Lecture Notes in Electrical Engineering 789

N. R. Shetty · L. M. Patnaik ·
H. C. Nagaraj · Prasad N. Hamsavath ·
N. Nalini *Editors*

Emerging Research in Computing, Information, Communication and Applications

ERCICA 2020, Volume 1

Springer

Lecture Notes in Electrical Engineering

Volume 789

Series Editors

Leopoldo Angrisani, Department of Electrical and Information Technologies Engineering, University of Napoli Federico II, Naples, Italy
Marco Arteaga, Departament de Control y Robótica, Universidad Nacional Autónoma de México, Coyoacán, Mexico
Bijaya Ketan Panigrahi, Electrical Engineering, Indian Institute of Technology Delhi, New Delhi, Delhi, India
Samarjit Chakraborty, Fakultät für Elektrotechnik und Informationstechnik, TU München, Munich, Germany
Jiming Chen, Zhejiang University, Hangzhou, Zhejiang, China
Shanben Chen, Materials Science and Engineering, Shanghai Jiao Tong University, Shanghai, China
Tan Kay Chen, Department of Electrical and Computer Engineering, National University of Singapore, Singapore, Singapore
Rüdiger Dillmann, Humanoids and Intelligent Systems Laboratory, Karlsruhe Institute for Technology, Karlsruhe, Germany
Haibin Duan, Beijing University of Aeronautics and Astronautics, Beijing, China
Gianluigi Ferrari, Università di Parma, Parma, Italy
Manuel Ferre, Centre for Automation and Robotics CAR (UPM-CSIC), Universidad Politécnica de Madrid, Madrid, Spain
Sandra Hirche, Department of Electrical Engineering and Information Science, Technische Universität München, Munich, Germany
Faryar Jabbari, Department of Mechanical and Aerospace Engineering, University of California, Irvine, CA, USA
Limin Jia, State Key Laboratory of Rail Traffic Control and Safety, Beijing Jiaotong University, Beijing, China
Janusz Kacprzyk, Systems Research Institute, Polish Academy of Sciences, Warsaw, Poland
Alaa Khamis, German University in Egypt El Tagamoa El Khames, New Cairo City, Egypt
Torsten Kroeger, Stanford University, Stanford, CA, USA
Yong Li, Hunan University, Changsha, Hunan, China
Qilian Liang, Department of Electrical Engineering, University of Texas at Arlington, Arlington, TX, USA
Ferran Martín, Departament d’Enginyeria Electrònica, Universitat Autònoma de Barcelona, Bellaterra, Barcelona, Spain
Tan Cher Ming, College of Engineering, Nanyang Technological University, Singapore, Singapore
Wolfgang Minker, Institute of Information Technology, University of Ulm, Ulm, Germany
Pradeep Misra, Department of Electrical Engineering, Wright State University, Dayton, OH, USA
Sebastian Möller, Quality and Usability Laboratory, TU Berlin, Berlin, Germany
Subhas Mukhopadhyay, School of Engineering & Advanced Technology, Massey University, Palmerston North, Manawatu-Wanganui, New Zealand
Cun-Zheng Ning, Electrical Engineering, Arizona State University, Tempe, AZ, USA
Toyoaki Nishida, Graduate School of Informatics, Kyoto University, Kyoto, Japan
Federica Pascucci, Dipartimento di Ingegneria, Università degli Studi “Roma Tre”, Rome, Italy
Yong Qin, State Key Laboratory of Rail Traffic Control and Safety, Beijing Jiaotong University, Beijing, China
Gan Woon Seng, School of Electrical & Electronic Engineering, Nanyang Technological University, Singapore, Singapore
Joachim Speidel, Institute of Telecommunications, Universität Stuttgart, Stuttgart, Germany
Germano Veiga, Campus da FEUP, INESC Porto, Porto, Portugal
Haitao Wu, Academy of Opto-electronics, Chinese Academy of Sciences, Beijing, China
Walter Zamboni, DIEM - Università degli studi di Salerno, Fisciano, Salerno, Italy
Junjie James Zhang, Charlotte, NC, USA

The book series *Lecture Notes in Electrical Engineering* (LNEE) publishes the latest developments in Electrical Engineering - quickly, informally and in high quality. While original research reported in proceedings and monographs has traditionally formed the core of LNEE, we also encourage authors to submit books devoted to supporting student education and professional training in the various fields and applications areas of electrical engineering. The series cover classical and emerging topics concerning:

- Communication Engineering, Information Theory and Networks
- Electronics Engineering and Microelectronics
- Signal, Image and Speech Processing
- Wireless and Mobile Communication
- Circuits and Systems
- Energy Systems, Power Electronics and Electrical Machines
- Electro-optical Engineering
- Instrumentation Engineering
- Avionics Engineering
- Control Systems
- Internet-of-Things and Cybersecurity
- Biomedical Devices, MEMS and NEMS

For general information about this book series, comments or suggestions, please contact leontina.dicecco@springer.com.

To submit a proposal or request further information, please contact the Publishing Editor in your country:

China

Jasmine Dou, Editor (jasmine.dou@springer.com)

India, Japan, Rest of Asia

Swati Meherishi, Editorial Director (Swati.Meherishi@springer.com)

Southeast Asia, Australia, New Zealand

Ramesh Nath Premnath, Editor (ramesh.premnath@springernature.com)

USA, Canada:

Michael Luby, Senior Editor (michael.luby@springer.com)

All other Countries:

Leontina Di Cecco, Senior Editor (leontina.dicecco@springer.com)

**** This series is indexed by EI Compendex and Scopus databases. ****

More information about this series at http://www.springer.com/series/7818

N. R. Shetty · L. M. Patnaik · H. C. Nagaraj ·
Prasad N. Hamsavath · N. Nalini
Editors

Emerging Research in Computing, Information, Communication and Applications

ERCICA 2020, Volume 1

Springer

Editors
N. R. Shetty
Nitte Meenakshi Institute of Technology
Bengaluru, Karnataka, India

L. M. Patnaik
National Institute of Advanced Studies
Bengaluru, Karnataka, India

H. C. Nagaraj
Nitte Meenakshi Institute of Technology
Bengaluru, Karnataka, India

Prasad N. Hamsavath
Nitte Meenakshi Institute of Technology
Bengaluru, Karnataka, India

N. Nalini
Nitte Meenakshi Institute of Technology
Bengaluru, Karnataka, India

ISSN 1876-1100 ISSN 1876-1119 (electronic)
Lecture Notes in Electrical Engineering
ISBN 978-981-16-1337-1 ISBN 978-981-16-1338-8 (eBook)
https://doi.org/10.1007/978-981-16-1338-8

© The Editor(s) (if applicable) and The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022
This work is subject to copyright. All rights are solely and exclusively licensed by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.
The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.
The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Singapore Pte Ltd.
The registered company address is: 152 Beach Road, #21-01/04 Gateway East, Singapore 189721, Singapore

Contents

About the Editors

Prof. N. R. Shetty is Chancellor of Central University of Karnataka, Kalaburagi, and Chairman of the Review Commission for the State Private University Karnataka. He is currently serving as an advisor to the Nitte Meenakshi Institute of Technology (NMIT), Bengaluru. He is also Founder Vice-President of the International Federation of Engineering Education Societies (IFEES), Washington DC, USA. He served as Vice Chancellor of Bangalore University for two terms and President of the ISTE, New Delhi three terms. He was also Member of the Executive Committee of the AICTE and Chairman of its South West Region Committee.

