

Leveraging blockchain technology to combat deception, deepfake, and counterfeit system

T. Gopalakrishnan *

*Department of Information Technology
Manipal Institute of Technology Bengaluru
Manipal Academy of Higher Education
Manipal 576104
India*

Hayder M. A. Ghanimi [†]

*Department of Information Technology
College of Science
University of Warith Al-Anbiyaa
Karbala 56001
Iraq*

and

*Department of Computer Science
College of Computer Science and Information Technology
University of Kerbala
Karbala 56001
Iraq*

Tanweer Alam [§]

*Department of Computer Science
Faculty of Computer and Information Systems
Islamic University of Madinah
PO Box: 170
Madinah 42351
Saudi Arabia*

* E-mail: gopalakrishnan.t@manipal.edu (Corresponding Author)

[†] E-mail: hayder.alghanami@uowa.edu.iq

[§] E-mail: tanweer03@iu.edu.sa

K. Sreekanth [†]

*Department of Computer Science and Engineering
Koneru Lakshmaiah Education Foundation
Vaddeswaram 522502
Andhra Pradesh
India*

K. E. Purushothaman [@]

*Department of Electronics and Communication Engineering
Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology
Chennai 600062
Tamil Nadu
India*

Sudhakar Sengan [#]

*Department of Computer Science and Engineering
PSN College of Engineering and Technology
Tirunelveli 627152
Tamil Nadu
India*

Pankaj Dadheech ^{\$}

*Department of Computer Science and Engineering
Swami Keshvanand Institute of Technology, Management & Gramothan (SKIT)
Jaipur 302017
Rajasthan
India*

Abstract

Counterfeit technology propagation and deepfake systems threaten authenticity, trust, and data integrity. This research article proposes a novel technique that leverages Blockchain Technology (BT) integrated with improved chameleon hashing to combat these threats. BT integration assures transparency and immutability, while improved Chameleon Hash Function (CHF) gives secure and efficient authentication. This combined technique focuses on enhancing the prevention and detection of illegal content changes, providing a robust solution for preserving the authenticity and integrity of digital content. The proposed blockchain-assisted improved Chameleon Hashing (BAiCH) promises substantial progression in combating deception and fake systems via a cryptographically and CHF

[†] E-mail: ksreekanth@kluniversity.in

[@] E-mail: k.e.purushothaman1992@gmail.com

[#] E-mail: sudhasengan@gmail.com

^{\$} E-mail: pankajdadheech777@gmail.com

secure system. The performance of the proposed framework *BACH* is compared with existing *state-of-the-art* techniques. The *BACH* give a minimal Bit Error Rate (BER) of *0.098 bits* and a higher Signal-Noise Ratio (SNR) of *30dB*, which is efficient over existing techniques.

Subject Classification: 34A06.

Keywords: *Cyber-physical system, Blockchain technology, Chameleon hash function, Bit error rate, Signal-noise ratio, Deepfake systems.*

1. Introduction

Digital technologies have transformed human lives in multiple methods, which would have been incredible a few years ago. With the revolution of the Internet of Things (IoT) devices, the collection of data and taking actions consequently has been made more accessible, and utilization of multiple emerging technologies to access the desired functionalities and operations right from self-driving automobiles to space automation has been accomplished through the magic of the Internet [1]. We live in a world of electronic services that provide users speed and implementation through secure primary technology. Hence, global governments have made commendable efforts towards this new research based on providing e-services to their people that would fill the gap between public services and citizens [2]. A Blockchain is depicted as a sequence of data blocks or structures containing multiple transactions, ensuring the data is secured, decentralized, and transparent. All the parties in the network have access to the data; hence, it's also called a distributed ledger [3]. Once the data is saved, it is not easy to alter it. Modifying data or adding new data will have to be approved by all network nodes [4]. A digital signature is one of the ways to secure the data and provide anonymity so that only the intended recipients have access to the data.

