek , Czech Republic  
Jan Vorel , Czech Republic  
Michael Vynnycky , Sweden  
Mohammad W. Alomari, Jordan  
Roman Wan-Wendner , Austria  
Bingchang Wang, China  
C. H. Wang , Taiwan  
Dagang Wang, China  
Guoqiang Wang , China  
Huaiyu Wang, China  
Hui Wang , China  
J.G. Wang, China  
Ji Wang , China  
Kang-Jia Wang , China  
Lei Wang , China  
Qiang Wang, China  
Qingling Wang , China  
Weiwei Wang , China  
Xinyu Wang , China  
Yong Wang , China  
Yung-Chung Wang , Taiwan  
Zhenbo Wang , USA  
Zhibo Wang, China  
Waldemar T. Wójcik, Poland  
Chi Wu , Australia  
Qihong Wu, China  
Yuqiang Wu, China  
Zhibin Wu , China  
Zhizheng Wu , China  
Michalis Xenos , Greece  
Hao Xiao , China  
Xiao Ping Xie , China  
Qingzheng Xu , China  
Binghan Xue , China  
Yi Xue , China  
Joseph J. Yame , France  
Chuanliang Yan , China  
Xinggang Yan , United Kingdom  
Hongtai Yang , China  
Jixiang Yang , China  
Mijia Yang, USA  
Ray-Yeng Yang, Taiwan

Zaoli Yang , China  
Jun Ye , China  
Min Ye , China  
Luis J. Yebra , Spain  
Peng-Yeng Yin , Taiwan  
Muhammad Haroon Yousaf , Pakistan  
Yuan Yuan, United Kingdom  
Qin Yuming, China  
Elena Zaitseva , Slovakia  
Arkadiusz Zak , Poland  
Mohammad Zakwan , India  
Ernesto Zambrano-Serrano , Mexico  
Francesco Zammori , Italy  
Jessica Zangari , Italy  
Rafal Zdunek , Poland  
Ibrahim Zeid, USA  
Nianyin Zeng , China  
Junyong Zhai , China  
Hao Zhang , China  
Haopeng Zhang , USA  
Jian Zhang , China  
Kai Zhang, China  
Lingfan Zhang , China  
Mingjie Zhang , Norway  
Qian Zhang , China  
Tianwei Zhang , China  
Tongqian Zhang , China  
Wenyu Zhang , China  
Xianming Zhang , Australia  
Xuping Zhang , Denmark  
Yinyan Zhang, China  
Yifan Zhao , United Kingdom  
Debao Zhou, USA  
Heng Zhou , China  
Jian G. Zhou , United Kingdom  
Junyong Zhou , China  
Xueqian Zhou , United Kingdom  
Zhe Zhou , China  
Wu-Le Zhu, China  
Gaetano Zizzo , Italy  
Mingcheng Zuo, China

# Contents

---

## **Mobile, Divisible, and Safe E-Cash System**

Ting Huang 

Research Article (3 pages), Article ID 5537965, Volume 2021 (2021)

## **An Improved Image Steganography Scheme Based on Partial Preservation Embedding Algorithm for Wireless Visual Sensor Networks**

Qian Shen , Tao Jiang , Yongjun Zhu , and Yin Wu 

Research Article (15 pages), Article ID 6618134, Volume 2021 (2021)

## Research Article

# Mobile, Divisible, and Safe E-Cash System

Ting Huang 

College of Computer and Information Technology, China Three Gorges University, Yichang, Hubei 443002, China

Correspondence should be addressed to Ting Huang; 3451292652@qq.com

Received 6 January 2021; Revised 26 February 2021; Accepted 11 March 2021; Published 19 April 2021

Academic Editor: Mohammed Fattah

Copyright © 2021 Ting Huang. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Mobile, divisible, and safe e-cash system adapts on mobile terminals for e-payment which can circulate in multiple banks. The usage of the divisible e-cash does not need pass bank, which the bank has not the bottleneck of e-business. The author's thesis discusses on the withdrawal protocol, payment protocol, transferable protocol, deposit protocol, and update of e-cash, based on elliptic curve cryptography (ECC). The system is simple, efficient, secure, and fit for the mobile e-payment terminals in which storage, power, operand capacity, and network bandwidth supply are extraordinarily restricted. The system can protect from double spending, non-frameability, eavesdropping, tampering, and "perfect crime" effectively too. It can save from mis-identity attacks, two-layer anonymity attacks, and linking attacks.

## 1. Introduction

With the development of science and technology and the progress of society, e-cash began to enter people's lives and gradually changed people's consumption concept and mode. Compared with the traditional paper money, e-cash has the advantages of fast transmission, wide coverage, and convenient use, which has replaced the paper money with an irreversible trend. But the e-cash systems use online payment nowadays. The usage of every e-cash system must pass the bank [1]; thus, the bank has turned into the bottleneck of the payment. The e-cash [2] only circulates in a single bank, which cannot meet the needs of reality. The e-cash system [3] based on RSA encryption algorithm problem which needs exponentiation compute. The e-cash [4] cannot be circulated in user's e-business. This paper researches on mobile, divisible, and safe e-cash system. The e-cash in this study is divisible, and the usage of the divisible e-cash system need not pass bank, which the bank has not the bottleneck of e-business. Meanwhile, the system can protect from double spending. ECC in this paper needs no exponentiation operation compared to RSA. The research effectively improves the efficiency and security of mobile e-cash system, which provides the theoretical basis and technical support for an electronic transaction system nowadays. In the system, the consumer can recover the lost

money even if the phone has crashed and all the files are removed accidentally or the e-cash wallet has been lost. The e-cash in this study can circulate in all the banks, which can meet the needs of reality. The e-cash in this study can circulate in user's e-business, which circulates any time offline between the users before getting saved in the bank. In comparison with the protocol in [5], the proposed protocol can protect from eavesdropping, tampering, and "perfect crime" effectively too. The e-cash in this study and its signatures cannot be forgery. It can save from mis-identity attacks, two-layer anonymity attacks, and linking attacks. The system is simple, efficient, secure, and fit for the mobile e-payment terminals in which storage, power, operand capacity, and network bandwidth supply are extraordinarily restricted. The e-cash in the system has a usage period. When the usage period ends, the bank will delete the e-cash. Thus, the storage space of the bank is saved.

## 2. Design of Protocol

### 2.1. Withdrawal Protocol

- (1) The user withdraws  $I$  yuan from the bank $_m$ . He takes  $a \in_R Z_n$  and then computes  $\delta = H(a + SK_U)$ . Next, he enters  $\delta$  in the database, encrypts  $ID_n U$ ,  $\delta$ , and  $I$  by the symmetric key, and sends them to the bank $_m$ .

- (2) The bank<sub>m</sub> produces the e-cash:  $\alpha_i = H[(ISK_{Bm1} + \delta SK_{Bm2}) \| SK_{Bm} \| t_1 \| b]$  and computes  $\beta_i = H[(cG_x) \| \alpha_i \| t_1 \| I]$ ,  $\gamma_i = c + \beta_i SK_{Bm}$ , and  $b, c \in_R Z_n$ . The bank<sub>m</sub> enters  $\alpha_i, b, \delta, t_1$ , in the database, encrypts IDnU, I,  $\alpha_i, \beta_i, \gamma_i$ , and  $t_1$  and sends to the user.
- (3) The user decrypts IDnU, I,  $\alpha_i, \beta_i, \gamma_i$ , and  $t_1$  and saves them to the database.

**2.2. Payment Protocol.** The user pays the e-cash to the merchant<sub>0</sub> by the credit center. First  $\alpha_i = H(b_1 \| t_2 \| SK_U \| \alpha_i \| j \| i)$ ,  $\beta_i = H[(c_1 G_x) \| \alpha_i \| t_2 \| j \| i]$ ,  $\gamma_i = c_1 + \beta_i SK_U$ ,  $b_1, c_1 \in Z_n$ ,  $d, e_1, e_2 \in Z_n$ ,  $d \neq 0$ ,  $\varepsilon = H(\alpha_i)$ ,  $\varepsilon_1 = dI D_{nU} - \varepsilon e_1$ ,  $\varepsilon_2 = d - \varepsilon e_2$ ,  $\alpha_i, \beta_i, \gamma_i, i, j, t_2, \varepsilon, \varepsilon_1, \varepsilon_2$  are sent to the credit center. The e-cash cannot be used the next time. Then the credit center checks  $\beta_i \stackrel{?}{=} H[(\gamma_i G - \beta_i PK_U) \| \alpha_i \| t_2 \| j \| i]$  and saves  $i, \alpha_i, \beta_i, \gamma_i, \varepsilon, \varepsilon_1, \varepsilon_2$ . It gets  $\varphi = H[i \| (SK_C PK_M)_x]$  and sends  $\varphi$ , NAU, and Timestamp to the merchant<sub>0</sub>. The merchant<sub>0</sub> checks  $\varphi \stackrel{?}{=} H[i \| (PK_C SK_M)_x]$  and then sends the goods to the user. The user receives the goods, gets  $f = H[(SK_U PK_C)_x]$ , deletes  $\alpha_i, \beta_i, \gamma_i, i$ , and sends  $f$ , merchant's address, NAU, and timestamp to the credit center. The credit center checks  $f \stackrel{?}{=} H[(SK_C PK_M)_x]$ , computes  $\varphi' = H[i \| (SK_C PK_M)_x \| \alpha_i]$ , and sends  $i, \alpha_i, NAU, f, \varepsilon, \varepsilon_1, \varepsilon_2$ , and timestamp to the merchant<sub>0</sub>. The merchant<sub>0</sub> tests  $\varphi' \stackrel{?}{=} H[i \| (SK_M PK_C)_x \| \alpha_i]$  and saves  $\alpha_i, i, \varepsilon, \varepsilon_1, \varepsilon_2$ .

The protocol that the merchant<sub>0</sub> pays the e-cash to the merchant<sub>i</sub> ( $i = 1, 2, \dots, n$ ) or factory is the same as the payments that the user pays to merchant.

**2.3. Transferable Protocol.** The e-cash can circulate in the user's e-business. First, the user<sub>1</sub> computes  $\varepsilon = H(\alpha_i)$ ,  $\varepsilon_1 = dI D_{nU1} - \varepsilon e_1$ ,  $\varepsilon_2 = d - \varepsilon e_2$ ,  $d, e_1, e_2 \in Z_n$ ,  $d \neq 0$ ,  $b_1, c_1 \in Z_n$ ,  $\alpha_i = H(b_1 \| t_3 \| SK_{U1} \| \alpha_i \| j \| i)$ ,  $\beta_i = H[(c_1 G_x) \| \alpha_i \| t_3 \| j \| i]$ ,  $\gamma_i = c_1 + \beta_i SK_{U1}$ , and sends  $\alpha_i, \beta_i, \gamma_i, i, j, t_3, \varepsilon, \varepsilon_1$ , and timestamp the e-cash cannot use again. Then the user 2 tests  $\beta_i \stackrel{?}{=} H[(\gamma_i G - \beta_i PK_{U1}) \| \alpha_i \| t_3 \| j \| i]$  and saves  $\alpha_i, \beta_i, \gamma_i, i, j, t_3, \varepsilon, \varepsilon_1, \varepsilon_2$ .