Prof. L. M. Patnaik obtained his Ph.D. in 1978 in the area of Real-Time Systems and D.Sc. in 1989 in the areas of Computer Systems and Architectures, both from the Indian Institute of Science (IISc), Bengaluru. During March 2008 to August 2011, he was Vice Chancellor, Defence Institute of Advanced Technology, Deemed University, Pune. Currently, he is Honorary Professor with the Department of Electronic Systems Engineering, Indian Institute of Science, Bengaluru, and INSA Senior Scientist and Adjunct Professor with the National Institute of Advanced Studies, Bengaluru. During the last 50 years of his long service, his teaching, research, and development interests have been in the areas of parallel and distributed computing, computer architecture, CAD of VLSI systems, high-performance computing, mobile computing, theoretical computer science, real-time systems, soft computing and computational neuroscience including machine cognition. In these areas, he has 1286 publications in refereed international journals and refereed international conference proceedings including 30 technical reports, 43 books and 26 chapters in books.

Dr. H. C. Nagaraj was born on 4th April, 1959 in Bengaluru. He obtained his B.E. Degree in Electronics and Communication Engineering securing first class with distinction from the University of Mysore in 1981. He obtained his M.E. in Communication Systems from P. S. G. College of Technology, Coimbatore, Bharathiyar University in 1984 and secured first rank. He got his doctoral degree in the area of

Biomedical Signal Processing and Instrumentation from Indian Institute of Technology Madras, Chennai in 2000. He assumed charge as Principal, Nitte Meenakshi Institute of Technology, Bengaluru in September 2003 and till date he is serving as Principal. He has about 38 years of experience in teaching, research and administration. During his term as Principal in NMIT, Bengaluru, the institution has been conferred with Autonomous Status by the Visvesvaraya Technological University, Government of Karnataka and UGC, New Delhi; accredited by the National Assessment and Accreditation Council, National Board of Accreditation, AICTE, New Delhi for UG programmes, and a pico satellite weighing less than 1 kg was designed and fabricated and handed over to ISRO and was launched on 12th July 2010 from Sriharikota, Andhra Pradesh, India. Dr. H. C. Nagaraj has published a number of papers in National and International Journals, Conferences and delivered invited talks in the field of Biomedical Signal Processing, Image Processing, Mobile Communication etc. He got the Best Paper Award in the National Conference of Biomechanics held during February 22–24, 1996 at IIT Madras. He was awarded the Best Paper Award at State Level Seminar on “Introduction of Flexible System in Technical Education” held by the Government of Karnataka during February 1999 in Bengaluru. He has guided several students for their Ph.D. programmes and written a book titled *VLSI Circuits* published in 2006 for B.E. Students. He is a member of expert teams visiting various colleges for accreditation by NAAC and affiliation of UG, PG and Ph.D. programmes under Electronics and Communication, Biomedical Engineering Streams, on behalf Institution of Engineers, Visvesvaraya Technological University, Belgaum and Kuvempu University, Shimoga. He is a Fellow of the Institution of Electronics and Telecommunication Engineers (IETE), Life member of ISTE, Life Member of Biomedical Engineering Society of India and Member of Global Engineering Deans Council India Chapter (GEDCIC). Dr. Nagaraj has visited countries like USA, Canada, UK, Singapore, Malaysia, South Korea, Hungary etc. in connection with collaboration for academic activities. Presently, he is the Member of the Academic Senate at Visvesvaraya Technological University (VTU), Belagavi. He is also the Member of Court at Pondicherry University and Member of Expert Team for the evaluation of R&D projects funded by VTU.

Dr. Prasad N. Hamsavath is currently working as Professor and Head of the Department of Master of Computer Applications at Nitte Meenakshi Institute of Technology, Bengaluru. He completed his Ph.D. at Jawaharlal Nehru University, New Delhi, India. Dr. Prasad has more than 12 years of experience in different roles in both public and private sector enterprises, including the Ministry of Human Resource and Development, New Delhi, Government of India. He has received the prestigious “Dr. Abdul Kalam Life Time Achievement Award” and also received a “Young Faculty” award at the 2nd Academic Brilliance Awards.

Dr. N. Nalini is currently working as Professor at the Department of Computer Science and Engineering at Nitte Meenakshi Institute of Technology, Bengaluru. She received her M.S. from BITS, Pilani, in 1999, and her Ph.D. from Visvesvaraya

Technological University in 2007. She has more than 17 years of teaching and 10 years of research experience. She has several international publications to her credit, and has received the "Bharath Jyothi Award" by Dr. Bhishma Narain Singh, Former Governor of Tamil Nadu and Assam, given out by the India International Friendship Society. She is Lifetime Member of the ISTE, CSI, ACEEE and IIFS.

Design of a Secure Blockchain Based Privacy Preserving Electronic Voting System

R. Shashidhara, M. Indushree, and N. S. Sneha

1 Introduction

Voting is the foundation of any successful democracy and must therefore be accessible and secure for all eligible citizens in the country. Several Electoral systems take on to permit citizens to cast their precious vote, which includes electronic methods, ballot based voting and Electronic Voting Machine (EVM). However, we argue that existing techniques for voting, based on electronic voting machines, provides mistrust kind of transparency to voters. The issue commonly known as voter confidence. The Voting Systems have to heighten privacy and secrecy to provide electoral services available to the voters but secured against security vulnerabilities like keeping the voter ballot from being modified with the impact of changing casted votes by the voter. Several voting machines depends on Tor to provide anonymity of voters. Nevertheless, this mechanism doesn't achieve voter privacy and integrity services. Because, most of the intelligence authorities in the world is controlled by various parts of the Internet, which leads attackers to eavesdrop votes. As a result, as an alternative of move back to an inefficient and traditional mechanisms, the modernization of state structure by the make use of emerging technology like Blockchain [9].

