

See discussions, stats, and author profiles for this publication at: <https://www.researchgate.net/publication/370466813>

# An efficient security system based on cancelable face recognition with blockchain over cognitive IoT

Article in *Multimedia Tools and Applications* · May 2023

DOI: 10.1007/s11042-023-15534-3

CITATIONS

0

READS

111

3 authors:



**Randa Kamal**

Menoufia University

6 PUBLICATIONS 41 CITATIONS

SEE PROFILE



**Ezz El-Din Hemdan**

Menoufia University

86 PUBLICATIONS 1,203 CITATIONS

SEE PROFILE



**Nawal El-Fishawy**

Faculty of Electronic Eng., Menoufia University, Menouf, Egypt

221 PUBLICATIONS 2,087 CITATIONS

SEE PROFILE



# An efficient security system based on cancelable face recognition with blockchain over cognitive IoT

Randa Kamal<sup>1</sup> · Ezz El-Din Hemdan<sup>1</sup> · Nawal El-Fishway<sup>1</sup>

Received: 26 August 2021 / Revised: 28 December 2021 / Accepted: 19 April 2023

© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2023

## Abstract

This paper presents a new authentication framework for cancelable face recognition biometrics. In recent years, biometric plays a pivotal role in Cognitive Internet of Things (C-IoT) security. The face trait solves a lot of security issues; it increases the resistance of these systems against severe authentication attacks especially in smart IoT-based applications. The proposed scheme runs in two phases; The first phase (enrollment), in which the face image of the person is hashed using SHA256, is passed to an algorithm to extract the main features. Then the image is decomposed using a wavelet transform algorithm. Wavelet transform is applied to hide the face details from the image. This step is done to protect the image against being stolen or modified by external hackers. The image, hash, and wavelet transform are passed through the raspberry Pi to be stored in a database. A block is added to the private blockchain with these files. In the second phase (authentication) the test image is hashed, passed to the system to extract the features, and compared with the stored images in the database. Then the decision is stored in a new block in the chain, whether the two images are identical or not. The simulation results based demonstrate that the proposed cancelable biometric system gives a very reliable and secure performance for securing the IoT applications.

**Keywords** Blockchain · Cancelable biometrics · Image authentication · Machine learning · Face recognition

---

✉ Randa Kamal  
randa.soltan@te.eg

Ezz El-Din Hemdan  
ezzvip@yahoo.com

Nawal El-Fishway  
nelfishawy@hotmail.com

<sup>1</sup> Department of Computer Science and Engineering, Faculty of Electronic Engineering, Menoufia University, Menoufia, Egypt

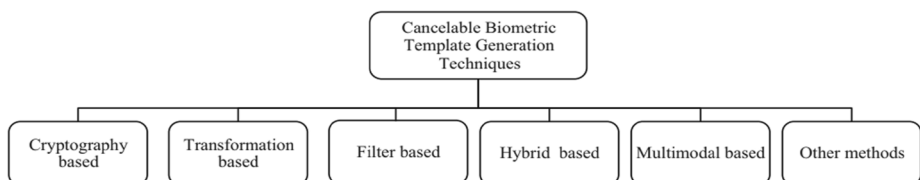
# 1 Introduction

Recently, superlative innovative and advanced technologies for instance Cloud and Internet of Things [4, 7, 8] mainly depend on the use of the network facilities for multimedia transmissions. Multimedia security has become one of the pretty research domains for many researchers around the world in numerous areas like Cloud and IoT Forensics [11]. In recent years, cancelable biometrics is widely used in various applications security. Cancelable biometrics is the art of using transformed or deformed versions of biometrics in the verification process [34]. It is one of the key types for biometric template protection principle as well biometric cryptosystem. Biometrics are widely used in various fields such as forensic, civilian, and commercial applications to launch identity in cybernetics, computational intelligence and human-machine systems, and computational intelligence [3].