**2.4. Deposit Protocol.** When the person saves the e-cash to the bank, the bank must verify the correctness of the e-cash. The distributed bank must check whether the used e-cash is less than or equal to the distributed e-cash. If the used e-cash is more than the distributed e-cash, the bank can trace the person's identification. When the person saves the e-cash to the bank<sub>n</sub>, the e-cash will save in the bank<sub>n</sub>; when the person saves the e-cash to the bank<sub>m</sub> (not the distributed bank<sub>n</sub>), the bank<sub>m</sub> will send the e-cash to the bank<sub>n</sub>. After the e-cash in the bank<sub>n</sub> is dealt well, the person finishes the deposit. The central bank that has the highest grade among banks can test the trading process of the bank to check the business errors and punishment them. Thus, the e-cash can circulate in all the banks, which can meet the needs of reality.

**2.5. Update of the E-Cash.** When the usage period of the e-cash is over, the person tells the bank and fetches the new e-cash.

### 3. Discussion of Safety and Efficiency

$\alpha_i, \beta_i$ , and  $\gamma_i$  are the right signatures of the e-cash  $i$ . Because  $\gamma_i G - \beta_i PK_U = (c + \beta_i SK_U)G - \beta_i PK_U = cG$ ,  $\beta_i \stackrel{?}{=} H[(\gamma_i G - \beta_i PK_U) \| \alpha_i \| t_2 \| j \| i]$  is verified. The e-cash and its signatures cannot be forged.

The e-cash and its signatures contain SK. Any attacker must gain SK so as to forge the e-cash and its signatures, which must solve ECDLP. ECDLP cannot be solved, so that the e-cash and its signatures cannot be forged. It can save from mis-identity attacks, two-layer anonymity attacks, and linking attacks. Therefore, the e-cash is safe and divisible.

When the user pays the e-cash with value  $i$  for the first time, the user sends  $\alpha_i = H(b_1 \| t_2 \| SK_U \| \alpha_i \| i \| i)$  ( $i < I$ ). The e-cash with value  $I-i$  can use next. When he pays the e-cash with value  $k$  for the second time, the user sends  $\alpha_i = H(b_1 \| t_2 \| SK_U \| \alpha_i \| j \| k)$  ( $j = i + k$ ). Similarly, the e-cash can be used repeatedly until ( $j = I$ ). Thus, the usage of the divisible e-cash need not pass bank, which the bank has not the bottleneck of e-business.

**3.1. Non-Frameability.**  $\varepsilon_1 = dI D_{nU} - \varepsilon e_1$ , so the user's identification is sent with the e-cash. Thus, illegal users cannot frame other users, due to the security against mis-identity attacks, two-layer anonymity attacks, and linking attacks.

When a person uses the e-cash normally, his identity cannot be gained. However, the bank will trace the identity of the user when his e-cash is used repeatedly.

If the person spends the e-cash repeatedly, the bank will find when his e-cash was deposited. Because  $b$  is not the same as different e-cash,  $\varepsilon = H(\alpha_i)$  and  $\alpha_i = H[(ISK_{Bm1} + \delta SK_{Bm2}) \| SK_{Bm} \| t_1 \| b]$  are different when the user's demand is the same. When the person uses the same e-cash repeatedly, the bank will fetch the other ( $\varepsilon', \varepsilon'_1, \varepsilon'_2$ ).  $d \neq 0$ ,  $\varepsilon'_1 = dI D_{nU} - \varepsilon' e_1$ , and  $\varepsilon'_2 = d - \varepsilon' e_2$ . Thus,  $ID_{nU} = ((\varepsilon' e_1 - \varepsilon \varepsilon'_1) / (\varepsilon' e_2 - \varepsilon \varepsilon'_2)) \pmod n = ((\varepsilon' dI D_{nU} - \varepsilon' dI D_{nU}) / (\varepsilon' d - \varepsilon d))$ . The bank will check the user's identity  $ID_{nU}$ . Thus, the system can prevent from double spending. So the system is safe, and the bank must be reliable and safe.

The anonymity and untraceability of signatures facilitate criminals to kidnap, launder, and extort money. So it is necessary to design a fair and controllable e-cash system. If he extorts money from the victim, the criminal can only ask the victim to transfer the money. After the victim transfers the e-cash, the criminal obtains the e-cash ( $I, \alpha_i, \varepsilon, \varepsilon_1, \varepsilon_2$ ) and releases the victim. Then the victim can report to the bank that the e-cash ( $I, \alpha_i, \varepsilon, \varepsilon_1, \varepsilon_2$ ) is obtained by extorting means. When the criminal is spending the e-cash, the merchant can call the police and arrest the criminal. After the case is solved, the bank will return the recovered e-cash to the victim. The system can protect from non-frameability, eavesdropping, tampering, and "perfect crime" effectively. So the system is secure.

The time of protocol realization and storage capacity in mobile, divisible, and safe e-cash systems are key to efficiency. 160b of ECC of the paper has the same function with 1024b of RSA [6]. The e-cash system [3] is based on RSA. ECC in the paper needs no exponentiation operation

compared to RSA. The calculation of ECC is very little compared to RSA. Therefore the efficiency of the system runs faster. The e-cash of spending process [3] is  $\bar{S}l, \bar{T}l, \bar{R}l, \bar{K}, \bar{S}, \bar{S}_0, \bar{S}_1, \bar{S}_2, \bar{C}, \bar{T}, b, t, B_1, D_1, D_2, \pi_2$ , the storage space of the e-cash is  $1024 * 10 + 128 + 1024 * 5 = 15488$  bit. While the e-cash of spending process in the paper is  $i, \alpha_i, \beta_i$ , and  $\gamma_i$ , the storage space of the e-cash is  $32 + 128 + 128 + 192 = 480$  bit (The actual cost in the experimental system), which decreases 96.9% of the storage space and the network bandwidth. Therefore, the system is simple, efficient, and fit for the mobile e-payment terminals in which storage, power, operand capacity, and network bandwidth supply are extraordinarily restricted.

The e-cash in the system has a usage period. When the usage period ends, the bank will delete the e-cash. Thus, the storage space is saved.

The e-cash in the system can circulate in multiple banks, which does not confine to the bank that distributes the e-cash.

The e-cash [1] is inseparable. When the user withdraws the money from the bank, he can only use the money at one time. The merchant has to deposit it in the bank to verify the authenticity. Therefore, the bank has become a bottleneck. The e-cash can be divided. After the user withdraws the money from the bank, he can spend several times without frequently looking for the bank to withdraw money. The merchant does not have to deposit every money that they receive into the bank for verification. When the merchant needs to deposit money, the bank will verify the authenticity of the cash and find out the illegal e-cash.

The e-cash [4] cannot work between the users. However, the e-cash in the system can circulate any time offline between the users before getting saved in the bank.

#### 4. Conclusions

The mobile, divisible, and safe e-cash system adapts on mobile terminals for e-payment which can circulate in multiple banks. The usage of the divisible e-cash needs not pass bank, which the bank has not the bottleneck of e-business. Experimental tests have been made, which prove that the system is simple, efficient, security, and fit for the mobile e-payment terminals in which storage, power, operand capacity, and network bandwidth supply are extraordinarily restricted.

#### Data Availability

The data used in the study are available at <https://www.hindawi.com/publish-research/authors/research-data/#composing-a-data-availability-satement>.

#### Conflicts of Interest

The authors declare that they have no conflicts of interest.

#### Acknowledgments

The author thanks 2020 International Conference on Artificial Intelligence and Advanced Manufacture for publishing the article "Electronic Cash System based on Multi-Bank Mobile Divisible, Recoverable and Transferable".

#### References

- [1] X. Liu and Q. Xu, "Improved e-cash system with anonymous user suspension" *Application Research of Computers*, vol. 33, no. 10, pp. 3099–3104, Oct.2016.
- [2] D. Shao, B. Kang, and J. Wang, "Analysis and improvement of two electronic cash schemes," *Journal of Computer Applications*, vol. 37, pp. 1–6, 2017.
- [3] X. Liu and Bo Zhang, "improved endorsed E-cash system with DAA-A," *Journal of Computer Research and Development*, vol. 53, no. 10, pp. 2412–2429, 2016.
- [4] Y. Liang, X. Zhang, and Z. Zheng, "Electronic cash system based on certificateless group signature," *Journal on Communications*, vol. 37, no. 5, pp. 184–190, 2016.
- [5] Z. Jiang-xiao, F. Chun-hui, Ma Jin-xin et al., "Transferable e-cash system with arbitrarily spending order," *Transactions of Beijing Institute of Technology*, vol. 39, no. 3, pp. 283–289, 2019.
- [6] A. J. Menezes, T. Okamoto, and S. A. Vanstone, "Reducing elliptic curve logarithms to logarithms in a finite field," *IEEE Transactions on Information Theory*, vol. 39, no. 5, pp. 1639–1646, 1993.



## Research Article

# An Improved Image Steganography Scheme Based on Partial Preservation Embedding Algorithm for Wireless Visual Sensor Networks

Qian Shen <sup>1</sup>, Tao Jiang <sup>2</sup>, Yongjun Zhu <sup>3</sup>, and Yin Wu <sup>4</sup>

<sup>1</sup>Faculty of Automation, Huaiyin Institute of Technology, Huai'an 223000, China

<sup>2</sup>Nanjing Electronic Devices Institute, Nanjing 210000, China

<sup>3</sup>School of Electronic & Information Engineering, Suzhou University of Science and Technology, Suzhou 215009, China

<sup>4</sup>College of Information Science & Technology, Nanjing Forestry University, Nanjing 210000, China

Correspondence should be addressed to Qian Shen; [qianshen@hyit.edu.cn](mailto:qianshen@hyit.edu.cn)

Received 7 November 2020; Accepted 14 February 2021; Published 28 February 2021

Academic Editor: Mohammed Fattah

Copyright © 2021 Qian Shen et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

With the continuous improvement of encryption algorithms, some applications based on the architecture of wireless visual sensor networks have gradually shifted their attention to the imperceptibility and antijamming performance of secret images. To reduce the probability of secret images being detected, the current research focuses on hiding secret data in the least-significant bit of the cover image in the spatial domain or embedding data into the coefficients of the high-frequency band in the transformational domain, which usually leads to poor performance in a hostile environment. Therefore, some researchers proposed to substitute the coefficients of the medium-frequency band in the transformational domain with secret information to enhance the anti-interference performance. However, this idea would severely affect the imperceptibility of secret images. As a result, an improved version based on the partial preservation embedding algorithm was designed in this paper. Theory analysis and simulation results indicate that the proposed scheme performs better than the existing methods by directly substituting the coefficients of the medium-frequency band in the transformational domain, especially in the case of strong noise interference.

## 1. Introduction

Because of the convenience in networking, low cost in maintenance, and strong resistance to natural disasters, Wireless Visual Sensor Networks (WVSN) are suitable for various applications such as traffic management and intelligent monitoring. Recently, continuous progress has been made in the security and compressibility of image encryption systems owing to the development of chaos and compressive sensing (CS) technology [1–4]. However, some applications might have specific requirements. For example, most of the tactical reconnaissance missions in battlefields need to transmit scenes obtained by visual acquisition nodes through the wireless channels, during which the corresponding electromagnetic signals exposed in the air are easy to be accessed by enemies. The most common solution is to

use various encryption algorithms to improve the security of data before transmitting. To get satisfactory security performance, systems designed for this kind of applications are also required that secret images must be imperceptible [5]. As a result, confidential information is generally transmitted by means of hiding in unrelated images. In this case, the hidden data should be safely transmitted in the channel and accurately reconstructed at the receiving terminals, while there are no strict requirements on the reconstruction accuracy of cover images. To delve into these questions, researchers combined information security theory with signal processing technology and then proposed the basic concept and specific scheme of information hiding [6–12].