Blockchain is a digital public ledger that records online transactions. Blockchain ensure security services like confidentiality, integrity, privacy by encrypting and

R. Shashidhara (✉) · M. Indushree
School of Engineering and Applied Sciences, Bennett University, Greater Noida, Uttar Pradesh, India

M. Indushree
e-mail: E20SOE815@bennett.edu.in

N. S. Sneha
Department of Computer Science and Engineering, Shri Madhwa Vadiraja Institute of Technology and Management, Udupi 574115, Karnataka, India
e-mail: snehans.cs@sode-edu.in

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

N. R. Shetty et al. (eds.), *Emerging Research in Computing, Information, Communication and Applications*, Lecture Notes in Electrical Engineering 789,
https://doi.org/10.1007/978-981-16-1338-8_1

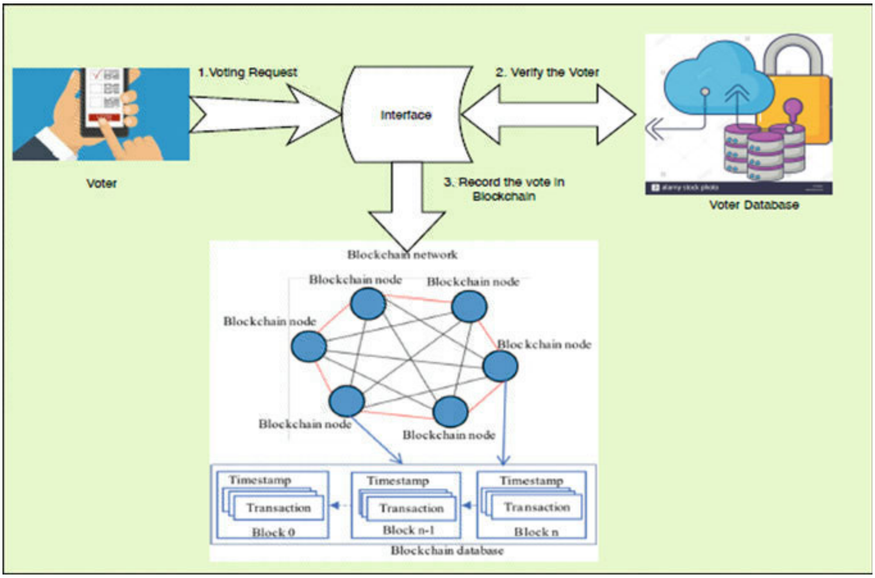


Fig. 1 The scenario of blockchain based E-Voting system

validating the transactions. In the Blockchain, when new block is added it will be connected to the last block using a cryptography hash produced from the information of the previous block, which assure that the chain in the blockchain is never broken and blocks are permanently stored. Further, it is highly impossible to modify previous transactions. Because, all the adjacent blocks must be modified first. This fundamental aspect of Blockchain is what makes the technology tamper-proof and secure. The scenario of Blockchain based E-Voting system is depicted in Fig. 1.

1.1 Motivations

Controversial E-Voting could have been avoided if the election and counting process is transparent, verifiable and secure. The existing voting system does offer voter privacy and even the vote counting by the officials is also not transparent. The voters are supposed to trust the result which is provided by the government body or Election Commission. There are also other electoral flaws like ballot stuffing, voter fraud and booth capturing. These issues makes difficult for election commission to differentiate between real votes and votes added without proper authentication and authorization. Some of the problems in current Electoral process are listed below:

1. Designing a secure electronic voting system that offers the transparency, privacy and fairness has been a challenging.

2. Current E-Voting protocols require a centralized authority to monitor and control the whole procedure from ballot to results.
3. The centralized systems are vulnerable to security attacks like Distributed Denial-Of-Service (DDOS).
4. Intelligence agencies have access to network and sufficient computing resources to analyze voting informative for the potential modification.

1.2 Research Contributions

1. Designing a secure and decentralized Blockchain based E-Voting system using smart contracts (Chain code).
2. A user credential model will be proposed to ensure authentication, authorization and non-repudiation services.
3. The voter can cast a vote using private key, after that transaction will be recorded in the decentralized Blockchain network.
4. With help of voter Ethereum address, he/she can verify the casted vote in the later stages.
5. Further, candidate count with details, Vote Count and winning proposal is implemented using smart contracts and deployed in Blockchain network.

1.3 Structure of the Article

The rest of the article is structured as follows: Sect. 2, covers background, it includes challenges of the E-Voting and Blockchain. Section 3, defines the security requirements of E-Voting. Section 4, describes the proposed Blockchain based E-Voting protocol. Section 5, provides the implementation details with the experimental results and provides a performance analysis of the proposed work. Section 6, concludes the article.

2 Background

Mistrust in the E-Voting process is a common circumstance even in the developed countries. To ensure the transparency and security, that can be implemented in Blockchain based E-voting system. This could helps in solving most of the issues being faced in the voting process.

The concept of E-voting was initiated in 2001 at Estonia. They use digital smart cards for identification and authentication. For voters to attain the voting process by displaying contestants and start casting the votes through portal in the web as well as similar desktop application. In this regard, anyone having the smart device with

Internet connection and ID card by the government, can easily vote from anywhere [5].

The E-voting is based on centralized solution have a single point of failure, which leads to security attacks and vulnerabilities. In this context, Denial of Service, Man-In-The-Middle and insider attacks could crash the centralized databases and servers. The admins of the systems could act malicious and manipulate the information [2].

Brennan Center for Justice in 2015 identified the security vulnerabilities in America voting machines and published in the news. The study identified that, 43 out of 50 US states used Electronic Voting Machines (EVM) that are old voting equipment's, exposed to crashes and failures. Further, the EVMs also easy to crack and modify with [8].

Zhao et al. presented an E-voting scheme, which proposes the reward and penalty based protocol for safe or unsafe conduct of voters. Notably, this is a first Blockchain based voting system [7]. Additionally, in 2016, Lee et al. introduced the voting scheme, which includes a trust third party using Blockchain to ensure choice of the voters. Although, the authors Bistarelli et al. presented an E-voting system, which partitions the voting process into two different parts called authentication and Distribution Server using token to safeguard privacy of the voters. Nevertheless, still there are some problems in this E-Voting scheme [1]. This system have been used in the countries like Ireland, Norway and Estonias [3]. Recently, there have been scenarios where it was faced several issues like transparency, fairness and not completely hygienic, which can be identified in countries like Brazil, Nigeria, India, Bangladesh and Pakistan [4, 6]. Notably, The issues causing the mistrust in the voting process are listed in Table 1.