Biometrics is defined as the automatic recognition of any person dependent on their physical or conduct attributes. The most commonly used biometrics in recent researches are fingerprints, faces, iris, and speech. Since biometric properties are implicitly associated with the person, they provide strong evidence of their identity [33]. Decomposition of cancelable biometrics can be achieved by many techniques; cryptography, transformation, filtering, hybrid methods, multimodal, or other methods. These methods are categorized in Fig. 1 [18]. The proposed framework applies wavelet transform for image hashing, as it defines a feature vector called short binary signature that characterizes the image independently.

In this work, we provide a new authentication framework for cancelable face recognition biometrics with blockchain for secure C-IoT applications. The main contribution of this work is as follows:

- Provide a new and efficient framework utilizing face images for providing a strong cancelable face-based authentication system with verifying the person through his/her faces. It can be more reliable and favored than existing methods that are used in building cancellable-based face recognition systems with the integration of blockchain as a novel contribution in this domain.
- Present an efficient cancellable biometric security system for smart Cognitive-IoT applications with providing protected and reliable face samples via sending through the blockchain network for secure face transfer over the Internet. Also, accomplish acceptable recognition accuracy rate and increase the security of IoT systems.
- Performing a methodical experimental evaluation of the proposed scheme through different experiment consequences over two different face datasets. The results assessment showed that the proposed scheme offered that the proposed approach attains supreme Blockchain-based cancellable biometric system.



**Fig. 1** Cancelable biometric template generation techniques [18]

This paper is structured as follows: Section 2 provides a summarized preliminary knowledge about blockchain, biometrics, wavelet transform, and face recognition. Section 3 briefly discusses the previous related work regarding the paper subject. Section 4 presents the proposed framework while the experimental environmental with results analysis are presented in Section 5. Finally, the conclusion and future scope are provided in Section 6.

## 2 Preliminary knowledge

In this section, we will briefly discuss the main knowledge points about blockchain, data integrity, and face recognition:

### 2.1 Blockchain

Blockchain is a decentralized database; named ledger. The blocks of blockchain are linked to each other in a linked list manner. The whole ledger is replicated among all participant nodes of the chain [19]. There are two main elements of each blockchain; which are transactions: which hold the action taken among the nodes and blocks: to record the transactions [30]. all blocks can be traced to the very first block; the genesis block.

The main characteristics of the blockchain are decentralization, anonymity, autonomy, speed, cost-saving, security, resiliency, and smart contracts. The blockchains are categorized according to the domain to the consortium, private, and public blockchain. They can be categorized according to authentications to permissioned or non-permissioned blockchains.

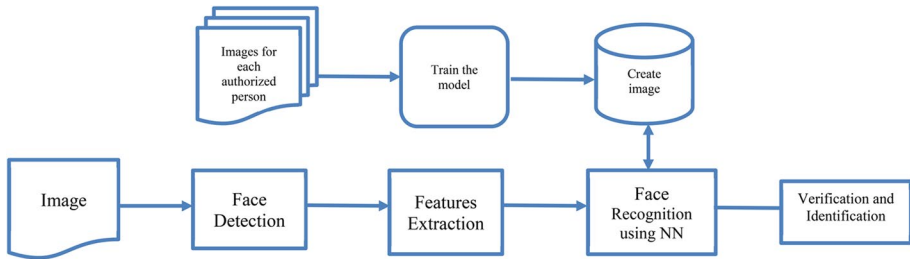
To add new blocks to the blockchain, consensus protocols are used for mining. There are many different protocols such as Proof-of-work (PoW), Proof-of-Stake (PoS), Delegate PoS (DPoS), Practical Byzantine Fault Tolerance (PBFT). Each protocol has its characteristics that are suitable for certain applications and blockchain types [32].

### 2.2 Biometrics

The biometric technology identifies and verifies personal features with an accurate, fast, and convenient way to control access to specific systems or applications [13]. Biometrics is defined as the unique physical (fingerprint, palm print, retina, iris, and face) or logical (voice, signature, keystroke pattern, and walking style) measured characteristics or traits of the human body, which are employed to ensure that only authorized individuals have access to the rendered services [13].