In general, all the network members must agree before making any changes. Hence, data stored in the blockchain is secured and will not be double-counted. In a network built on blockchain [5], it's easier to detect fake activity and anomalies. Dynamic fraud prediction and prevention techniques usually fail. Post-distribution study of content applying Machine Learning (ML) and ethical techniques for detecting anomalies is standard. AI models which generate accurate fakes avoid these techniques. Addressing these problems involves a more pre-emptive and effective method. [6]

Optimising the Chameleon Hashing Function (CHF) would boost the blockchain's security and accuracy in authenticating digital content integrity. CHF emits hashing keys that can only be manipulated by certified users with trapdoor credentials. It ensembles settings that need limited data alteration functionality with minimal privacy. Image classification gets better by weak supervised area selection in Gaze Latent Support Vector Machine (GL-SVM). Image recognition and phrases have been enhanced by Long Short-Term Memory (LSTM). Recurrent Convolutional Neural Network (RCNN) Methods identify video face applications. These approaches use sophisticated algorithms to fix CV problems [7-9]. Blockchain-Assisted Improved Chameleon Hashing (BAiCH) is efficient for detecting deepfakes and fraudulent systems. CHF enables reliable, accurate authentication, whereas Blockchain Technology (BT) secures and monitors data.

This proactive approach not only detects but also prevents unauthorized content alterations, thereby maintaining the integrity and authenticity of digital content. By leveraging BACH, a more robust digital ecosystem can be developed where data integrity and trust are secured against advanced Artificial Intelligence (AI)-generated fake content threats [10-11]. This integration is vital for protecting the reliability of transactions and digital communications in an era where the line between real and fake is increasingly blurred [12].

The paper's organization is as follows: Section 2 provides the background for the work, Section 3 presents the proposed model, Section 4 presents the experimental analysis, and Section 5 concludes the work and future study of the proposed work.

2. Improved CHF and BT to Combat Deception, Deepfake, and Counterfeit System

Computing systems are classified into two types: complete systems and delicate systems. Complete systems reproduce the entire blockchain when adding a block, ensuring consistency [13]. Delicate systems, however, only copy the block title for transaction validation. Upon network resettlement or alerts on wallet changes, delicate systems verify against a complete system's copy. In our model, divisional systems act as complete systems, while citizens' or businesses' devices act as delicate systems, although any connected system can copy the entire BT. Broadband Remote Access Server with Wi-Fi can provide peer-to-peer connectivity.

All systems must agree on block addition and validation methods for BT functionality. The Delegated Proof of Stake (DPoS) method efficiently adds and secures blocks. In DPoS, systems vote for representatives to manage blockchain validation. Representatives selected managers based on voting impact. This method ensures justice by allowing users with more votes to influence elections. Problematic agents are excluded from elections, maintaining network integrity. DPoS's efficiency and resource utilization are crucial, as seen in Ethereum's use of DPoS and Smart Contracts (SC), which are similar to economic devices. This method supports secure, private user data storage and transaction management, enhancing economic device accessibility and organization.

3. CHF in Deepfake Identification (DI)

CHF, also known as trapdoor hashing, uses a one-way Hash Function (HF) with public and private keys (trapdoor keys). Its characteristics include:

- Non-transferable signatures
- Detection of forged signatures and non-repudiation
- Hash collision prevention without the trapdoor key

Signers can reuse signatures to validate specific messages, but unauthorized reuse by receivers leads to hash collisions, preventing fraud. Signers can adjust input parameters without changing the output HF. This functionality is crucial for DI, as it allows for secure, verifiable signatures on digital content, ensuring authenticity and preventing manipulation.

Hence, the HF is called the CHF. It's not easy to find the hash-code using collision on given messages $[m, m^1]$ and random numbers $[r, r^1]$ when only hash-key (HK) is available $h(m, r) = h(m^1, r^1)$. Alternatively, it's straightforward to compute the value of ' r ' using CHF-key HK_R and private-key $TK_{R'}$ where the HF is mentioned as $h(m, r) = h(m^1, r^1)$. The value of CHF as CHAMHASHR(...), generated on a random value and message, will adhere to the following properties.