Table 1 Nature of problems causing mistrust in the E-Voting process

Issues	Description
Casting duplicate votes	If there is no proper authentication and authorization, it is possible to cast again for the ones who have not voted
Pre-poll rigging	In few places the polling stations are made too far and voters have no interest or refuse to vote
Use of power to influence	The use of power to influence the voters or polling staff either by threats or by incentives based
Lack of interest by public	Voters are not fully trusted and convinced with current voting system. These issues can be dealt with trustworthy E-Voting platforms like Blockchain
Unsupervised vote counting	For the parties who do not have a strong representation in a region, it is likely their votes can be miscounted
Lack of audit and appeals	The process of hearing and deciding the appeals on some issues is slow that can be finalized before the next elections

3 Security Requirements for E-Voting

The proposed Blockchain based E-voting protocol should satisfy the following security requirements:

1. Eligibility: The authorized voters should be allowed to participate in voting process and cast their vote only once in the election. Further, the system must validate the voter identities.
2. Voter Privacy: E-Voting protocol should not reveal the identities of the voter and not establish any links between identity information and ballots. Participants should remain anonymous and voting information is untraceable during and after the election.
3. Fairness: No election results should be leaked before completion of the election process. This ensures that the voters might not be affect by others in the voting process.
4. Verifiability: This security service assure that all entities in E-Voting should have the facility to verify whether the vote casted have been counted or not. Here, an individual verifiability gives the voter to verify that one's vote has been counted.
5. Forgiveness: The ability of the voter to modify ones vote after it has been cast.

4 Proposed System

The motive beyond the proposed mechanism is to have the Blockchain based system that satisfies the mentioned security requirements and goals. The proposed system has been designed to achieve the high degree of decentralization to create the system which the voter reign as the network of nodes.

The first transaction added to the blockchain will represent the genesis block. When a voter cast his/her vote, the transaction is updated in the Blockchain network. The proposed e-Voting protocol permit for the protest vote, where an user might be return the blank vote to the refusal of the election system or like NOTA to dissatisfaction with all candidates. The Blockchain is decentralized Peer-to-Peer network and cannot be immutable. Even there is no central point of failure. In order to ensure the security and trust, the current block will uses the previous block hash like the previous voters data. If any of the blocks are corrupted, modified then it will be effortless to trace out. Because, all blocks in the blockchain are linked to each other with previous hash and serves as chain. During voting in the Blockchain, the vote gets transmitted to the nodes on Blockchain network. After that the node adds vote to the decentralized network.

The proposed protocol consists of the following phases:

1. **Setup**: This is an initialization phase to obtain the private key and public key pair using asymmetric cryptosystem.

2. **Voter Authentication**: The user should logs to the system using the credentials. The protocol will authenticate the voter based on his/her identity information issued by the Election Commission. The E-voting system should verify and validate all information entered by the voter. If the verification is successful, the voter will be authenticated and authorized to cast the vote.
   The prototype for voter authentication is described below:
   - **(ID, PW)**: Enter the login details and link the node identity to the e-governance.
   - **(Credentials, node id, user-Info)**: The system of E-governance authenticates voter credentials.
3. **Casting a vote:** Voters should choose the candidates from list of contestants to cast their vote. The voter can cast the vote through a friendly user interface. The prototype for this phase is shown below:
   - **V = vote (ID of the voter, candidate selected).**
   - **Add (V, Chain)**, the Vote V is added to the Blockchain network.
   - Next, the updated Blockchain data is reacted in all the nodes.
   - **Vote (ID, user List, true)**: Finally, Voter field will be switched to vote.
4. **Formation of the Block:** Upon casting the vote by the voter will be recorded as a unconfirmed transaction in the Blockchain. The nodes in the Blockchain network will validate the casted vote based on consensus protocols.
5. **Sealing of Blocks:** The transactions are stored in the Blockchain, by the end of polling time all blocks in the network needs to be sealed by cryptographic hash (SHA-256) using nonce and merkle root. Once the electoral process is complete and the results have been published, then there is no significance for the Blockchain mining.
6. **Counting of votes:** We have implemented a mechanism to count the casted votes in a fair manner. Further, the proposed system supports the voter to check the casted vote is successfully counted during counting process or not. With help of the Ethereum address, a user can verify the status of the casted vote.
   The prototype for counting process is given below:
   - **Candidates = get Candidates (candidate List).**

   Receive the candidate details from E-Governance.
   - **Results = count (chain, candidates)**

   Here, vote counting process will be completed and winner will be identified based on the maximum number of votes.

5 Implementation and Experimental Evaluation

The proposed E-voting protocol is implemented using Ethereum platform called public Blockchain network. An Ethereum network provides a broader range of applications, with the power of smart contracts. Ethereum Blockchain consists of Ethereum nodes. The node is any device that is running the Ethereum protocol (blockchain). When we connect to the Ethereum protocol we are on the Ethereum Blockchain network. By running an Ethereum node we can connect to other nodes in the network, have direct access to the Blockchain, and even do things like mine blocks, send transactions, and deploy smart contracts. Many applications, that may normally require a web server, can be run through these smart contracts using Blockchain network. Hence, it is impossible to manipulate the transactions or smart contracts deployed in the Blockchain network.

After performing the transactions on Ethereum Blockchain network, the transaction fee is calculated in Gas, and paid for in Ether. The gas is the fuel of the Ethereum network, which is mainly used to conduct transactions, execute smart contracts and Launch Decentralized Applications (Dapps). The frequently used parameters in the Ethereum network are Gas, Gas price and Gas limit.

1. Ether (ETH) is the Ethereum network's native cryptocurrency, the second largest by market cap on the crypto market.
2. **Gas**: is the unit of calculation that indicates the fee for a particular action or transaction.
3. **Gas Limit**: is the maximum amount of Gas that a user is willing to pay for performing this action or confirming a transaction (a minimum of 21,000).
4. **Gas Price**: is the amount of Gwei that the user is willing to spend on each unit of Gas.

Additionally, we have set up a MetaMask wallet in order to perform the transacttions on Ethereum Blockchain network. MetaMask is just an Ethereum Browser and Ether wallet. It interacts with Ethereum Dapps and Smart Contracts without running a full Ethereum node. Furthermore, MetaMask supports to connect different Ethereum based Blockchain networks and possible to import the accounts from other accounts through private keys.

We have defined the E-voting protocol through smart contracts, which consists of programming code and stored on a Blockchain network, then it execute when certain terms and conditions are met. It is called smart because of its ability to verify and execute a contract without any help from third parties. The contract exists in the decentralized Blockchain network and contains all the terms of a particular agreement. The smart contracts are meant to provide accuracy, transparency, autonomy, security and standardization.

Smart contracts defined in solidity programming language is executed by the Ethereum nodes in the blockchain network in every 10 s, and its validated by at least by two other nodes in the blockchain network. After that, functions of contracts can be triggered and executed.