Nowadays, image hiding has become a hotspot of relevant areas. Since images are naturally redundant, they are quite suitable for embedding confidential information.

According to the basic architecture of image hiding systems, the key indicators include not only the security and anti-interference performance but also the maximum information embedding capacity and imperceptibility [5]. Traditional image steganography schemes focused on hiding secret data to the least significant bit (LSB) of cover images in the spatial domain or replacing the coefficients of the high-frequency band in the transformational domain with secret images [13–15]. These methods are simple and feasible to be utilized. Moreover, the desired imperceptibility could be obtained because the human visual system is insensitive to changes in the low-significant bits of pixel values. Nevertheless, even basic image processing operations (compression, filtering, etc.) would cause serious distortion to secret information [16]. More importantly, the propagation in a wireless channel is likely to be affected by various kinds of interference, which is unqualified to WWSN applications.

To address this problem, Li et al. [17] designed a reversible image steganography scheme based on block compressive sensing (BCS). In the front node, each element of bit-serialized pixels in the secret image would be hidden into one nonoverlapping block. When secret information was being extracted, a priori knowledge of the strong correlation between adjacent pixels on the boundary of each block could be utilized to recognize hidden information from each block of the stego image. However, this method requires the terminal users to take the correlation between adjacent pixels on the blocks' boundary as an evaluation function for extracting secret images, which results in low maximum embedding capacity because for that size of blocks must be big enough to ensure the accuracy of judgment. For example, the maximum embedding rate would be less than 0.05% if employing  $16 \times 16$  blocks. Furthermore, for special cover images, such as images with flat texture in the vertical or horizontal direction, it is likely to have misjudgement in the process of extracting hidden information by the weak correlation between adjacent pixels on some boundaries. It would definitely reduce the accuracy of the extracted information. In conclusion, the BCS-based steganography method exhibits low practical value because of its low embedding rate and poor universality. Later, some other research studies were proposed to hide secret images in the space of the medium-frequency band to boost the maximum embedding capacity and antijamming performance [18, 19]. However, it would lead to a sharp decrease in the similarity between the stego image and cover image, which affected the imperceptibility of the secret image.

To improve the imperceptibility of secret images without reducing the antijamming performance and the maximum embedding capacity, this paper designed an optimized image steganography scheme based on the partial preservation embedding algorithm (ISS-PPEA). The rest of this paper would be organized as follows. First, the preliminary knowledge would be briefly introduced in the next section. Then, in Section 3, the framework of the proposed system and the detailed steps are explained in detail. In addition, the simulation results and the corresponding analysis are illustrated in Section 4. Lastly, all the work in this paper would be summarized in Section 5.

## 2. Preliminary Knowledge

Due to the characteristics of deterministic randomness, extreme sensitivity to initial states, etc., chaotic systems are widely used as the generator of encryption sequences in image encryption systems. In addition, CS has been considered as an optimal technique to counter threats caused by open channel, big data, and harsh communication circumstances in WWSN. Since the image encryption algorithm based on CS and nonuniform quantization (IEA-CS-NQ) has been proved to be safe enough for WWSN [20], this paper takes it directly as part of the proposed scheme. To make the designed system easier to be understood, the main steps of the encryption part in IEA-CS-NQ would be reviewed in this section as follows.

*2.1. Measurement.* In sensor nodes, scenes are directly acquired by a micromirror array controlled by the measurement matrices. Therefore, the core problem in this step is the construction of it. Considering the Restricted Isometry Property (RIP), building the Gaussian random matrix and Bernoulli random matrix are the preferable solutions. However, due to the security requirements, the measurement matrix is generally generated indirectly by the secret key transferred, which makes this plan inappropriate. As a result, IEA-CS-NQ employs the chaotic sequence to construct a cyclic matrix to boost the generation efficiency of the measurement matrix. More importantly, it has been proved that this Toeplitz-structured matrix provides better performance in irrelevant measurements. The circulant matrix is as follows:

$$\Phi = \sqrt{\frac{1}{m}} \cdot \begin{bmatrix} S_1(n) & S_1(n-1) & \cdots & S_1(1) \\ S_1(1) & S_1(n) & \cdots & S_1(2) \\ \vdots & \vdots & \ddots & \vdots \\ S_1(m-1) & S_1(m-2) & \cdots & S_1(m) \end{bmatrix}, \quad (1)$$

which would be employed to measure the original scene, whose elements  $S_1(1)$  and  $S_1(2), \dots, S_1(n)$  are pseudo-random sequences generated by specific chaotic systems. Here, the symbol  $n$  represents the length of the serialized original image, while  $m$  stands for the sequence length obtained by compressive measurement. Thus, the compression ratio (CR) could be defined as  $m/n$ . Besides, the coefficient  $\sqrt{1/m}$  is the scale factor to realize the column normalization. Then, the process of measuring could be represented as follows:

$$y = \Phi \cdot x, \quad (2)$$

where  $x$  represents the serialized scene and  $y$  stands for the measurement result.

*2.2. Quantization.* As we know, the calculation result should be quantized to match the data type of pixel values in the digital image. However, the traditional uniform quantization



(UQ) method would lead to significant loss of data accuracy because of the uneven distribution of quantization resources. Moreover, it is vulnerable against CPA based on differential analysis algorithms. Therefore, IEA-CS-NQ designed a nonuniform quantization (NQ) method by adding a nonlinear pretreatment function with adaptive parameters to solve these problems. This function,

$$z = \frac{1}{1 + e^{-a(y-os)}}, \quad (3)$$

contains two parameters regulated by the measurement result  $y$ . The parameter  $a$  determines the convergence rate, while the parameter  $os$  determines the convergence centre of the result  $z$ .

**2.3. Confusion and Substitution.** The last step of encryption in IEA-CS-NQ is the process of confusion and substitution. To be specific, the confusion is controlled by an index sequence  $I$  ranging from 1 to  $m$ , which is generated by a chaotic system. Substitution is operated by the following formula:

$$C(i) = Q_{rc}(i) \oplus B(i), \quad (4)$$

with the help of chaotic sequence  $B$ . Here,  $C$  is the cipher image to be sent, and  $i$  represents the index of the sequence. In addition,  $Q_{rc}$  stands for the result of confusion.

After all steps mentioned above have been completed, the corresponding cipher image could be obtained. Theory analysis and simulation experiments have proved that IEA-CS-NQ performs better in terms of security and antijamming.

### 3. The Proposed Scheme

The structure of the image steganography scheme proposed by this paper is illustrated in Figure 1. It could be divided into two parts: the encryption-hiding process in sensor nodes and the extraction-decryption process in terminal user nodes.

For sensor nodes, the information which is being necessary to generate chaotic sequences is extracted from the secret key allocated in a safe way firstly. Then, the construction of the measurement matrix, generation of the confusion sequence, substitution sequence, and embedding position are completed based on the generated sequences. After that, the secret image containing information about the current scene captured by a sensor node could be obtained by executing the encryption process of IEA-CS-NQ. And, it would be embedded into the medium-frequency band in the Discrete Cosine Transformation (DCT) coefficients of a cover image bit by bit with the proposed partial preservation embedding algorithm (PPEA) afterwards. Finally, Inverse Discrete Cosine Transformation (IDCT) would be performed to obtain the stego image that is visually similar to the cover image, and it would be sent to the

database nodes or terminal user nodes through the wireless channel.

After the stego image is captured by terminal users, DCT should be conducted to acquire coefficients containing secret information. Then, the secret image about the original scene captured by the sensor node could be extracted by the inverse scheme of PPEA used in the sensor node. Afterwards, the estimation of the original scene would be reconstructed by the decryption part in IEA-CS-NQ. In most applications, the terminal user just needs to precisely get the original scene, and there is no requirement for the quality of reconstruction for the cover image. However, as the cover image reconstructed in the terminal node is equivalent to the stego image transmitted in the wireless channel, the accurate reestablishment of the cover image is beneficial to the improvement in the imperceptibility of secret images.

Without loss of generality, this paper assumes that the size of the cover image in the sensor node is  $\sqrt{N_1} \times \sqrt{N_1}$ , and the size of the scene in front of the sensor is  $\sqrt{N_2} \times \sqrt{N_2}$ . Besides, all images are eight-bit grey-scale, whose elements range from 0 to 255. The Orthogonal Matching Pursuit (OMP) is taken as the reconstruction algorithm of CS for the reason that this paper does not concern the corresponding design. The workflow of the designed system would be introduced in the following steps by taking the hiding process as an example.

**3.1. IEA-CS-NQ.** According to Figure 1, the scene at the sensor node would be captured and encrypted by IEA-CS-NQ. The necessary information such as parameter values and initial values used by chaotic systems are extracted from the key sequence allocated in a safe way. After all steps in the encryption part of IEA-CS-NQ are accomplished, the secret image containing information about the original scene could be obtained, which is clearly the object to be hidden. On the basis of equation (1), its size should be  $m \times \sqrt{N_2}$  if the measurement matrix  $\Phi$  has  $m$  rows. In this situation, the number of bits that need to be hidden is  $8m \times \sqrt{N_2}$ .

**3.2. DCT Transformation.** As described earlier in this article, the hiding method designed is executed in the medium-frequency band in the transformational domain of the cover image. For the sake of convenience, DCT was selected to convert the cover image from the spatial domain to the frequency domain by the following formula:

$$F(u, v) = \alpha(u)\alpha(v) \sum_{k=0}^{N_1-1} \sum_{l=0}^{N_1-1} f(k, l) \cos \left[ \frac{(2k+1)u\pi}{2N_1} \right] \cdot \cos \left[ \frac{(2l+1)v\pi}{2N_1} \right], \quad (5)$$

where  $f(k, l)$  stands for the  $k^{\text{th}}$  row and the  $l^{\text{th}}$  column element in the cover image. In addition,  $\alpha(u)$  and  $\alpha(v)$  are the normalization coefficients defined by

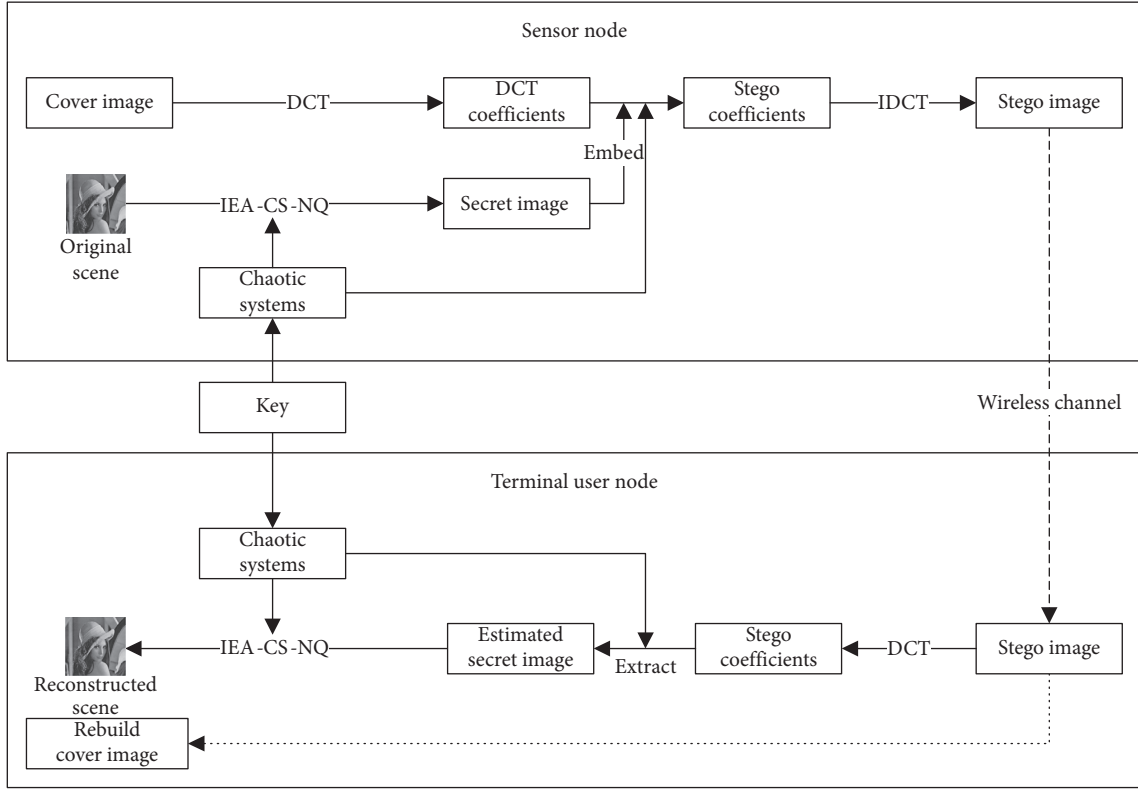


FIGURE 1: The framework of the proposed scheme.