Collision Resistance: It's impossible to find an input where CHAM-HASH_R (...) will lead to the same output HF code, EQU (1).

$$CHAM - HASH_R(m_1, r_1) = CHAMHASH_R(m_2, r_2) \quad (1)$$

Trapdoor Collisions: This relates to a private key which can compute the value ' r_2 ' from the given input pair m_1 and r_1 along with a message ' m_2 ', EQU (2).

$$CHAMHASH_R(m_1, r_1) = CHAM - HASH_R(m_2, r_2). \quad (2)$$

Uniformity: Consistent random values selected will result in a similar probability distribution of messages.

Lemma: Design of CHF as $CHAM-HASH_R(.,.)$ for the given input parameters, which provides non-transferable and collision resistance functionality.

To combat DI using BT, initialize the entire network node for integration, allowing other clients to initialize lightweight nodes. New node addresses are tagged with blockchain wallets using pre-generated keys, and registration details are published to all peers. Nodes then prepare for transaction verification. The network is created using the new node based on the available directives and parameters, and a delegate node authenticates the new node. All nodes are updated with the latest network changes to prevent data tampering. This ensures the secure addition and validation of new nodes, maintaining network integrity. Input parameters include a function call to register a new node and the total number of nodes (N), resulting in the successful addition and validation of the new node. This approach ensures that any attempt to manipulate digital content, such as DI, is detected and prevented through

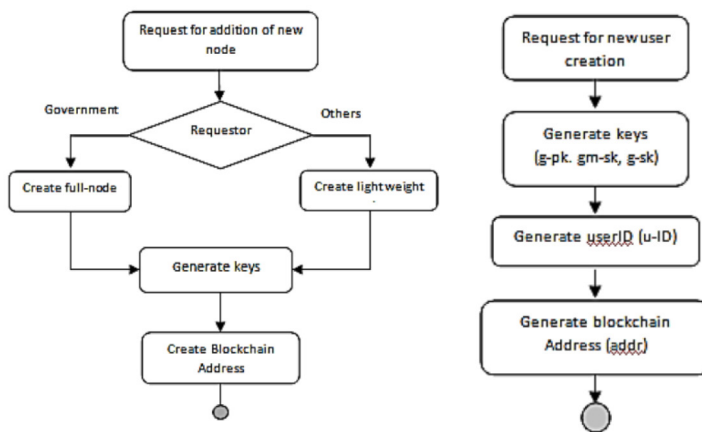


Figure 1
New Node and User Registration Process

a decentralized and secure verification process. Users register via mobile app, web browser, or department visit. Upon registration, a user ID and blockchain address with multiple keys are generated, validated by peers, and stored securely. The new node and user registration process is given in Figure 1.

The function call and sum of nodes (N) are input to register a new user. **Output:** New user (u) is added and validated. A transaction request updates the block and is validated by peers. Client address stores user ID, value, owner details, and key. Third-party applications access data via the blockchain Application Program Interface (API) after obtaining address details. In the critical loss, the user generates a new address and requests data transfer. This ensures data security and prevents unauthorized access. The next step is given in Algorithm 1.

Algorithm 1. Key Generation, Signing, Verification, and Opening Algorithm

- Step 1. $G\text{-Keygen}(1k, 1n) \rightarrow g\text{-pk}, g\text{-sk}, g\text{-sk}$
 where ' k '-parameter to secure data; ' n '-Total size of the group; $H \in \mathbb{H}$: Subset of data from Chameleon-Hash function
- Step 2. $g\text{-pk}' \leftarrow g\text{-pk} \parallel H$
- Step 3. $g\text{-sk}' \leftarrow g\text{-sk} \parallel H$
- Step 4. $g\text{-sk}' \leftarrow g\text{-sk}[i]$, Where $i \in n$
- Step 5. $g\text{-sk}' = g\text{-sk}[1] \parallel H, g\text{-sk}[2] \parallel H, \dots, g\text{-sk}[n] \parallel H$
- Step 6. $\text{Sign}(g\text{-sk}', m) \rightarrow \text{signature } \sigma$
- Step 7. $g\text{-sk}' \leftarrow g\text{-sk} \parallel H$
- Step 8. $\text{rand}() \rightarrow \text{random-number}, r \in (0, 1^k)$
- Step 9. Evaluate $x = H(r, m)$
- Step 10. HF using random numbers and message
- Step 11. $\sigma \leftarrow \text{Sign}(g\text{-sk}'[i], X)$
- Step 12. $\text{Verify}(g\text{-pk}, m, \sigma) \rightarrow \text{Allow} / \text{Decline}$
- Step 13. $\sigma' \leftarrow \sigma \parallel H$
- Step 14. $g\text{-pk}' \leftarrow g\text{-pk} \parallel H$
- Step 15. Compute $x = H(\dots)$, Parameters: r and m
- Step 16. HF using random numbers and message
- Step 17. $\text{Allow} / \text{Decline} \leftarrow \text{Verify}(g\text{-pk}, x, \sigma')$
- Step 18. $\text{Open}(g\text{-sk}', m, \sigma) \rightarrow (i / \perp)$
- Step 19. $G\text{-sk}' \leftarrow g\text{-sk} \parallel H$
- Step 20. $\sigma' \leftarrow \sigma \parallel H$
- Step 21. $\text{rand}() \rightarrow \text{random-number}, \in (0, 1k)$