### 2.3 Face recognition

As mentioned in [17], for a face recognition system to be useful it has to ensure some characteristics: the ability to work with images and videos, the robustness in different conditions of lighting, and the ability to work with faces from different angles. The structure of the proposed face recognition system is shown in Fig. 2. This face recognition system has three basic phases:



**Fig. 2** A Typical Face Recognition System

1. **Face detection:** to make sure whether there is a human face in the image/video or not using different techniques; histogram of oriented gradient (HOG), principal component analysis (PCA), or Viola-Jones detector.
2. **Feature extraction:** in this phase, the signature of the face is presented; nose, mouth, eyes..etc. using different techniques; HOG, Haar wavelets, independent component analysis (ICA), linear discriminant analysis (LDA), and many more.
3. **Face recognition:** in the last phase, the extracted signature of the detected face is compared to the faces stored in the database for identification and verification of the face using Correlation filters (CFs), convolutional neural network (CNN), or other techniques.

## 2.4 Wavelet transform

Wavelet transform is one of the most widely used mathematical tools in recent years, which can extract information from images effectively. It is used to decompose the histogram of the image in multi-scale. Firstly, the rough value of the image segmentation threshold is found on a large scale, and then the scale is gradually reduced to locate the segmentation threshold accurately. The image segmentation method based on wavelet transform can effectively avoid the influence of noise [10].

## 3 Related work

Many research papers related to cancelable face recognition in the last years. However, recently blockchain has attracted wide interest in this subject. In [34], the authors proposed a cancelable color face recognition algorithm based on a full quaternion matrix and an extreme learning machine. The structural information (local variance and gradient) and color components are respectively served as the real and imaginary parts to construct a full quaternion matrix. They aimed to make images completely invisible via using the random permutation operation. The proposed system in [3] suggests novel two proposed cancellable biometric realization techniques recognition and template protection by utilizing Homomorphic Key (HK) encoding for cancelable face system. In [1], presents several cancelable fusion-based face recognition (FR) methods; region-based, multi-biometric, and hybrid-feature.

In [2], the authors suggest two novels presented cancellable biometric realization approaches recognition and template protection. The first approach is applied by applying

the ATrous Transform (AT), and the Homomorphic Filtering Masking (HFM) encoding. The second approach presents a new technique for Facial Expression Recognition detection using Canny Edge Detection (CD) and Hough Transform (HT).

In [31], they introduced a cancelable fingerprint biometric system based on the Hadamard transform implemented on the binary representation of the fingerprint minutiae. Authors in [5] proposed a blockchain-based video integrity framework to verify the authenticity of a video captured by a streaming IoT device for forensic investigation purposes. In [16], the authors proposed A blockchain-based Data Verification System for CCTV Surveillance Cameras in Smart Cities. In [23], the authors proposed a lightweight blockchain-based framework for data integrity for surveillance cameras. In [22], the authors proposed blockchain-based video forensics and integrity verification framework for IoT devices. In [14], the authors proposed a framework for enhancing control management, security, and comfortability of smart homes using biometric techniques and cloud services. Authors in [24] proposed a framework for smart home security and automation based on face and speech recognition.

In [6], the authors proposed a blockchain-based face recognition system based on artificial intelligence and edge computing. Authors in [27] proposed a framework for securing face recognition Systems by applying blockchain technology. In [9], they developed a multi-level security framework for telehealthcare services is provided using hybrid cryptography and watermarking. In [15], the authors provided and proposed a new blockchain-based framework for the integrity verification of videos. In [26], the authors developed an efficient iris recognition model based on chaotic encryption and deep Convolutional Neural Networks (CNNs) is proposed for C-IoT applications. In [12, 20, 21] presented techniques for Detecting Deepfake Videos and applying steganographic methods.

Most of the recent work in face recognition focused only on using traditional techniques for building cancelable systems. Therefore, our work aims to provide a new security blockchain-based framework for enhancing biometric security through presenting a new authentication framework for cancelable face recognition biometrics for cognitive IoT applications.

## 4 Proposed system

In recent years, face-based biometric recognition is widely used for security purposes, but the face images are stored on third-party servers in most cases. Since the sensitive information of an individual is contained in the facial image such as the age and health condition, it is necessary to protect its privacy and security [34]. As most if not all digital devices of these days which are used for capturing data can capture colored images, we applied our system on colored images. to protect human privacy, cryptography-based-biometric recognition is a promising approach.