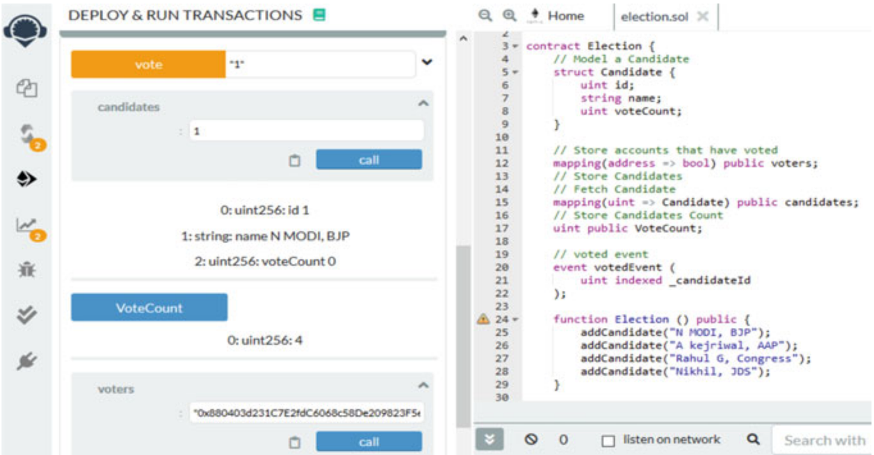


Fig. 2 Smart contract call and execution during E-Voting

The Candidate is defined as a struct, the state variables are ID, Name and VoteCount. We used solidity mapping for storing and fetching the voter details. ID is the wallet address associated with the voter account in the Ethereum Blockchain. The state variable VoteCount is used to count the number of votes received by the candidate.

Of the proposed protocol is evaluated by testing five ballots in the Ethereum Blockchain network. In this work, The E-Voting system scope is restricted for smaller elections and polls. The E-Voting with huge number of voters would require dynamic network structure and need to handle complex problems. The Blockchain networks scalability is still unknown. In addition, the proposed smart contracts are implemented using solidity using Ethereum platform. The wallet is supported in windows, Linux and mac machines. Furthermore, a voter who willing to cast their vote should the Ethers in his/her wallet to complete the voting transaction (Fig. 2).

6 Conclusion

In this article, a Blockchain based decentralized and peer-to-peer electronic voting protocol is proposed. The legitimate voters could have the power to vote through Internet by using smart devices like Mobiles, PCs, etc. The transaction will be recorded in the Blockchain network, which is verifiable, anonymous and adversaries are unable to modify the records in the network. The solidity smart contract is used to accomplish recording, managing, validating the voters during the electoral process. In order to provide the privacy and transparency of E-Voting protocol, secure cryptographic functions has been employed to ensure that the registration and voting is anonymous. The digital signatures using public key infrastructure makes the voting process more secure and reliable.

Further, the proposed protocol does not require mining like Bitcoin network since the voter's information is registered and authentic. Notably, the proposed approach addresses some of the security pitfalls that conventional E-voting protocols have. As a result of the proposed work, the concept of Blockchain technology, security algorithms and cryptographic primitives like hash functions, nonce and digital signatures, has become adaptable to elections and polls to secure the E-Voting environment.

References

1. Akbari E, Wu Q, Zhao W, Arabnia HR, Yang MQ (2017) From blockchain to internet based voting. In: 2017 international conference on computational science and computational intelligence (CSCI). IEEE, pp 218–221
2. Ayed AB (2017) A conceptual secure blockchain-based electronic voting system. Int J Netw Sec Appl 9(3):01–09
3. Batubara FR, Ubacht J, Janssen M (2018) Challenges of blockchain technology adoption for e-government: a systematic literature review. In: Proceedings of the 19th annual international conference on digital government research: governance in the data age, pp 1–9
4. Casino F, Dasaklis TK, Patsakis C (2019) A systematic literature review of blockchain-based applications: current status, classi_cation and open issues. Telematics Inform 36:55–81
5. Hanifatunnisa R, Rahardjo B (2017) Blockchain based e-voting recording system design. In: 2017 11th international conference on telecommunication systems services and applications (TSSA). IEEE, pp 1–6
6. Hsiao JH, Tso R, Chen CM, Wu ME (2017) Decentralized e-voting systems based on the blockchain technology. In: Advances in computer science and ubiquitous computing. Springer, pp 305–309
7. Johnson D (2019) Blockchain-based voting in the US and EU constitutional orders: a digital technology to secure democratic values? Eur J Risk Regul 10(2):330–358
8. Li J, Wang X, Huang Z, Wang L, Xiang Y (2019) Multi-level multi-secret sharing scheme for decentralized e-voting in cloud computing. J Parallel Distrib Comput 130:91–97
9. Moura T, Gomes A (2017) Blockchain voting and its effects on election transparency and voter confidence. In: Proceedings of the 18th annual international conference on digital government research, pp 574–575
10. Shahzad B, Crowcroft J (2019) Trustworthy electronic voting using adjusted blockchain technology. IEEE Access 7:24477–24488
11. Yavuz E, Koc AK, Cabuk UC, Dalkilic G (2018) Towards secure e-voting using ethereum blockchain. In: 2018 6th international symposium on digital forensic and security (ISDFS). IEEE, p 17

A Nature Inspired Algorithm for Enhancement of Fused MRI and CT Brain Images

Leena Chandrashekar and A. Sreedevi

1 Introduction

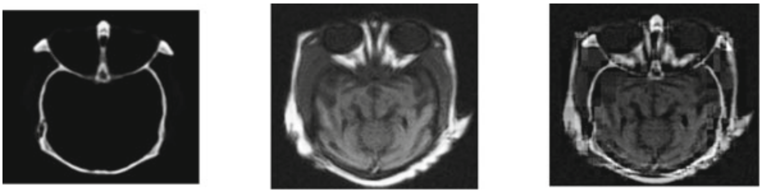
Glioblastomas are the fastest growing Grade IV malignant tumors found in the brain with a survival time of less than a year after their detection [1]. The detection of these tumors is an unceasing challenge to doctors. The failure to recognize the early symptoms, lack of awareness, inadequate imaging facilities, preliminary screening for the patients and expertise with doctors are some of the factors that delay the detection. For this reason, medical imaging is paramount in detection, identification, grading and diagnosis of the Glioblastomas. Doctors recommend various imaging techniques for detection of Glioblastomas like Computed Tomography (CT), Magnetic Resonance Imaging (MRI) and its variants, Fluid Attenuated Inverse Recovery (FLAIR) and Positron Emission Tomography (PET) [2]. These images are acquired sequentially through different scanning machines at different times. Doctors assess the images independently and conclude the analysis based on their experience and expertise. Each of the modalities provide different information of the brain. For example, the CT image provides the structural information of the brain like bone structure, tissue symmetries, changes in tissue density and space occupying lesions [3]. It also shows changes made in the nearby skull region due to tumor extension and calcification of tumors. Conversely, CT images fail to indicate tumor borders and infiltration in the nearby regions. These can be easily visualized with Magnetic Resonance Image (MRI), which provide structural and functional information of the brain along with high contrast and resolution for soft tissues like tumors or lesions [3]. These multimodal images are the noninvasive ways to detect Glioblastomas. Based on the multimodal images, surgical resection or complete removal of tumor is made followed