- Step 22. Evaluate $x \leftarrow H(\dots)$
 Step 23. HF using random numbers and message
 Step 24. $i, \perp \leftarrow \text{Open}(gm-sk, X, \sigma')$
 Step 25. End
-

In the above step, the key generation algorithm is executed to find the value of the group primary key (gpk), group manager secret key ($gmsk$) and group secret key (gsk). The gpk , $gmsk$ and gsk are generated by running a HF algorithm with input values ' $1k$ ' and ' $1n$ '. ' N ' is the size of the primary group, and ' K ' is the parameter to secure the data transmission. In CHF as $H \in H$, N -dimensional keys are formed by $g-pk' = g-pk \parallel H$ and $g-sk'$. At the same time, $g-sk[i]$ is the confidential key the signer $i \in [N]$ uses. In other words $g-sk' = [g-sk[1] \parallel H, g-sk[2] \parallel H, \dots, g-sk[N] \parallel H]$. The validation algorithm uses the confidential key used by the group for validation of the message ' m ' ($g-sk > \text{group-secret-key}$) and generates the signature ' σ '. Verify the authenticity of signature ' σ ', using group primary-key (gpk), on message ' m '. ' σ ' and $g-pk'$ are evaluated using subsets $\sigma' \parallel H$ and $g-pk \parallel H$. Compute $x \leftarrow H(\dots)$ with parameters ' r ' and m and verify the signature using $g-pk$ and $x[\text{verify}(g-pk, x, \sigma')]$. Accept or discard the messages based on the result of this test. The open algorithm inputs the following parameters: the $gmsk$, the message that needs to be signed (m) and the signature ' σ '. Decode the value of σ , $g-pk'$ as $\sigma' \parallel H$ and $g-pk \parallel H$. Derive the value of ' $x \leftarrow H(\dots)$ ' with parameters ' r ' and ' m ' and get the DI $i \leftarrow \text{Open}(gm-sk, x, \sigma')$ or $\perp$ to confirm a failure operation. Any group associate is competent to open the signature; hence, it is called self-less secrecy.

4. Result and Discussion

Security is a key challenge in achieving authenticity, reliability, and accountability in logistic structures. Protection against unauthorized cyber-attacks, assurance of trust through authenticated, protected integrity mechanisms, and remote data availability are the objective attributes of a secured system. The following section studies the method's security, privacy and authenticity with primary BT. Experiments were accomplished using Python and MATLAB on a laptop with an Intel i7-1185G7 processor and 64 GB of RAM. The video clip, a 190.0240-second speech, has a frame rate of 29.97 *fps* and a speech signal sampled at 44.1 *kHz* with a 16-bit resolution. Only this single video clip was used for proof-of-concept valuation. Bit Error Rate (BER) and Signal-to-Noise Ratio SNR serve to assess the recommended BAiCH's functionality. BAiCH is juxtaposed to

GL-SVM, LSTM, and RCNN. Communications and digital signal processing utilise SNR to contrast the targeted signal with background noise—a key factor for measuring the quality of communication. Higher SNRs imply better, more precise signals with less noise, which implies more precise and accurate data in transmission. SNR is characteristically stated in decibels (*‘dB’*). The simulation result is projected in Table 1 and Figure 2. The performance is assessed by the EQU (3).