$$\alpha(u), \alpha(v) = \begin{cases} \sqrt{\frac{1}{N_1}}, & u, v = 0, \\ \sqrt{\frac{2}{N_1}}, & u, v = 1, 2, \dots, N_1 - 1. \end{cases} \quad (6)$$

In the practical image processing operation, for reducing the complexity of DCT, the cover image is usually divided into nonoverlapping image blocks with equal size before transmitting. Thus, the final results calculated by equation (5) are generally DCT coefficient blocks. Current research has proven that, in the process of image segmentation, the accuracy of the reconstructed image would be reduced, and the segmentation effect would be obvious if the block size is too small. However, if the size of the block is oversize, the complexity of the transformation would increase dramatically. Therefore, most researchers chose a compromise that the block size was set to  $16 \times 16$ .

This paper also assumes that the block size of the cover image and the corresponding DCT coefficient matrix are both  $16 \times 16$ , by which  $\sqrt{N_1}$  could be divisible. Research studies have proved that most elements in the DCT coefficient matrix block are close to zero, for the reason that digital images usually contain a large amount of redundant data. Besides, the upper left to lower right elements in the coefficient block are generally considered as the low-frequency to high-frequency DCT coefficients. That is to say, the major information is concentrated in the upper left

corner of the DCT coefficient block, while the minor information is concentrated in the lower right corner. If all coefficients in a block are serialized with the zigzag order, the elements of the obtained vector could be considered as a coefficient sequence ordered by importance, and the specific process is drawn in Figure 2. It can be found that the coefficient matrix arranges its elements in the order indicated by the dotted line from the top left corner to the lower right corner. As a result, the importance of elements in this sequence is gradually descending. For facilitating subsequent theoretical analysis and simulation experiments, the low-frequency, medium-frequency, and high-frequency bands in the DCT coefficient matrix of an image block sizing  $16 \times 16$  are defined as the elements whose indexes are  $1 \sim 15$ ,  $16 \sim 143$ , and  $144 \sim 256$  in the zigzag sequence, respectively.

**3.3. Secret Information Embedding.** As we all know, the physiological structure of the human eyes determines that the human visual system is only sensitive to the information expressed by the high-significant bits in the pixel values of an image, and it is rather difficult for them to distinguish changes in the low-significant bits. In other words, the information contained in different significant bits could be considered to have different weights. As for DCT, this characteristic is directly reflected by the fact that different frequency coefficients are of different importance.

To intuitively perceive the different importances of coefficients in different bands, the standard Baboon image with size  $256 \times 256$  was taken as an example to conduct

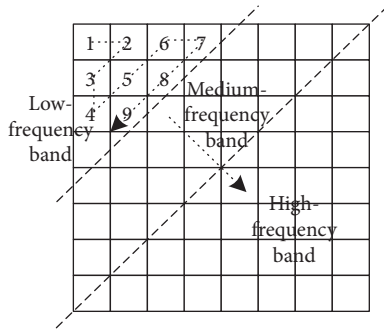


FIGURE 2: The diagram of the zigzag structure in the DCT coefficient matrix.

experiments. Suppose that fifteen low-frequency DCT coefficients, thirty medium-frequency DCT coefficients, or sixty high-frequency DCT coefficients were lost, the peak signal-to-noise ratio (PSNR) values of the corresponding reconstructed images were 26.97, 38.67, and 41.80, respectively. They are plotted in Figure 3. Surely, the extent of information loss in the reconstructed image is not positively correlated with the number of lost coefficients, but closely related to the frequency band of the lost coefficients. Specifically, the number of coefficients lost in the low-frequency band is the least, but the information loss in the reconstructed image is the most severe. The degree of loss in high-frequency coefficients is the worst, while the information loss is slightest. It means that the low-frequency coefficients are definitely essential during image reconstruction. Besides, even if the medium- and high-frequency coefficients are severely lost, the reconstruction would not be significantly affected.

Based on the conclusion mentioned above, this paper proposed to embed secret information into the medium-frequency band in the DCT coefficient matrix of the cover image to improve the antijamming performance of the image steganography system without significant influence on the reconstruction accuracy. Without loss of generality, it is assumed that the size of the cover image is  $512 \times 512$ , and the size of the original scene at the sensor node is  $128 \times 128$ . In addition, the value of CR utilized in IEA-CS-NQ is marked with  $cr$ . Clearly, the cover image could be transformed into 1024 groups of DCT coefficient block sizing  $16 \times 16$ , while the measurement result acquired by the sensor node could be converted into 1024 groups of bit sequence with  $128 \in cr$  elements. According to the condition that  $cr \in (0, 1]$ , the lengths of the bit sequence in each group assembled by the measurement results are certainly less than 128, which ensures that each group of the bit sequence could be embedded into the medium-frequency coefficients of one DCT coefficient block.

It is necessary to specify the embedding positions and the specific hiding method in the hiding process. As shown in Figure 1, the positions are determined by the sequence generated by a specific chaotic system. Before the  $l^{\text{th}}$  group of operation, a total of 128 elements from  $(128 \cdot (l - 1) + 1)^{\text{th}}$  to  $(128 \cdot l)^{\text{th}}$  in the chaotic sequence are indexed by values to get a sequence correlated to the embedding positions. Then, the elements indexed from 1 to  $128 \cdot cr$  in this sequence

would add 15 to be taken as the embedding positions of the current group. The process of hiding the  $i^{\text{th}}$  bit  $B(i)$  for the  $l^{\text{th}}$  group of operation into the  $j^{\text{th}}$  element  $A(j)$  in the corresponding DCT coefficient sequence  $A$  would be taken as an example to demonstrate PPEA. Suppose that  $B(i) = 0$ , the embedding operation designed by

$$A'(j) = \begin{cases} A(j), & A(j) \leq -\alpha \cdot |A_{\text{mid}}|, \\ -\alpha \cdot |A_{\text{mid}}|, & -\alpha \cdot |A_{\text{mid}}| < A(j), \end{cases} \quad (7)$$

would be applied to hide the bit sequence in the medium-frequency band of the DCT coefficient matrix orderly. Otherwise, the embedding operation would be

$$A'(j) = \begin{cases} A(j), & \alpha \cdot |A_{\text{mid}}| \leq A(j), \\ \alpha \cdot |A_{\text{mid}}|, & A(j) < \alpha \cdot |A_{\text{mid}}|. \end{cases} \quad (8)$$

Here, the conditions  $l \in \{1, 2, \dots, 1024\}$ ,  $i \in \{1, 2, \dots, 128 \cdot cr\}$ , and  $j \in \{16, 17, \dots, 143\}$  should be met. Besides, the symbol  $|A_{\text{mid}}|$  represents the absolute value of the average for all 128 medium-frequency coefficients  $A(16) \sim A(143)$ . In addition, the parameter  $\alpha$  is utilized to regularize the region size, whose value could be increased to enhance the antijamming performance of the steganography system or be reduced properly to improve the imperceptibility for secret information. Sign  $A'(j)$  is the result of the embedding operation for the medium-frequency band coefficient  $A(j)$  chosen from one group of DCT coefficients.

According to equations (7) and (8), the designed PPEA could improve the imperceptibility of secret information for the reason that it preserves most elements in the process of steganography. In other words, it only affects the elements valued between  $-\alpha \cdot |A_{\text{mid}}|$  and  $\alpha \cdot |A_{\text{mid}}|$  in the medium-frequency band of DCT coefficients for the cover image. Besides, the result of the embedding operation is constrained outside the interval  $(-\alpha \cdot |A_{\text{mid}}|, \alpha \cdot |A_{\text{mid}}|)$ , which could guarantee the antijamming performance of the steganography system. Indeed, the result of the embedding operation is not only determined by the absolute value of the average for all medium-frequency band coefficients but also by the region regulation parameter  $\alpha$ .

**3.4. IDCT Transformation.** Before data is transmitted through the wireless channel, the modified coefficient blocks obtained by the embedding operation should be converted to the stego image by applying IDCT. The obtained stego image would be visually safe but contains confidential information, which means the entire steganography is completed.

According to the structure shown in Figure 1, the extraction-decryption process in terminal user nodes is the inverse operation corresponding to the encryption-hiding process in sensor nodes. It is worth mentioning that each bit extracted is determined by the sign of the corresponding coefficient. After the extraction process is completed, the reconstructed scene could be obtained by directly applying the decryption part in IEA-CS-NQ.

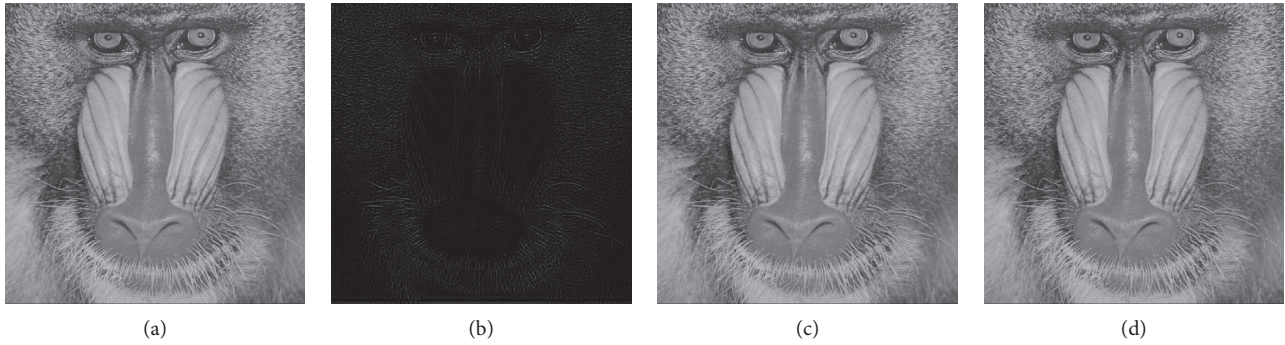


FIGURE 3: Reconstruction results of the Baboon image in different coefficient-loss situations. (a) No loss. (b) Fifteen low-frequency DCT coefficient losses. (c) Thirty medium-frequency DCT coefficient losses. (d) Sixty high-frequency DCT coefficient losses.