L. Chandrashekar (✉) · A. Sreedevi
RVCE, Bangalore, India

A. Sreedevi
e-mail: sreedevia@rvce.edu.in

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

N. R. Shetty et al. (eds.), *Emerging Research in Computing, Information, Communication and Applications*, Lecture Notes in Electrical Engineering 789,
https://doi.org/10.1007/978-981-16-1338-8_2



(a) (b) (c)

Fig. 1 **a** CT image, **b** MR image, **c** fused image

by radio chemotherapy [4]. Thus, a single imaging technique is never sufficient to confirm the presence or extent of the tumor [5]. This helps in early detection of tumors and requires lesser digital storage [7, 8]. Some of the techniques for fusing the multimodal images are Discrete Wavelet Transform (DWT), Laplace Transform (LT), Contourlet Transform (CT) and Non-sub Sampled Contourlet transform (NSCT) [6]. The process of fusion begins with decomposing the multimodal images in to approximation coefficients (low frequency components of the image) and detailed coefficients (high frequency components) using the above techniques. These components are combined using different rules like averaging, summing, weighted summing, max–min or max-max fusion rules [7]. The fused coefficients are recomposed using inverse transforms to generate a fused image. The visual quality of the fused image is evaluated based on contrast, edge information and peak signal to noise ratio.

The fusion process introduces blocking effect, noise and artifacts that greatly reduce the visual quality of the fused image. Figure 1 shows a CT, MR and fused image obtained by DWT, indicating blocking effect at the edges and corners [6, 7]. The fused images with poor visual quality make it difficult for experts to interpret the tumor presence or its spread. Hence, there is a need for an enhancement technique to improve the visual quality and reduce blocking effect, noise and artifacts. Most of the enhancement techniques deal with improving image contrast, as it helps in differentiating the Glioblastomas and the normal cells. Nevertheless, the drawback with these techniques is that it only increases the dynamic range of the image, which is a function of pixel intensity alone. Tumors or any abnormality in the brain appears distinct, bright or light intensity in MR images. Thus, by varying the contrast, the normal and the tumorous cells can be differentiated easily. On the contrary, the high contrast images or low contrast MR image makes it challenging to differentiate the Glioblastomas. The contrast enhancement is mostly a twofold process, consisting of contrast stretch and tonal enhancement. The contrast stretch improves the brightness differences uniformly across the dynamic range of the image and tonal enhancement improve the brightness differences in different areas like dark, gray or bright regions in the image [6]. The paper deals with enhancement techniques for CT and MRI fused images that mostly focus on improving the contrast, structural information, peak signal to noise ratio with minimum loss of information.

2 Enhancement Techniques

Generally, the contrast enhancement is achieved by the following techniques—Non-Linear Transfer function, Histogram based and Frequency Domain [11]. Among them, Histogram Equalization (HE) is the most popular technique for contrast enhancement performed in a spatial domain. This deals with remapping the gray scale values of the original input image to a new level of gray scale values using linear or non-linear functions. This remapping aims at flattening and stretching the dynamic range of the image histogram. Although HE is a popular enhancement technique, it suffers from visual artifacts like intensity saturation and amplification due to large number of homogenous pixels. The equalization is accomplished uniformly for all the pixels of the image, leading to enhanced global contrast. However, the lowest intensity pixels become less significant, thereby reducing the local contrast [12]. In order to overcome the drawbacks of HE, newer enhancement techniques are proposed for improved visual quality with the use of median filters, adaptive gamma correction and homomorphic filtering [13, 14].

An Adaptive Histogram Equalization (AHE) technique is a block based adaptive method, that deals with the local contrast rather than global contrast. The local contrast is more significant in the detection of Glioblastomas as it can clearly distinguish the normal and tumor cells. In this technique, histogram equalization is performed on sub-images or small and equal sized blocks obtained by splitting the image. The equalization is executed on every block independently and mapped to new intensity levels based on a transformation function. The new pixel values are solely based on the neighboring pixel characteristics. Then, bilinear interpolation is used to combine the blocks after equalization [14]. The major challenge with AHE is the selection of the block size and the transformation function. AHE also suffers from blocking effect, at the time of combining the blocks. Over-amplification is also seen due to large homogenous regions of the image. Youlian Zhu et al. have proposed an adaptive histogram equalization technique for CT images. A user defined parameter β, is suggested based on the gray level of the image. The entropy is used as an objective function to select the β adaptively [15].

A variant of AHE is the Contrast Limited Adaptive Histogram Equalization (CLAHE), proposed by *K* Zuierveld, is also a block-based contrast enhancement technique with focus on local contrast. Unlike AHE, CLAHE provides uniform equalization with clipping the excess portion of large peaks found after the histogram equalization, thereby avoiding over-amplification. The excess portion removed depends on a parameter called clip limit, which is a function of the dynamic range of the image and block size. CLAHE involves setting of three operational parameters—clip limit, block size and distribution function, which must be carefully chosen before performing the image enhancement to achieve good contrast images, free from noise and artifacts [16]. Various histogram-based enhancement techniques are compared and analyzed, CLAHE is observed to perform better for MRI brain Images [17].

The simplest technique of setting the operational parameters for CLAHE is by trial and error, however, this is time consuming, may deviate from the actual values and varies with every image. Some of the techniques used to set the parameters are based on textureness of the image, maximum curvature of entropy, Least Mean Square (LMS) algorithm, multi-objective optimization technique and fuzzy rules. In spite of various techniques for contrast enhancement, CLAHE seems to provide good local contrast, however it largely fails to enhance the pixels with low gray level intensity. Moreover, there is no standard for finding the optimal clip limit for a specific region of interest in medical images. Generally, clip limit is proportional to the multiple of mean of the histogram, where the multiplication factor is user-defined and varies for different images. Therefore, there is a need to choose clip limit adaptively for every block of image without any user intervention [23].

The clip limit is also a function of dynamic range of the grayscale image, block size and slope of transformation function. Initially, the clip limit and block size are chosen empirically and then obtain the optimal values based on statistical parameters like entropy, peak signal to noise ratio or edge information. Yet clip limit may change depending on the type of images. This makes the enhancement process very extensive and time consuming [23]. Moreover, inaccurate selection of clip limit can cause over-amplification in CLAHE. Bilateral Filter and Median filters are used to overcome this drawback [24, 25]. Optimization techniques provide a convenient way of determining the CLAHE parameters without any heuristics and compute them adaptively for every image block. Particle Swarm Optimization (PSO)—a population-based optimization technique proposed by Eberhart and Kennedy [27]. The motivation for PSO is from the biological social groupings of animals, which interact with each other to find food or save each other from predators. A swarm is defined as a group of possible solutions to the optimization problem, also called particles. Each particle of the swarm is identified with its velocity and position, which are updated through iterations. The performance of the optimization is evaluated based on a fitness function. The search for best solution terminates at the end of the iterations or when the solution generates the highest fitness value [27, 28].