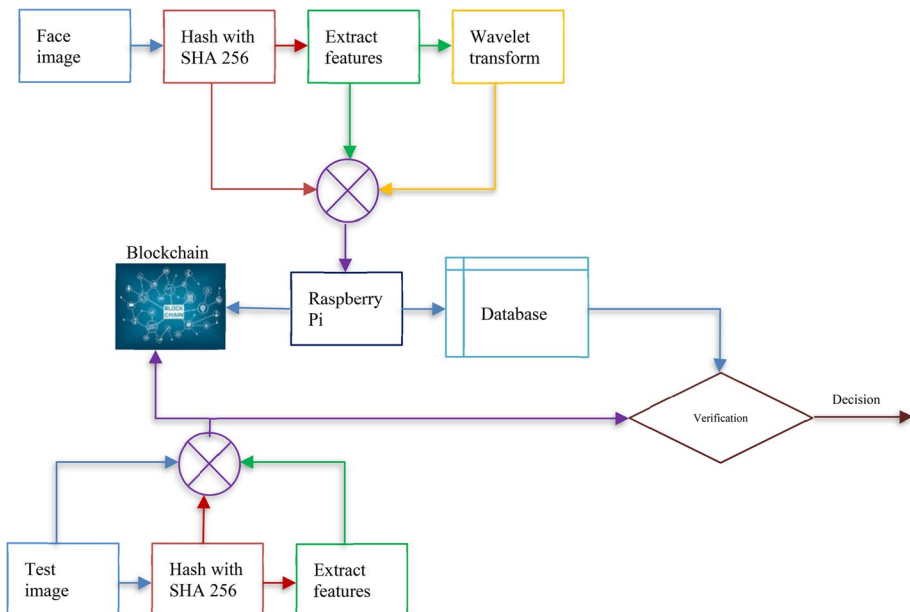
In the proposed system, the Haar cascade classifier is applied for face recognition. The result of the classifier is either positive or negative pictures for the trained classifier. Each feature of the face in the image is acquired by subtracting the sum of pixels in a white rectangle from the summation of pixels in a black rectangle. In which it detects the faces of different individuals in different environments. Haar classifier has high accuracy in face recognition than other face recognition algorithms. The input image is first converted into grayscale. The cascade classifier detects the face, then it checks for eyes, then it normalizes the face images size and orientation. [28, 29].

In the proposed system, two-tier security schemes to secure the face images of any application user are applied. Figure 3 as the following:

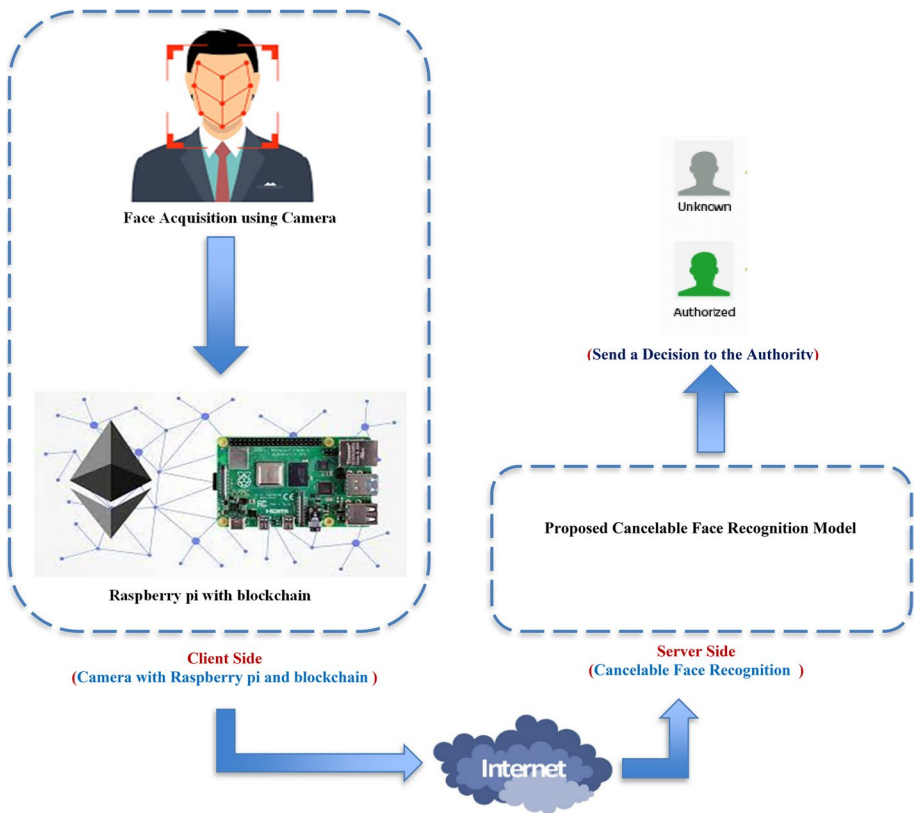
1. **Phase 1:** the enrolment: in which the reference image is hashed via SHA 256 algorithm, extracting face features from the image using the Haar cascade classifier. The image then is decomposed via wavelet transform to hide the face details. All the images, decomposed image, hash value, and the file containing the extracted features are passed to Raspberry Pi; which then propagates these files to the ledger by creating a new block. All files are stored as well in local storage for later authentication.
2. **Phase 2:** the test image is inserted into the system. It is hashed by SHA 256, extracting the face features using haar cascade classifier, these files are passed to Raspberry pi which compares the hash value and the extracted features with the stored in the database to make the decision; authenticated or not.