## 4. Simulation and Analysis

For simplicity, simulation experiments were conducted with scenes of size  $128 \times 128$  and cover images of size  $512 \times 512$ . According to the definition of the medium-frequency band and the designed embedding scheme introduced above, the maximum number of bits embedded is half of the number of elements in the DCT coefficient block for the cover image. Therefore, one secret image of size no more than  $128 \times 128$  could be embedded in a cover image. The security performance of ISS-PPEA could be obtained by analysing the experimental results. Moreover, the imperceptibility of the secret information, the anti-interference performance, and the operating efficiency of the system were also evaluated.

Some standard images were taken as examples to verify the effectiveness of the proposed scheme in conditions of zero-mean additive white Gaussian noise (AWGN) with standard deviations of 2% or 6.25% occlusion by rectangular shape in the corresponding stego images. Assuming that CR was set to 0.7, the results shown in Figure 4 indicated that ISS-PPEA had satisfactory imperceptibility and robustness.

### 4.1. Security Performance

**4.1.1. Ability of Resisting CPA.** According to the conclusion that IEA-CS-NQ is invulnerable to various kinds of attacks [20], ISS-PPEA could also be safe enough to resist common attacks including CPA because IEA-CS-NQ is directly utilized by the image steganography scheme proposed in this paper.

**4.1.2. Key Space and Key Sensitivity.** Current research suggests that the key space in a safe cryptosystem should be larger than  $2^{112}$  when confronting brute-force attacks [21]. Actually, it depends on the complexity of the chaotic system utilized in the designed steganography scheme. Due to the Optimized Coupled Map Lattice (OCML) model applied, the IEA-CS-NQ and specified embedding positions in ISS-PPEA require a key stream of more than 240 bits if the data precision is 16 bit, which is enough to satisfy the demand for key space. Moreover, users could tailor the size of the key

space on the basis of realistic situation and system requirements. In other words, the size of the key space in the designed scheme could easily meet the needs of different applications.

Key sensitivity is also an important characteristic of cryptosystems. Generally speaking, it requires that the cipher images encrypted with different secret keys should be totally different, and that the decrypted images obtained by incorrect keys would lose all useful information about the original image. However, due to the imperceptibility demanded of secret information in steganography systems, the corresponding requirements in the encryption part should be removed. To be specific, the stego images obtained with different secret keys might be visually similar. It was assumed that there existed a slight difference between the two groups of keys  $k_1$  and  $k_2$ , which resulted in a 0.001 deviation of the parameters in the corresponding chaotic system for generating the confusion sequence. Then, hiding the confidential Bridge scene into the Baboon cover image was taken as an example to verify the key sensitivity of ISS-PPEA. As shown in Figure 5, the difference between stego image A obtained with key  $k_1$  and stego image B obtained with key  $k_2$  is visually hard to be discovered, and it reflects the admirable imperceptibility in the steganography system. However, in the extraction-decryption process, the reconstructed images obtained from stego image A with different secret keys would be completely different according to Figure 6. It means that, even if there exists a tiny deviation in the secret key during the extraction-decryption process, the information in the original scene would be unrecoverable. Moreover, it is believed that the secret image annotated in Figure 1 is still extremely sensitive to key variations due to IEA-CS-NQ utilized in the designed scheme. In summary, the key sensitivity of ISS-PPEA conforms to the requirements in image steganography systems.

**4.1.3. Statistical Histogram.** By analysing the statistical histograms of the cover image and stego image, the change rule of the pixel values' distribution could be revealed, and then, some features of the corresponding steganography system might be leaked [22]. However, as shown in Figure 7, the stego images obtained mostly retained the statistical features of the original cover





FIGURE 4: Experimental results of standard images in different interference situations. (a) The cover images of (i) Baboon, (ii) Barbara, and (iii) Pepper. (b) The scenes of (i) Bridge, (ii) Couple, and (iii) Lena. (c) The stego images of (i) Baboon, (ii) Barbara, and (iii) Pepper with AWGN. (d) The reconstruction results of (i) Bridge, (ii) Couple, and (iii) Lena by stego images with AWGN. (e) The stego images of (i) Baboon, (ii) Barbara, and (iii) Pepper with occlusion. (f) The reconstruction results of (i) Bridge, (ii) Couple, and (iii) Lena by stego images with occlusion.

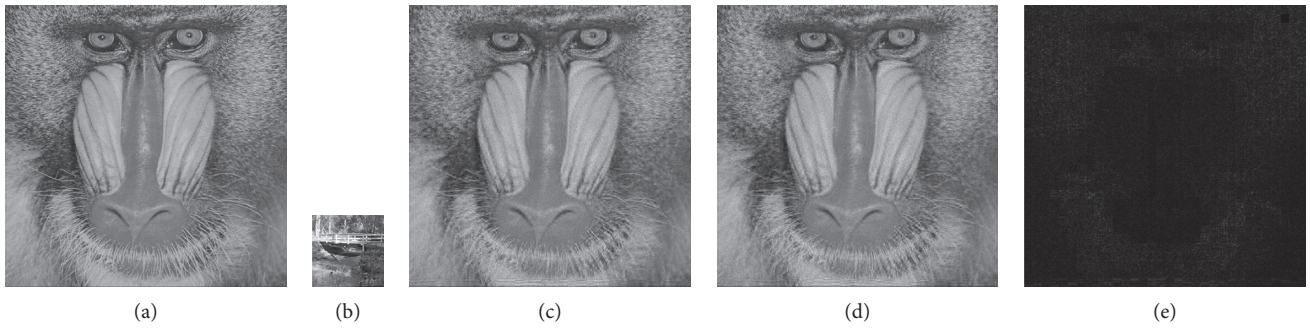


FIGURE 5: The key sensitivity in the encryption-hiding process for ISS-PPEA. (a) The cover image of Baboon. (b) The confidential scene of Bridge. (c) The stego image A obtained with key  $k_1$ . (d) The stego image B obtained with key  $k_2$ . (e) The difference between stego images A and B.

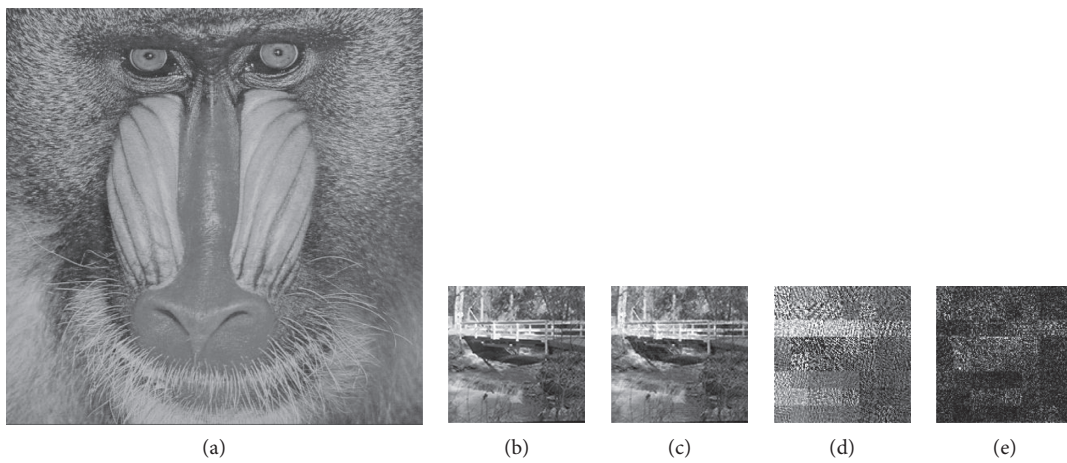


FIGURE 6: The key sensitivity in the extraction-decryption process for ISS-PPEA. (a) The cover image of Baboon. (b) The confidential scene of Bridge. (c) The reconstructed image A obtained from stego image A with key  $k_1$ . (d) The reconstructed image B obtained from stego image A with key  $k_2$ . (e) The difference between two reconstructed images A and B.

images, making it difficult for attackers to extract the information about the system from the statistical features of the stego images.

**4.1.4. Correlation Coefficients.** Generally speaking, the cipher images obtained by a cryptosystem could effectively eliminate the correlation between adjacent pixels of the scene image acquired by the sensor node. However, to optimize the imperceptibility of the secret information contained in the stego image, it is necessary for the stego image to maintain the characteristics of correlation similar to that of the corresponding cover image. An example of embedding the scene of Bridge into the cover image of Baboon is conducted to evaluate the characteristics of correlation in ISS-PPEA. The relationship of 1024 groups of adjacent pixel pairs in horizontal, vertical, and diagonal directions in the cover image and the corresponding stego image are drawn in Figure 8. Owing to the similar distribution of correlation, it could be considered that exploring system characteristics from adjacent pixel values is difficult for attackers. In addition, the correlation coefficients listed in Table 1 further provided evidence for the above conclusion.

**4.1.5. Randomness Analysis.** Information entropy  $H(s)$  is usually used to estimate the statistical measure of uncertainty. It could be defined as

$$H(s) = \sum_{i=0}^{255} P(s_i) \log_2 \frac{1}{P(s_i)}. \quad (9)$$

Here, the symbol  $s$  is a discrete random variable, and  $P(s_i)$  represents the probability density function of the appearance of  $s_i$ . If all values have the same probability, that is,  $P(s_i) = 1/2^8$ , then the value of  $H(s)$  should be 8. The information entropy of a meaningful image must be less than that. For an image steganography system, the information entropy of the stego image should be close to that of the corresponding cover image to improve the imperceptibility of the secret information. Some scene images embedded to cover images were taken as examples to evaluate this performance in ISS-PPEA. According to the results listed in Table 2, the characteristics of randomness in the cover images could be well preserved in the corresponding stego images. Therefore, the random characteristics of ISS-PPEA are believed to meet the design requirements.