Based on the recent literature, we propose an enhancement technique for fused Multimodal and Multiresolution brain images, that suffer from blocking effect, noise and artifacts during the fusion process. CLAHE can be used to improve the contrast of the fused image, but the structural information in the fused MRI and CT images is lost due to AHE. The PSO algorithm enable the selection of the operational parameters of CLAHE based on a multi-objective fitness function which is essentially dependent on entropy and edge information of the image. Hence, the enhanced image is improved in terms of contrast, structural information with minimum mean square error.

3 Proposed Enhancement Technique for Fused CT and MRI

The proposed enhancement technique begins with preprocessing of MRI and CT images, image registration, and image fusion followed by image enhancement. More than 200 MRI and CT images containing Grade IV tumors—Glioblastoma are taken from www.Radiopedia.org for the experiment. There are quite a few databases available publicly for MRI images, but the challenge in our research is to get multimodal images for the same patient. Since these are acquired at different times and from different machines, they must be registered and preprocessed before fusing them. The simulation is performed on MATLAB 2020. Figure 2 shows the block diagram for the enhancement process. The preprocessing stage resizes the image to size 256 × 256 and converts them to gray scale. The images contain Gaussian and Rician noises, that are eliminated; Non-Local Means Filter is used in filtering the CT and MRI images [29]. The preprocessing is followed by image registration—a mandatory step, where both the as are matched for size, orientation and scaling. Subsequently, the images are fused using Laplacian Pyramid or Non-sub sampled Contourlet transform. The former fusion technique provides good structural information and latter offers enhanced contrast in the fused images as shown in Table 1.

The fusion process introduces blocking effect and noise in the fused image, thereby reducing the image quality as discussed in Sect. 1 [30]. Since the focus is the tumor region and differentiating the healthy and tumorous cells, adaptive block-based enhancement technique like CLAHE is chosen. The operational parameters for

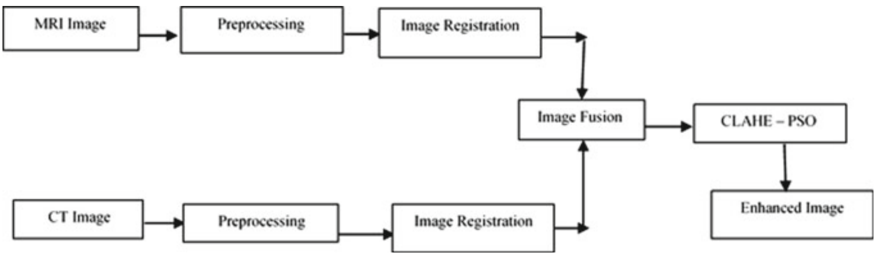


Fig. 2 Methodology for the proposed enhancement process

Table 1 Performance of Laplacian Pyramid and non-sub sampled contourlet transform image fusion

Dataset D6	STD	En	SSIM	PSNR	UIQI	MSE
LP Fused	72.87	4.04	0.75	19.07	0.42	804.22
Proposed	68.04	3.93	0.85	20.4	0.84	3.44E+04
NSCT fused	76.34	5.81	0.53	18.88	0.42	848.33
Proposed	75.87	5.65	0.65	20.29	0.59	6.07E+02
Dataset D13	STD	En	SSIM	PSNR	UIQI	MSE
LP Fused	72.22	5.39	0.63	11.92	0.57	948.58
Proposed	69.92	5.25	0.83	12.29	0.78	810.07
NSCT fused	77.96	6.24	0.57	18.61	0.57	894.85
Proposed	79.77	6.17	0.67	19.22	0.67	776.99

CLAHE are block size, clip limit and distribution function. The proposed technique is executed for different block sizes like 2 × 2, 3 × 3, 4 × 4, 5 × 5, 7 × 7, 8 × 8 and 10 × 10. It must be noted that, the 8 × 8 provided superior results in terms of contrast and structural information, hence chosen to be constant for the enhancement process. Similarly, the enhancement process was performed with the various distribution functions like Uniform, Rayleigh and Exponential distribution. The Uniform distribution allows distribution of clipped pixels unvaryingly in the image histogram and hence preferred. The clip limit is initialized randomly in the range of 0–0.01, the PSO algorithm adaptively choses the clip limit based on a fitness function, given in Eq. (1).

$$F(I_e) = \log(\log(E(I_s))) \times \frac{n\_\text{edges}(I_s)}{M \times N} \times H(I_s) \quad (1)$$

The proposed enhancement process is two-fold; firstly, the contrast of the MRI and CT fused image is enhanced by CLAHE algorithm, which increases the dynamic range of the image. Secondly, the multi-objective fitness function assists in choosing the clip limit for CLAHE that maximizes the entropy and edge information of the image. The Particle Swarm Optimization (PSO) algorithm finds the optimal clip limit. A swarm of 50 particles, each representing the clip limit is initialized in the range of 0–0.01. With each of them, the fused image is enhanced by CLAHE and a fitness function that is product of entropy, sum of edge intensities and number of edge pixels is computed. The clip limit that gives maximum fitness value is chosen. Since, multiple parameters are considered to measure the degree of enhancement; this function is called multi-objective function. Every particle i in the swarm is represented by two parameters velocity and position. For any particle 'i', the position and velocity indicate its location in the swarm and fitness value respectively. The velocity and position are computed based on some random values and is updated in every iteration using Eqs. (2) and (3).

$$v_i(t+1) = wv_i(t) + c_1r_1(p_i(t) - x_i(t)) + c_2r_2(g(t) - x_i(t)) \quad (2)$$

$$x(t+1) = x_i(t) + v_i(t+1) \quad (3)$$

where $v_i(t)$ and $x_i(t)$ represent the velocity and position for an particle i and iteration t. Equation (2) comprises of three components—first component representing the initial velocity of the particle, the second component represents the particle's decision based on its own experience and the third component indicates the particle's decision based on swarm's experience. In every iteration, the image is enhanced using CLAHE with the selected clip limit (each particle). The fitness function is computed using Eq. (1). This process is repeated for all the particles to get the best fit (clip limit). The clip limit that maximizes the fitness function can be accessed from the swarm based on its position and velocity and is represented as 'p_{best}' or $p_i(t)$. This denotes the best local solution for that iteration. The enhancement process is repeated for all

Initialize the particle swarm
For each iteration
For each particle
Enhance the image using CLAHE
Compute the fitness value for the enhanced image as per Eq. (1) for every particle
If the fitness value is greater than the previous fitness value (pbest)
Set current value as the new pbest (gbest)
End
Choose the particle with the best fitness value among all the pbest (gbest)
For each particle
Calculate particle velocity as per Eq. (2)
Calculate the particle position as per Eq. (3)
End
Continue while maximum iterations are attained.
End
Report the gbest and pbest

Fig. 3 Pseudocode for proposed technique

the iterations to get 'p_{best}' or $p_i(t)$ for each iteration. In case the 'p_{best}' value in the current iteration is greater than the previous one, then the 'p_{best}' is updated with a new 'p_{best}' and 'g_{best}', otherwise the 'p_{best}' from previous iteration is retained as 'p_{best}' and 'g_{best}'. The 'g_{best}' or $g(t)$ in Eq. (2) is the global solution for the enhancement process obtained at the end of all the iterations. When 'p_{best}' appears equal 'g_{best}' over a predefined number of iterations the enhancement process terminates.