$$SNR = 10\log_{10}\left(\frac{P_{Signal}}{P_{Noise}}\right)$$

(3)

Table 1
Comparison of SNR

Frame Count	GL-SVM	LSTM	RCNN	BACH
50	16	17	19	23
100	16.5	18	19.5	24
150	17	19	20	25
200	18	21	20.5	28
250	18.5	21.5	21	30

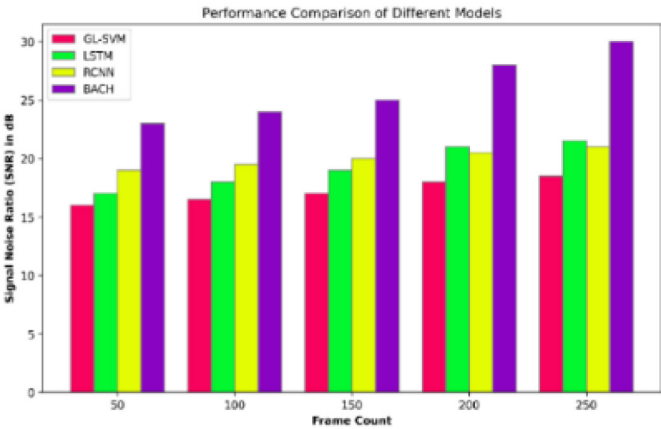


Figure 2
Comparison of SNR

Measuring SNR and BER with frame counts for GL-SVM, LSTM, RCNN, and BAiCH proves performance differences. BAiCH frequently outperforms the other models in SNR, beginning at 23 dB for 50 frames

and hitting 30 dB at 250 frames. From 19 dB for 50 frames to 21 dB at 250 frames, RCNN improves well. LSTM and GL-SVM exhibit lower SNR values as the frame count increases, respectively, 17–21.5 and 16–18.5 dB. In digital communication systems, BER monitors the data flow error rate. It is the proportion of error-received bits to total bits sent over a period. A decreased BER implies a more precise and secure transmission system, which is vital to data security. A summary is in Table 2 and Figure 3. The subsequent EQU (4) measures performance.

$$BET = \frac{N_{error}}{N_{total}} \quad (4)$$

Table 2
Comparison of BER

Frame Count	GL-SVM	LSTM	RCNN	BACH
50	0.42	0.39	0.31	0.14
100	0.41	0.38	0.33	0.12
150	0.39	0.37	0.35	0.1
200	0.38	0.36	0.36	0.099
250	0.37	0.34	0.38	0.098

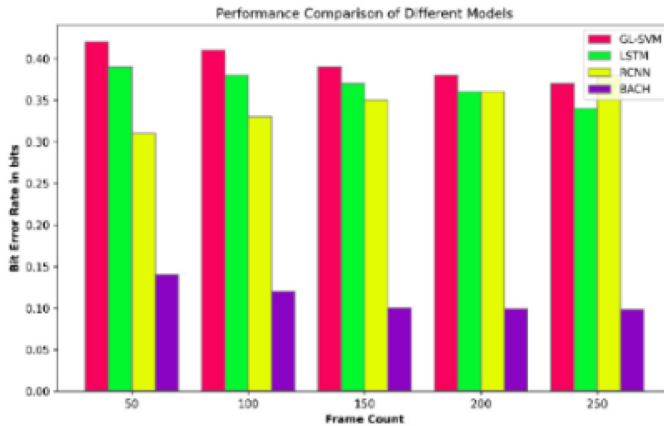


Figure 3
Comparison of BER

BACH demonstrates more accuracy for BER with the lowest error rates, starting at 0.14 for 50 frames and reducing to 0.098 for 250 frames. RCNN shows slightly higher error rates, beginning at 0.31 and reaching

0.38. LSTM performs better than RCNN but worse than BAiCH, decreasing BER from 0.39 to 0.34. GL-SVM has the highest BER, starting at 0.42 for 50 frames and decreasing to 0.37 for 250. These results indicate that BAiCH offers the best combination of high SNR and low BER, making it the most reliable model for maintaining signal integrity and minimizing transmission errors.