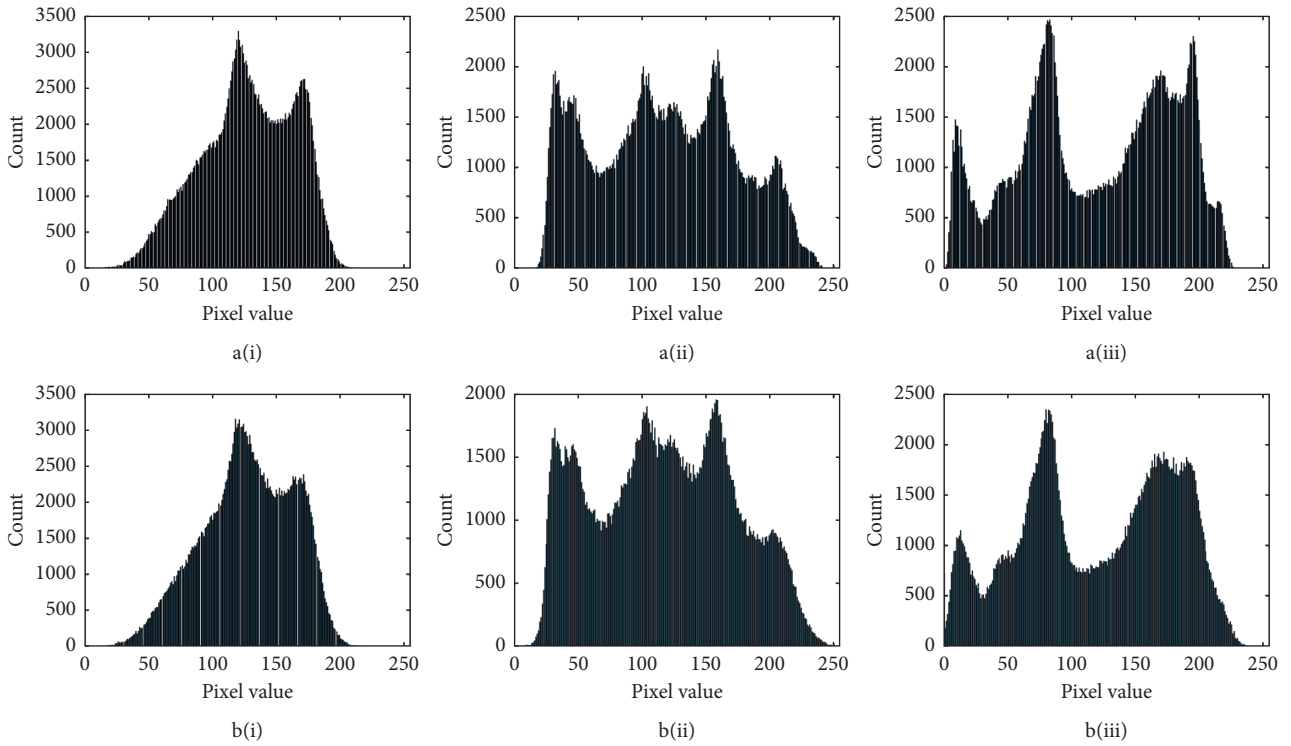


FIGURE 7: The statistical histograms for ISS-PPEA. (a) Histogram of the cover image for (i) Baboon, (ii) Barbara, or (iii) Pepper. (b) Histogram of the stego image using the cover image for (i) Baboon, (ii) Barbara, or (iii) Pepper.

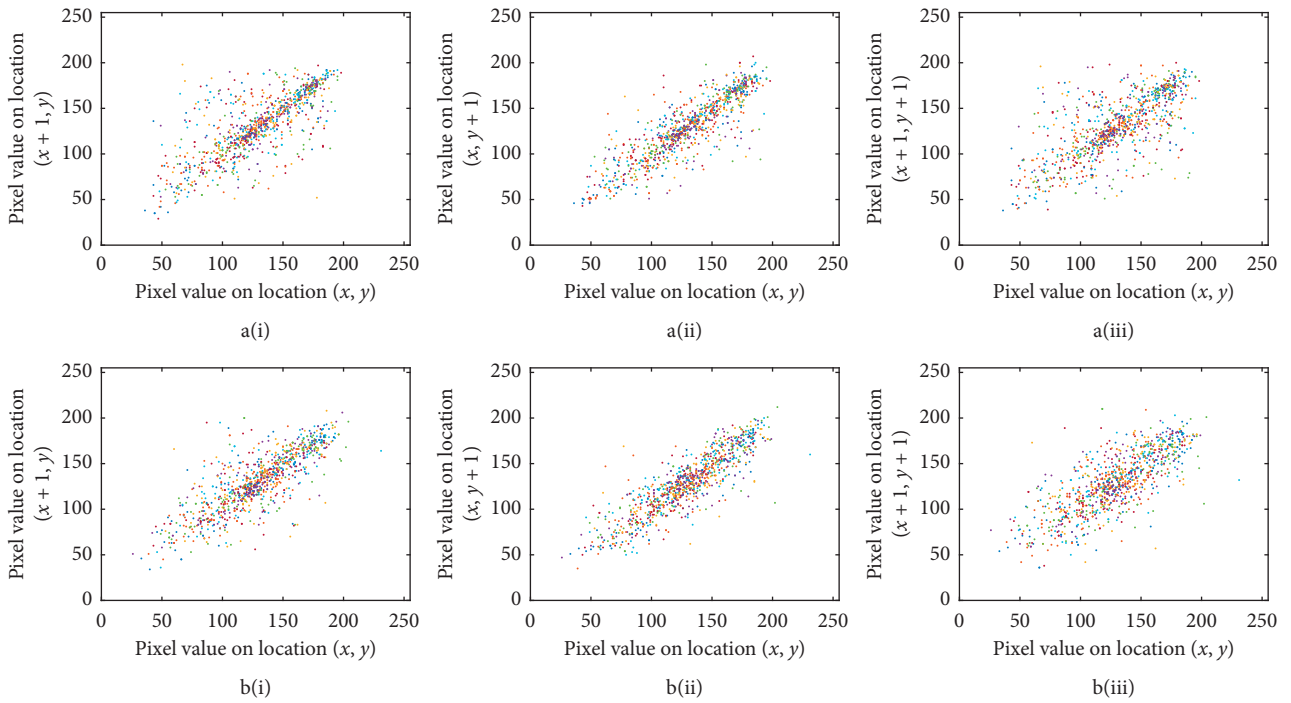


FIGURE 8: The correlation of adjacent pixel pairs for ISS-PPEA. (a) The correlation in the cover image of Baboon by (i) horizontal direction, (ii) vertical direction, or (iii) diagonal direction. (b) The correlation in the stego image using the cover image of Baboon by (i) horizontal direction, (ii) vertical direction, or (iii) diagonal direction.



TABLE 1: The correlation coefficients of adjacent pixel pairs in the cover image and stego image for ISS-PPEA.

Cover image/Scene	Horizontal direction	Vertical direction	Diagonal direction
Baboon/Bridge	0.7317/0.7598	0.8578/0.8698	0.7093/0.7304
Barbara/Couple	0.9621/0.9643	0.9098/0.9197	0.8897/0.9052
Pepper/Lena	0.9828/0.9826	0.9861/0.9857	0.9768/0.9766
Average value	0.8922/0.9022	0.9179/0.9251	0.8586/0.8707

TABLE 2: The information entropies in cover images and stego images for ISS-PPEA.

Cover image/Scene	Cover image	Stego image
Baboon/Bridge	7.1560	7.1235
Barbara/Couple	7.6332	7.6752
Pepper/Lena	7.6396	7.6644
Average value	7.4763	7.4877

## 5. Imperceptibility

Existing research shows that when observing an image, the human visual system would be highly adaptive to extract its structure information. And, it judges the degree of distortion by comparing the differences in the image structure information. Thus, the image steganography system should minimize the visual difference between the stego image and the corresponding cover image to reduce the detectability of secret information. According to the diagram illustrated in Figure 1, the imperceptibility of the secret information is primarily determined by the structural similarity between the stego image and the cover image and is positively correlated with it. Therefore, the Structural Similarity Index (SSIM) is utilized to evaluate the imperceptibility of secret information. It could be calculated with

$$\text{SSIM}(x, y) = l(x, y)^\alpha \cdot c(x, y)^\beta \cdot s(x, y)^\gamma. \quad (10)$$

Within this formula, there are definitions of

$$l(x, y) = \frac{2\mu_x\mu_y + C_1}{\mu_x^2 + \mu_y^2 + C_1}, \quad (11)$$

$$c(x, y) = \frac{2\sigma_x\sigma_y + C_2}{\sigma_x^2 + \sigma_y^2 + C_2}, \quad (12)$$

$$s(x, y) = \frac{\sigma_{xy} + C_3}{\sigma_x\sigma_y + C_3}. \quad (13)$$

Here, the symbols  $x$  and  $y$  represent the pixel values of the stego image and the corresponding cover image. Signs  $\mu_x$  and  $\sigma_x$  are the average and variance of the stego image, respectively. Symbol  $\sigma_{xy}$  stands for the covariance between the stego image and the cover image. Besides,  $C_1$ ,  $C_2$ , and  $C_3$  are constants with small values, which are used to ensure the stability of the denominators for equations (11) to (13). Parameters  $\alpha$ ,  $\beta$ , and  $\gamma$  are conveyed to adjust the weight distribution of brightness (average), contrast (variance), and structural information in the model. Surely, from the perspective of image information composition, SSIM defines the structure information as a special property reflecting the

scene structure independent of brightness and contrast and models the whole scene information as a combination of brightness, contrast, and structure. According to the definition of SSIM, the mean value of pixel values is taken as the estimation of brightness, while the standard deviation of pixel values is used as the estimation of contrast, and the covariance between two images acts as the estimation of the approximate degree of structure. In general, there are  $C_1 = (k_1 \cdot L)^2$ ,  $C_2 = (k_2 \cdot L)^2$ ,  $C_3 = C_2/2$ ,  $k_1 = 0.01$ ,  $k_2 = 0.03$ , and  $L = 255$ . Equation (10) could be simplified to

$$\text{SSIM}(x, y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)}, \quad (14)$$

when  $\alpha = \beta = \gamma = 1$ . On the basis of equations (7) and (8), the designed steganography scheme could modify the region adjustment parameter  $\alpha$  to meet the requirements for different applications. Specifically, the smaller  $\alpha$  would result in the smaller loss of the medium-frequency band of DCT coefficients in the encryption-hiding process. It means a larger SSIM of the stego image and the corresponding cover image, which optimizes the imperceptibility of the secret information. However, in this situation, the anti-interference performance would be influenced due to the smaller judgment threshold used for information extraction. On the contrary, if the value of the parameter  $\alpha$  is enlarged, the loss of the medium-frequency band of DCT coefficients would increase. It means a smaller SSIM of the stego image and the corresponding cover image, which degrades the imperceptibility of the secret information. However, the anti-jamming performance would be optimized because of the larger judgment threshold used for information extraction. In general, it is necessary to balance the relationship between the imperceptibility and anti-interference performance according to the requirements for different applications. Then, the appropriate region adjustment parameter could be found out.

Assuming that CR was set to 0.7 for measurement and zero-mean AWGN with standard deviation of 2/4/6 existed in the channel, experiments were conducted with different region adjustment parameters to verify the theoretical analysis mentioned above. As shown in Figure 9, the larger parameter  $\alpha$  correlated with better anti-interference performance and worse imperceptibility. Moreover, the environment with greater noise intensity would be related to the more obvious improvement in the anti-interference performance. Conversely, the smaller parameter  $\alpha$  would result in worse anti-interference performance and better imperceptibility. And, greater AWGN strength correlates with the more obvious improvement in the imperceptibility.