The proposed framework considers enrollment and authentication processes over the C-IoT authentication server. The proposed cancelable face recognition biometrics system uses wavelet transform and blockchain. Figure 4 illustrates the complete structure of the proposed framework over C-IoT. The proposed framework consists of two sides, client-side, and server-side. The Client-side is practically instigated using a raspberry [25], keyboard, mouse, screen, and a cable for internet connection through this system the block-chain network is executed. It is supposed that will be sensing devices to capture the face images from users for authentication objectives.

The server side is practically employed using a laptop and a cable for internet connection as shown in Fig. 5 which is used for authentication and recognition purposes. The proposed framework architecture comprises of main stages as follows:



**Fig. 3** Flowchart of the proposed system



**Fig. 4** Structure of the proposed Cancellable Face Recognition with Blockchain Over Cognitive IoT framework

- **Stage 1 at the client-side:** This stage includes two steps;
  - (1). Face Acquisition;
  - (2). Sending the face to the enrollment and the authentication server after passing through the blockchain network over the internet.
- **Stage 2 at the server-side:** This stage includes applying the proposed cancelable face recognition system over the server.

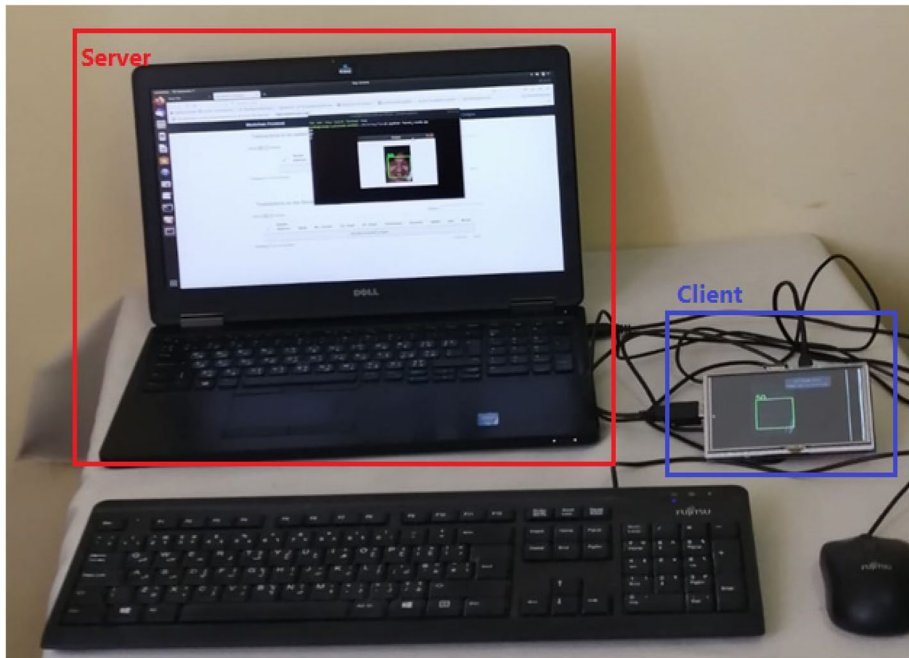
## 5 Experimental study and results analysis