5. Conclusion

By providing efficient communication and data exchange between administrative groups, the system solves shortcomings in current models while focusing on interoperability. A distributed open-source system that can dynamically run enormous data sets while maintaining privacy and integrity is necessary for its implementation. Heterogeneous networks can be enabled by adapted Blockchain Technology (BT) without losing efficiency or reliability. However, BT must be robust and permanent in order to adjust to innovative technologies. Algorithmic hashes are the core of BT's security, but they are susceptible to quantum-based attacks, particularly attacks addressing the Grover and Shor algorithms. Although it has a promising time preceding it, BT will need to be robust and unchangeable to deal with technological advances.

References

- [1] H. R. Hasan and K. Salah, "Combating Deepfake Videos Using Blockchain and Smart Contracts," in *IEEE Access*, vol. 7, pp. 41596-41606 (2019).
- [2] A. Yazdinejad, R. M. Parizi, G. Srivastava and A. Dehghantanha, "Making Sense of Blockchain for AI Deepfakes Technology," *IEEE Globecom Workshops*, Taipei, Taiwan (2020),
- [3] U. Patil et al. "An Effective Blockchain Technique to Resist Against Deepfake Videos," *Third International Conference on Inventive Research in Computing Applications*, Coimbatore, India, pp. 1646-1652 (2021).
- [4] T. Qiao, S. Xie, Y. Chen, F. Retraint and X. Luo, "Fully Unsupervised Deepfake Video Detection Via Enhanced Contrastive Learning," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 46, no. 7, pp. 4654-4668, July (2024),

- [5] M. S. Rana, M. N. Nobi, B. Murali and A. H. Sung, "Deepfake Detection: A Systematic Literature Review," in *IEEE Access*, vol. 10, pp. 25494-25513 (2022).
- [6] X. Wang, N. Thome and M. Cord, Gaze latent support vector machine for image classification improved by weakly supervised region selection. *Pattern Recognition*, vol. 72, pp. 59-71 (2017).
- [7] J. Donahue, L. Anne Hendricks, S. Guadarrama, M. Rohrbach, S. Venugopalan, K. Saenko and T. Darrell, Long-term recurrent convolutional networks for visual recognition and description, *IEEE Conference on Computer Vision and Pattern Recognition*, pp. 2625-2634 (2015).
- [8] E. Sabir, J. Cheng, A. Jaiswal, W. AbdAlmageed, I. Masi and P. Natarajan, Recurrent convolutional strategies for face manipulation detection in videos. *Interfaces*, vol. 3, no. 1, pp. 80-87 (2019).
- [9] J. A. Costales, S. Shiromani and M. Devaraj, "The Impact of Blockchain Technology to Protect Image and Video Integrity from Identity Theft using Deepfake Analyzer," *International Conference on Innovative Data Communication Technologies and Application*, Uttarakhand, India, pp. 730-733 (2023).
- [10] U. Patil, P. M. Chouragade and P. Ambhore, "An Effective Blockchain Technique to Resist Against Deepfake Videos," *3rd International Conference on Inventive Research in Computing Applications*, Coimbatore, India, pp. 1646-1652 (2021).
- [11] M. Jiwtode, A. Asati, S. Kamble and L. Damahe, "Deepfake Video Detection using Neural Networks," *IEEE International Conference on Blockchain and Distributed Systems Security*, Pune, India, pp. 1-5 (2022).
- [12] Ankit Kumar, Rajesh Mehta, and Priya Sharma, "An Enhanced Quantum Key Distribution Protocol for Security Authentication," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 22, no. 4, pp. 499-507 (2019).
- [13] Ghanimi, Hayder M. A., Melgarejo-Bolivar, Romel P., Tumi-Figueroa, Alfredo, Ray, Samrat, Dadheech, Pankaj & Sengan Sudhakar, Merkle-Damg hash functions and blockchains : Securing electronic health records, *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 27, no. 2-A, pp. 237-248 (2024).