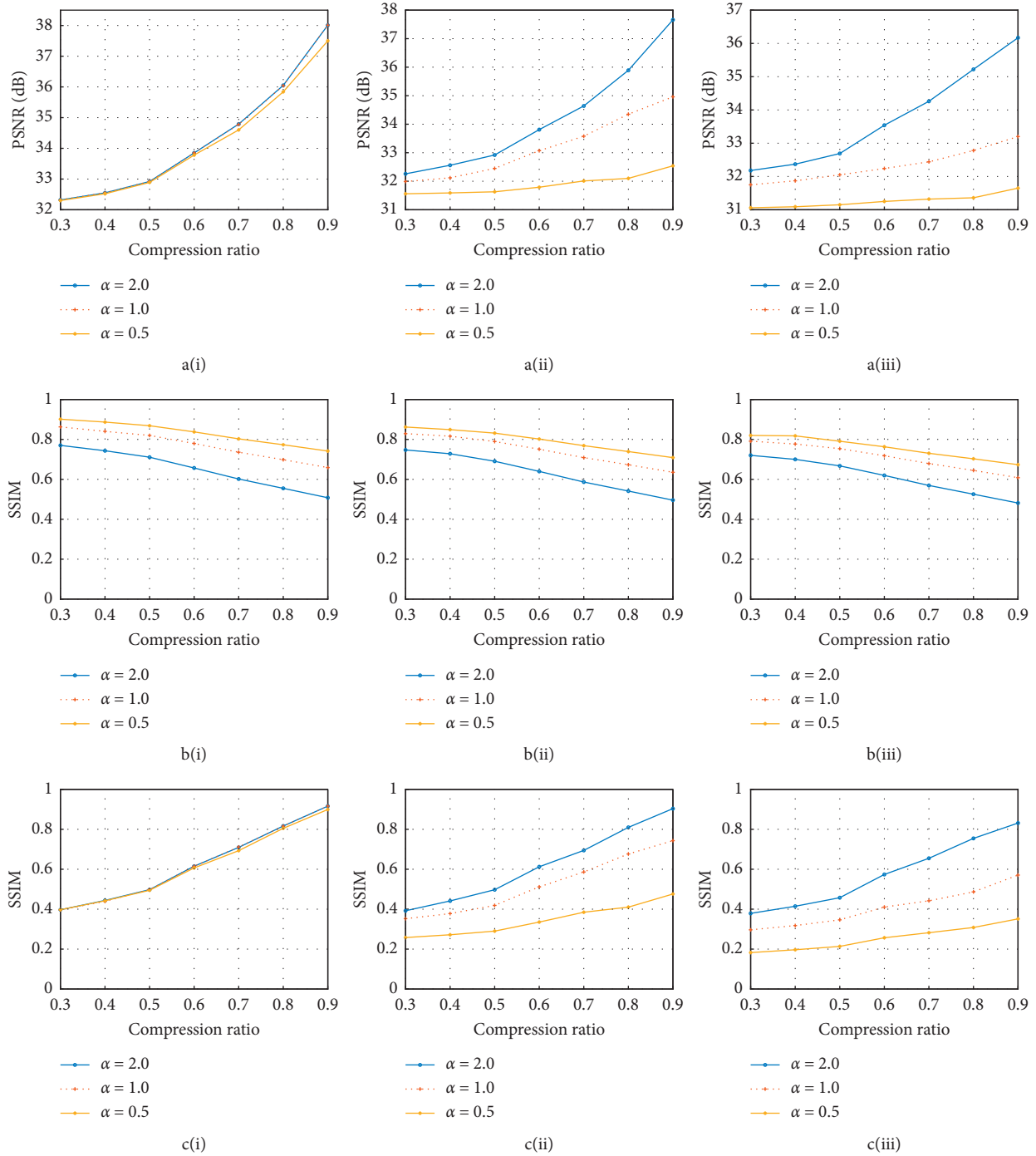


FIGURE 9: The reconstruction performance of ISS-PPEA with the channel containing AWGN. (a) The PSNR values of the reconstructed image with the channel containing zero-mean AWGN with standard deviations of (i) 2, (ii) 4, or (iii) 6. (b) The SSIM values of the stego image and the cover image with the channel containing zero-mean AWGN with standard deviations of (i) 2, (ii) 4, or (iii) 6. (c) The SSIM values of the reconstructed image and the original scene with the channel containing zero-mean AWGN with standard deviations of (i) 2, (ii) 4, or (iii) 6.

### 6. Anti-Interference Performance

In the steganography applications based on the WWSN structure, the data transmitted in the wireless channel is not only easy to be affected by various kinds of interference but also easy to be attacked by hackers artificially. To obtain most

of the scene information captured by the sensor node, the requirements for anti-interference performance of the system must be taken seriously. Most current schemes hid secret information into the LSB of the cover images in the spatial domain or into the coefficients of the high-frequency band of the cover images in the transformational domain.

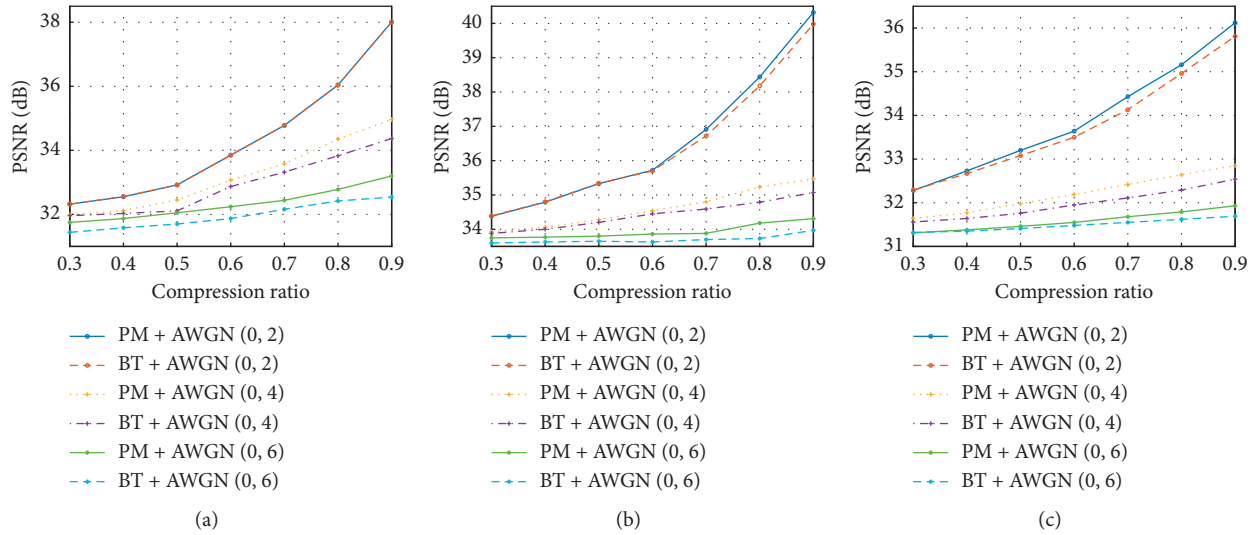


FIGURE 10: The PSNR values of the reconstructed image under AWGN interference of different intensities for PM and BT. (a) The cover image is Baboon, and the scene is Bridge. (b) The cover image is Barbara, and the scene is Couple. (c) The cover image is Pepper, and the scene is Lena.

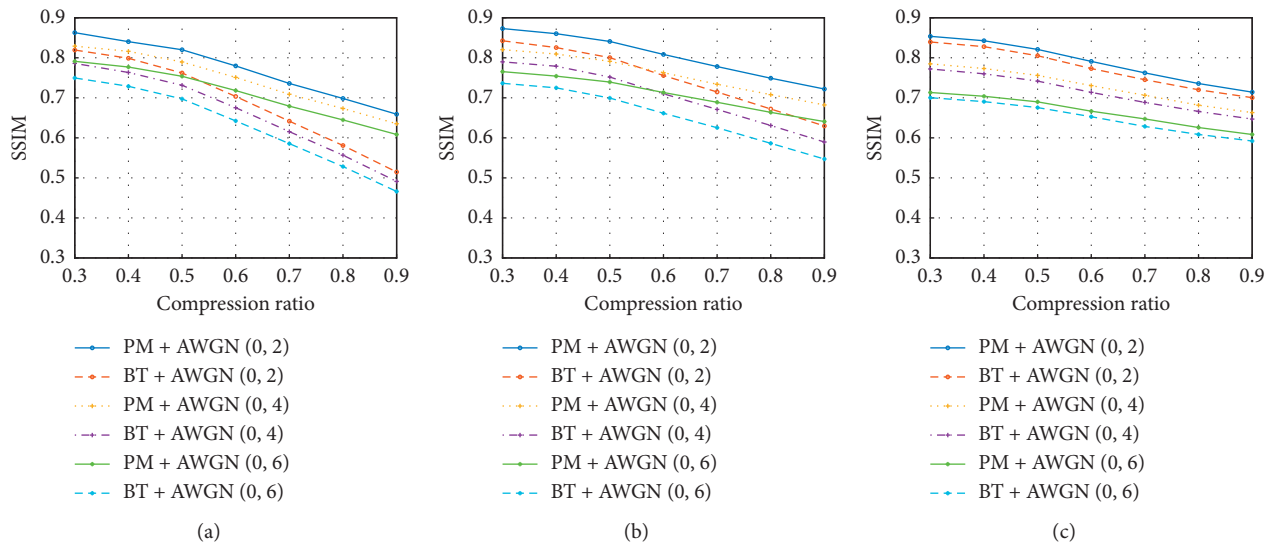


FIGURE 11: The SSIM values of the stego image and cover image under AWGN interference of different intensities for PM and BT. (a) The cover image is Baboon, and the scene is Bridge. (b) The cover image is Barbara, and the scene is Couple. (c) The cover image is Pepper, and the scene is Lena.

These methods are unable to meet the specific requirements of WWSN. Therefore, this paper proposed to hide the measurement results of the scenes into the medium-frequency DCT coefficients of the cover image bitwise randomly, which is surely beneficial to reduce the influence of AWGN and improve the anti-interference performance of the system. Because ISS-PPEA involves the entire structure of IEA-CS-NQ, the reconstruction accuracy in front of occlusion would not be worse than that in the existing literatures. Since the designed embedding algorithm has

little effect on the image reconstruction ability in the case of data loss, this section would merely evaluate the system performance under AWGN interference.

By comparing ISS-PPEA with the similar embedding method proposed by Poljicak et al. [19], it could be found that

- (1) In the scheme proposed by Poljicak, the binarization treatment for the coefficients selected by the embedding operation was carried out on the basis of the average of the medium-frequency DCT coefficient,

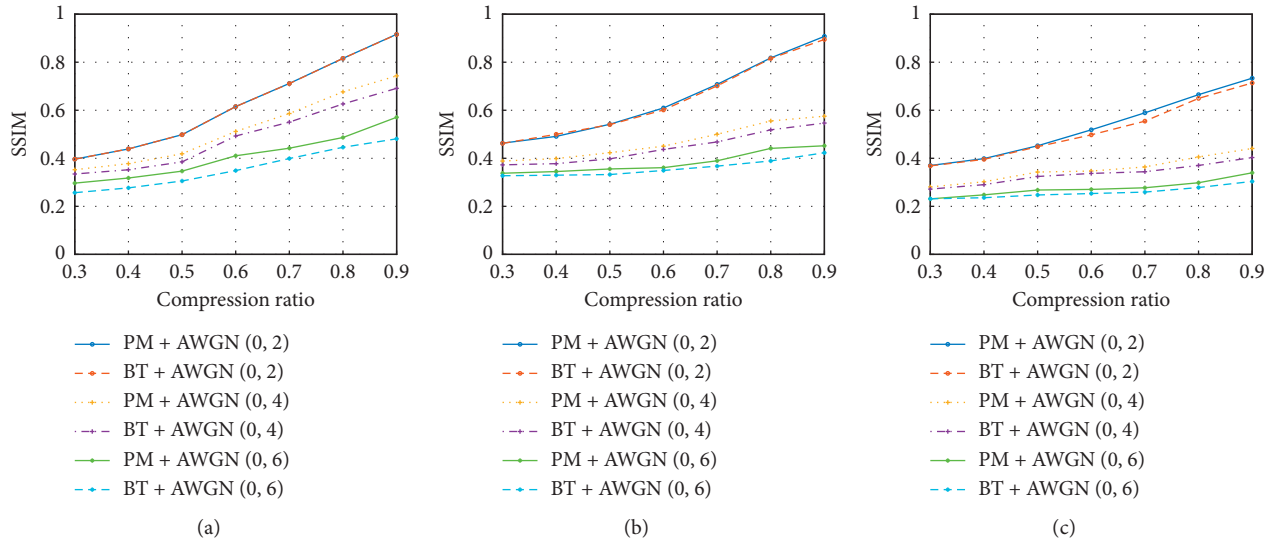


FIGURE 12: The SSIM values of the reconstructed image and scene under AWGN interference of different intensities for PM and BT. (a) The cover image is Baboon, and the scene is Bridge. (b) The cover image is Barbara, and the scene is Couple. (c) The cover image is Pepper, and the scene is Lena.

which significantly affected the SSIM for the stego image and the cover image. In ISS-PPEA, the coefficients chosen by the embedding operation are modified by the partial preservation treatment method described in equations (7) and (8) based on the region adjustment parameter according to specific requirements for applications. It could sharply reduce the number of DCT coefficients that have to be changed in the hiding process. Indeed, ISS-PPEA could help to improve the SSIM and imperceptibility.