This section provides the experimental setup with evaluation results analysis.

### 5.1 Experiment installation

The proposed system is accomplished and implemented on a dell laptop core i5 CPU 2.30 GHz, 8 GB RAM, 256 GB SSD storage, Ubuntu 11.3 (64 bit). Besides, Raspberry Pi





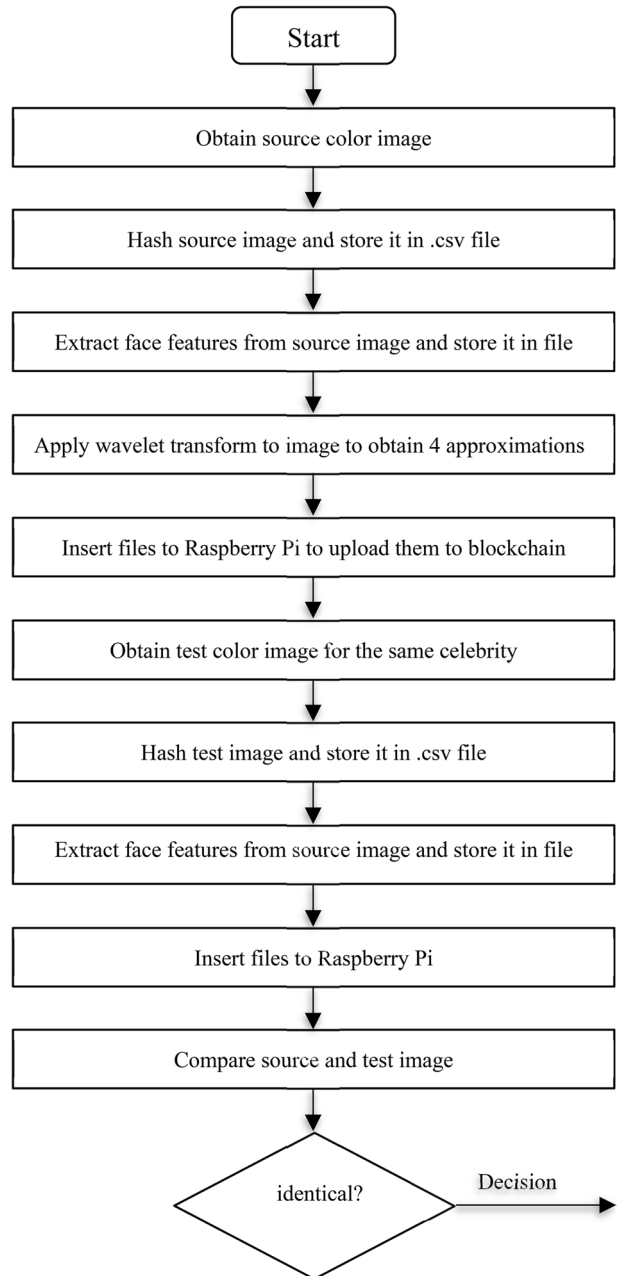
**Fig. 5** The practical physical connection and used devices in the proposed system

3. Also, Python 3.7 is used for programming the proposed system. There were two datasets used to test our algorithm: the first one is: 5-celebrity-faces-dataset. It contains images of 5 celebrities; Ben Affleck, Elton John, Jerry Seinfeld, Madonna, and Mindy Kaling. The other dataset is the GTdb\_crop face dataset which contains 50 different persons, with 15 different images for each person captured with different imaging angles.