A balance between 'p_{best}' and 'g_{best}' is achieved by inertia weight represented as w, c_1 and c_2—the positive acceleration constants ($c_1 = 2.5$, $c_2 = 1.5$) and r_1 and r_2 are random values in the range of [0, 1]. Figure 3 shows the pseudo code for proposed CLAHE-Particle Swarm Optimization algorithm with Uniform distribution function.

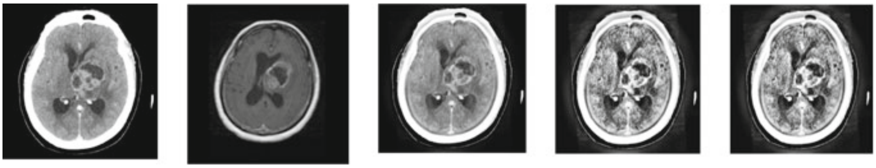
4 Experiments and Results

The CT and MRI images prior to enhancement are preprocessed, registered and fused using Laplacian Transform. The dataset includes many variants for CT and MRI images—(i) images with contrast agent (ii) images without contrast agent and (iii) delayed images with contrast agent. The combination of CT and MRI T1 image, CT and MRI T2 and CT and MRI FLAIR images is used to generate the fused image. The proposed enhancement technique is tested on more than 200 MRI and CT fused images, containing the different types of Glioblastomas—Multicentric Glioblastoma, Multifocal Glioblastoma, Cystic Glioblastoma and Giant Cell Glioblastoma. Table 2 lists the characteristics of the datasets considered for enhancement.

Figures 4, 5, 6 and 7 shows 4 sample CT, MRI, fused image, CLAHE enhanced image and the enhanced image from the Proposed method. The datasets chosen belong to Group I representing large tumors and Group II with small tumors. In

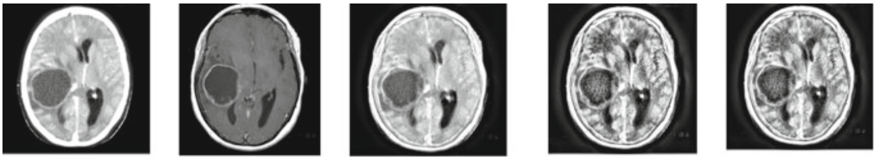
Table 2 Characteristics for sample dataset

Dataset	CT	MRI	Size of tumor	Group	Type of tumor
D20	High contrast	Low contrast	Large	I	Cystic high-grade glioblastoma
D53	Large size	Small size	Large	I	Glioblastoma (Grade IV)
D60	Large size	Large size	Large	I	Giant cell glioblastoma
D67	Large size	Small size	Large	I	Primary CNS lymphoma
D65	Small size	Large size, Poor contrast	Large	I	differential diagnosis—metastasis and glioblastoma
D17	Misaligned	Aligned, Poor contrast	Small	II	Glioblastoma (Grade IV)
D16	Aligned	Misaligned, Poor contrast	Small	II	Multicentric glioblastoma
D15	Aligned	Misaligned, Poor contrast	Small	II	Multifocal glioblastoma
D6	Large	Small, Poor contrast	Small	II	Glioblastoma (Grade IV)
D50	Small	Large	Small	II	Glioblastoma (Grade IV)



(a) (b) (c) (d) (e)

Fig. 4 Dataset D20. **a** CT image, **b** MRI image, **c** Fused image, **d** CLAHE

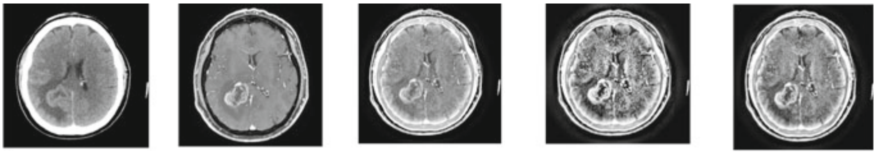


(a) (b) (c) (d) (e)

Fig. 5 Dataset D53. **a** CT image, **b** MRI image, **c** Fused image, **d** CLAHE

(a) (b) (c) (d) (e)

Fig. 6 Dataset D67. **a** CT image, **b** MRI image, **c** Fused image, **d** CLAHE



(a) (b) (c) (d) (e)

Fig. 7 Dataset D50. **a** CT image, **b** MRI image, **c** Fused image, **d** CLAHE

addition, high contrast CT and poor contrast MRI images are also tested with the proposed technique. For example, the CT image in dataset 20 (Fig. 4) has very high contrast and MRI T1 in dataset 16 and 17 has poor contrast are considered for the proposed enhancement method. Table 3 shows the expressions for various performance parameters, the detailed definitions are discussed in [30–33]. The proposed enhancement technique provides high PSNR, SSIM, UIQI and a minimum MSE. It can be observed that images enhanced by CLAHE seem enhanced, however it is only in terms of contrast or variaion of brightness but the structural information is poor. Although, the standard deviation and entropy is high for enhanced image obtained by CLAHE, the PSNR, SSIM, UIQI is lesser than those obtained with the

Table 3 The performance parameters for evaluation of the enhanced image

S. No.	Parameter	Equation
1	Standard Deviation (SD)	$\sqrt{\frac{1}{H\times W}\sum_{x=1}^{H}\sum_{y=1}^{W}(F(x,y)-\mu)^2}$
2	Entropy (En)	$\sum_{l=0}^{L-1} p(l)\log_2 p(l)$
3	Mean Square Error (MSE)	$\frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}(I_1(i,j)-E(i,j))^2$
4	Peak Signal to Noise Ratio (PSNR)	$20\log_{10}\left(\frac{255}{\sqrt{\text{MSE}}}\right)$
5	Structural Similarity Index Metric (SSIM)	$\frac{(2\mu_e\mu_s+C_1)(2\sigma_e+C_2)}{(\mu_e^2+\mu_s^2+C_1)(\sigma_e^2+\sigma_s^2+C_2)}$
6	Universal Image Quality Index (UIQI)	$\frac{4\sigma_e\sigma_s(\mu_e+\mu_s)}{(\sigma_e^2+\sigma_s^2)(\mu_e^2+\mu_s^2)}$