- (2) According to the embedding method described in equations (7) and (8), the proposed scheme could make the revised coefficients have regional distribution. That is to say, compared with the binarization treatment method designed in [19], the absolute value of stego coefficients in ISS-PPEA is larger, and the probability of misjudgement in the process of extracting sign is surely lower for the same AWGN. In other words, ISS-PPEA could improve the accuracy of information reconstruction.

Several groups of standard images were applied to verify the theoretical analysis mentioned above. The designed steganography scheme based on the partial preservation treatment was compared with the available scheme based on the binarization treatment by assuming that zero-mean AWGN with standard deviations of 2/4/6 existed in the channel. The results are drawn in Figures 10–12. It is worth mentioning that the symbols PM and BT are taken as the abbreviations for the proposed partial preservation treatment method and the available binarization treatment method, respectively. As shown in Figure 10, with AWGN interference of different intensities, the reconstruction result of the proposed scheme is more accurate. Moreover, the higher the noise intensity is, the more obvious the improvement of PSNR would be. According to Figure 11, the

designed scheme significantly boosts the SSIM value for the stego image and the cover image. It means that the imperceptibility of secret information has been improved by the proposed method. Figure 12 shows that ISS-PPEA contributes to enhance the structural similarity of the reconstructed image and scene information. It should be noted that although the PSNR and SSIM values shown in Figures 10–12 were quite small, this would not affect the correctness of the experimental results and conclusions. In practice, it is easy to choose a better reconstruction algorithm to improve the performance of the reconstruction.

As mentioned above, the ISS-PPEA designed by this paper could improve the reconstruction precision for the scene information under noisy environment, comparing with current schemes based on hiding secret data in the LSB of the cover image in the spatial domain or embedding data into the coefficients of the high-frequency band in the transformational domain. When comparing with the binarization embedding treatment method designed in the literature [19], the partial preservation scheme is better at improving the imperceptibility and reconstruction accuracy of scene information, which is equivalent to improving the anti-interference performance.

## 7. Efficiency

The operating efficiency of the image steganography system based on the partial preservation embedding algorithm would be evaluated from the aspects of time complexity, space complexity, information embedding rate, communication efficiency, and system consumption in this part.

**7.1. Time and Space Complexity.** Suppose the size of the cover image is  $\sqrt{n_1} \times \sqrt{n_1}$ . According to the system framework shown in Figure 1, the size of objects and results

of DCT/IDCT operation is still  $\sqrt{n_1} \times \sqrt{n_1}$ . Therefore, the time and space complexity of the proposed system are both  $O(n_1)$ , equal to the existing schemes.

**7.2. Information Embedding Rate and Communication Efficiency.** For image steganography systems, the information embedding rate is defined as the ratio of the information amount in the confidential scene to the cover image. And, the communication efficiency could be considered as the ratio of the data volume in the scene to be hidden and the stego image transmitted in the channel.

Indeed, the information embedding rate of the system is closely related to the information embedding method, while the communication efficiency is connected with the compression ratio during the measurement operation in CS. Suppose the size of the cover image is  $\sqrt{n_1} \times \sqrt{n_1}$ , the size of the scene is  $\sqrt{n_2} \times \sqrt{n_2}$ , and the compression ratio during measurement is 1. According to the definition that the medium-frequency DCT coefficients occupy 50% space of the cover image, the proposed system could work normally as long as the condition  $n_1/16 \geq n_2$  is met. Therefore, the maximum embedding capacity of the steganography system is  $n_1/2$  bits, and the maximum embedding rate of information is  $6.25\% ((n_1/16)/n_1)$ . Since the communication efficiency is  $n_2/n_1$ , the communication efficiency would be the maximum value of 6.25% if  $n_2 = n_1/16$ . In addition, if the compression ratio is less than 1, the communication efficiency of the system would be improved accordingly.

**7.3. System Consumption.** According to the scheme designed in Figure 1, a sensor node only needs to complete the work of scene information acquisition, encryption, and embedding, which corresponds with limited consumption requirements. Reconstruction is confined to the terminal user node with powerful hardware for its difficulty. Therefore, it can be considered that the image steganography scheme designed by this paper is very suitable for the applications with WWSN architecture.

## 8. Conclusions

The key technical problems of available image steganography schemes employed by applications with the structure of WWSN were firstly analysed in this paper. It was found that the performance of existing systems in the hostile environment was unsatisfactory. Besides, the current solutions based on the medium-frequency band in the transformational domain of the cover image have greatly affected the SSIM of the stego image and cover image. Thus, to settle these problems, an image steganography scheme based on PPEA is proposed in this paper. Theoretical analysis and simulation results have proved that the designed scheme possesses the following advantages:

- (1) Due to IEA-CS-NQ being taken as part of the proposed scheme, it could be considered that the proposed ISS-PPEA inherits its advantages of high-

level encryption efficiency and the ability to resist all kinds of attacks including CPA

- (2) Comparing with existing schemes of embedding scene information into LSB in the spatial domain or hiding it to the high-frequency band in the transformational domain, the proposed scheme has better performance in the hostile communication environment
- (3) The designed PPEA performs better in terms of optimizing the imperceptibility and boosting the reconstruction accuracy of the original scene information, when making a comparison with the existing method proposed by Poljicak et al. [19]
- (4) The proposed scheme could adapt to different performance requirements in various applications by setting region adjustment parameters, which ensures its practical value

## Data Availability

The simulation results used to support the findings of this study are included within this article.

## Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

## Acknowledgments

This work was supported by the Youth Program of National Natural Science Foundation of China (31700478).

## References

- [1] S. Y. Chen and T. Y. Tsou, "Compressive sensing-based adaptive top-k query over compression domain in wireless sensor networks," in *Proceedings of the 2017 IEEE Wireless Communications and Networking Conference*, pp. 1–6, San Francisco, CA, USA, May 2017.
- [2] S. A. Unde and P. P. Deepthi, "Design and analysis of compressive sensing based lightweight encryption scheme for multimedia IoT," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 67, Article ID 2897839, 2019.
- [3] Y. Zhang, L. Y. Zhang, J. Zhou, L. Liu, F. Chen, and X. He, "A review of compressive sensing in information security field," *IEEE Access*, vol. 4, no. 4, pp. 2507–2519, 2016.
- [4] L. Chen, B. Ma, X. Zhao, and S. Wang, "Differential cryptanalysis of a novel image encryption algorithm based on chaos and Line map," *Nonlinear Dynamics*, vol. 87, no. 3, pp. 1797–1807, 2017.
- [5] M. Saidi, H. Hermassi, R. Rhouma, and S. Belghith, "A new adaptive image steganography scheme based on DCT and chaotic map," *Multimedia Tools and Applications*, vol. 76, no. 11, pp. 13493–13510, 2017.
- [6] R.-Z. Wang, C.-F. Lin, and J.-C. Lin, "Image hiding by optimal LSB substitution and genetic algorithm," *Pattern Recognition*, vol. 34, no. 3, pp. 671–683, 2001.
- [7] P. Tsai, Y.-C. Hu, and H.-L. Yeh, "Reversible image hiding scheme using predictive coding and histogram shifting," *Signal Processing*, vol. 89, no. 6, pp. 1129–1143, 2009.

- [8] C.-C. Chang, M.-H. Lin, and Y.-C. Hu, "A fast and secure image hiding scheme based on LSB substitution," *International Journal of Pattern Recognition and Artificial Intelligence*, vol. 16, no. 4, pp. 399–416, 2002.
- [9] Y.-H. Yu, C.-C. Chang, and L.-C. Lin, "A new steganographic method for color and grayscale image hiding," *Computer Vision and Image Understanding*, vol. 107, no. 3, pp. 183–194, 2007.
- [10] M. Li, L. Wang, J. Fan, Y. Zhang, K. Zhou, and H. Fan, "Fidelity preserved data hiding in encrypted highly auto-correlated data based on homomorphism and compressive sensing," *IEEE Access*, vol. 7, no. 1, pp. 69808–69825, 2019.
- [11] X. Zhang, F. Peng, and M. Long, "Robust coverless image steganography based on DCT and LDA topic classification," *IEEE Transactions on Multimedia*, vol. 20, no. 12, pp. 3223–3238, 2018.
- [12] S. W. Sari, E. H. Rachmawanto, and A. C. Sari, "A good performance OTP encryption image based on DCT-DWT steganography," *Telkomnika*, vol. 15, no. 4, pp. 1987–1995, 2017.
- [13] C.-K. Chan and L. M. Cheng, "Hiding data in images by simple LSB substitution," *Pattern Recognition*, vol. 37, no. 3, pp. 469–474, 2004.
- [14] C.-H. Yang, C.-Y. Weng, S.-J. Wang, and H.-M. Sun, "Adaptive data hiding in edge areas of images with spatial LSB domain systems," *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 3, pp. 488–497, 2008.
- [15] A. S. El-Rahman, "A comparative analysis of image steganography based on DCT algorithm and steganography tool to hide nuclear reactors confidential information," *Computers & Electrical Engineering*, vol. 70, no. 1, pp. 380–399, 2018.
- [16] B. Hu, L. Li, J. Qian et al., "Perceptual evaluation of compressive sensing image recovery," in *Proceedings of the 2016 Eighth International Conference on Quality of Multimedia Experience (QoMEX)*, pp. 1–6, Lisbon, Portugal, June 2016.
- [17] M. Li, D. Xiao, and Y. Zhang, "Reversible data hiding in block compressed sensing images," *ETRI Journal*, vol. 38, no. 1, pp. 159–163, 2016.
- [18] X. Chai, Z. Gan, Y. Chen et al., "A visually secure image encryption scheme based on compressive sensing," *Signal Processing*, vol. 1, no. 134, pp. 35–51, 2016.
- [19] A. Poljicak, G. Botella, C. Garcia, L. Kedmenec, and M. Prieto-Matias, "Portable real-time DCT-based steganography using OpenCL," *Journal of Real-Time Image Processing*, vol. 14, no. 1, pp. 87–99, 2018.
- [20] Q. Shen, W. Liu, Y. Lin et al., "Designing an image encryption scheme based on compressive sensing and non-uniform quantization for wireless visual sensor networks," *Sensors*, vol. 19, no. 14, Article ID 3081, 2019.
- [21] E. Barker and A. Roginsky, *Recommendation for the Transitioning of Cryptographic Algorithms and Key Sizes*, NIST Special Publication, Princeton, NJ, USA, 2010pp. 800–131, CiteSeerx.
- [22] Q. Shen and W. Liu, "A novel digital image encryption algorithm based on orbit variation of phase diagram," *International Journal of Bifurcation and Chaos*, vol. 27, no. 13, Article ID 1750204, 2017.