## 5.2 Assessment steps

The following steps show the phases of our system, the algorithms 1 to 3 of the system, Fig. 6 shows the flowchart of the proposed framework. Figures 7, 8, 9, 10, 11, 12, 13 and 14 show snapshots during the execution of the system and the results of the experiments on both datasets as follows:

1. Source images were obtained from each dataset.
2. Each image is hashed using SHA256 and the value is stored in (image\_name.csv).
3. In python, a file named train.py is executed. This file takes the images from (1) to extract face features. The features are saved for each image in ('image\_name'\_enc).
4. Another python file named wavelet.py is executed for each image to decompose the image. The result is 4 approximation images for each source image. The approximations are cA, cH, cV, cD.
5. All the resultant files from 2,3,4 are then passed to the Raspberry Pi which is connected to the private blockchain.

**Fig. 6** Flow chart of the proposed framework

```
File Edit View Search Terminal Help
randa@randa-Latitude-E5550:~/paper5/blockchain/blockchain_client$ python blockchain_client.py
* Serving Flask app "blockchain_client" (lazy loading)
* Environment: production
WARNING: This is a development server. Do not use it in a production deployment.
Use a production WSGI server instead.
* Debug mode: off
* Running on http://127.0.0.1:8080/ (Press CTRL+C to quit)
127.0.0.1 - - [28/Feb/2021 22:55:25] "GET / HTTP/1.1" 200 -
127.0.0.1 - - [28/Feb/2021 22:55:26] "GET /static/vendor/bootstrap/css/bootstrap.min.css HTTP/1.1" 200 -
```

**Fig. 7** Open `blockchain_client.py` file “the blue rectangle shows the URL to view the blockchain client on the browser”

6. Run both `blockchain.py` and `blockchain_client.py` to create the permissioned blockchain. Both files give a URL to open in the browser. Open both to complete the blockchain creation. To grant privileges blockchain clients generate an account tab that is opened for the authorized participants and generate random public and private keys to be used in creating blocks. Algorithm 1 shows the description of this step.
7. A new block is created with the source image, CSV file, approximation images, and the hash value and propagated to the participant nodes of the blockchain.
8. The last phase in the system is authentication. The test image is hashed, inserted into the python code for face feature extraction as steps 2,3. Then the resultant files are compared to the files stored in the database. A decision is then made; whether or not the source and test images are identical.
9. A new block is created according to step 8 decisions and propagated to participant nodes.

---

**Algorithm 1:** Create a blockchain account

---

**Result:** an account is created

**Initialization**

Generate random public key  
Generate a random private key

---



---

**Algorithm 2:** create hash, features, approximations from source color image

---

**Input:** colored face image of each celebrity

**Result:** SHA256 value, extracted features, approximation images of the input image

**Initialization**

Hash the image using SHA 256  
Extract face features using haar function in python  
Store the features in ('celebrity\_name'\_enc)  
Apply wavelet transform with the approximations  $cA$ ,  $cH$ ,  $cV$ ,  $cD$   
Save files in the database  
Pass files to Raspberry Pi

---

**Algorithm 3:** Extract face features using haar function

---

**Input:** colored face images**Result:** extracted face features**Initialization**

Load the input image

Convert it to grayscale mode

Load the haar cascade classifier

$$\text{Pixel value} = (\text{Sum of the Dark pixels} / \text{Number of Dark pixels}) - (\text{Sum of the Light pixels} / \text{Number of Light pixels})$$

---

**Algorithm 4:** Add a new block to the chain

---

**Input:** SHA256 value, extracted features, approximation images of the input image**Result:** a new block added to the chain**Initialization****If** *authorized public and private keys*, **then**

SHA256 value, extracted features, approximation images of the input image

Mine

Add new block

**End**

---

The following algorithms show the steps of the proposed model, while Figs. 6, 7, 8, 9, 10, 11 and 12 show the results of the experimental work during system execution and testing. The practical testing of the proposed system for face detection is shown in Fig. 15. Likewise, Fig. 16 shows how the proposed system can detect a test image as an authorized user.

### 5.3 Comparative analysis

From the previous discussion, our framework outperforms the related literature in the following points as shown in Table 1. A cancelable biometric framework for face recognition based on blockchain is proposed and compared with other work.

To evaluate the proposed system, a comparative analysis for face recognition techniques; CNN and Haar cascade classifier is shown in Table 2.

For comparison, the proposed system applied face recognition using both techniques. The comparison was held to the Gtdb\_crop dataset. When Haar cascade classifier is applied, the recorded time was 13 s and it reaches 96% accuracy. When CNN is applied and many different dense neurons, epochs, and steps were tried to reach the most efficient system. Each experiment was done 10 times, the average time and accuracy were recorded as tabulated in Table 3.

```
File Edit View Search Terminal Help
randa@randa-Latitude-E5550:~/paper5/blockchain/blockchain$ python blockchain.py
* Serving Flask app "blockchain" (lazy loading)
* Environment: production
WARNING: This is a development server. Do not use it in a production deployment.
Use a production WSGI server instead.
* Debug mode: off
* Running on http://127.0.0.1:5000/ (Press CTRL+C to quit)
```

Fig. 8 Open blockchain.py file “the blue rectangle shows the URL to view the blockchain on the browser”

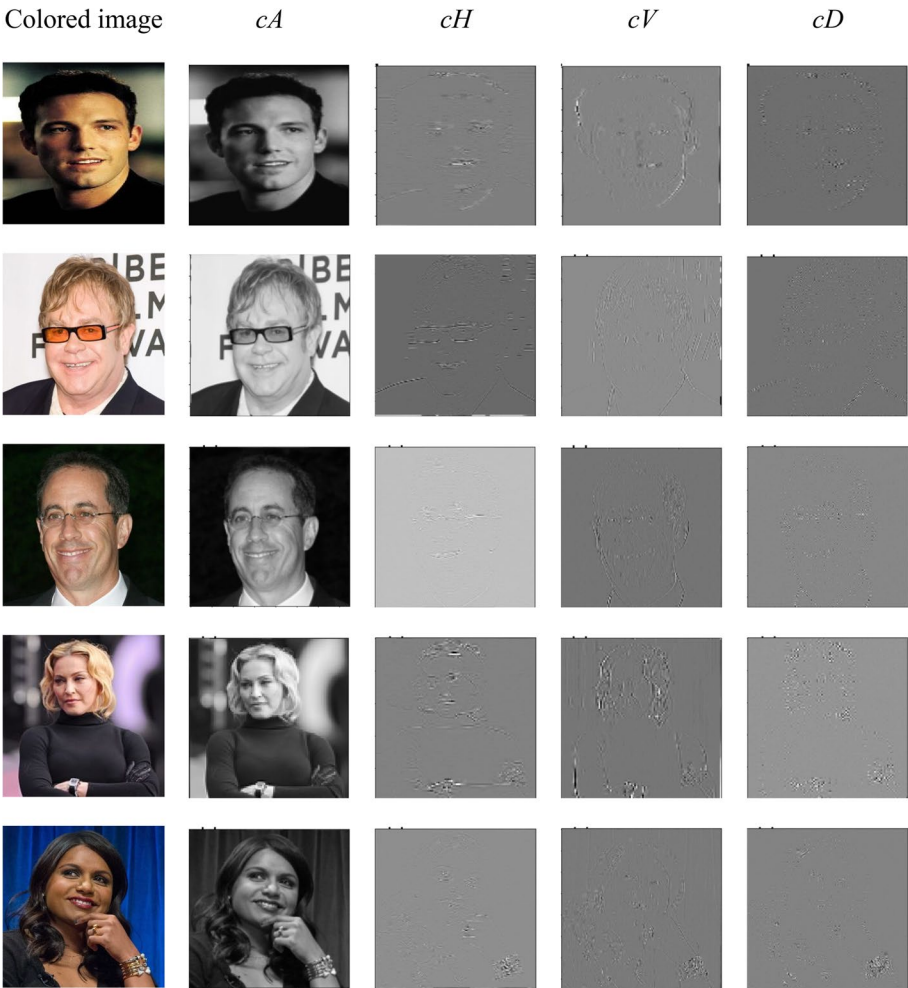


Fig. 9 Wavelet transform for 5- celebrities dataset

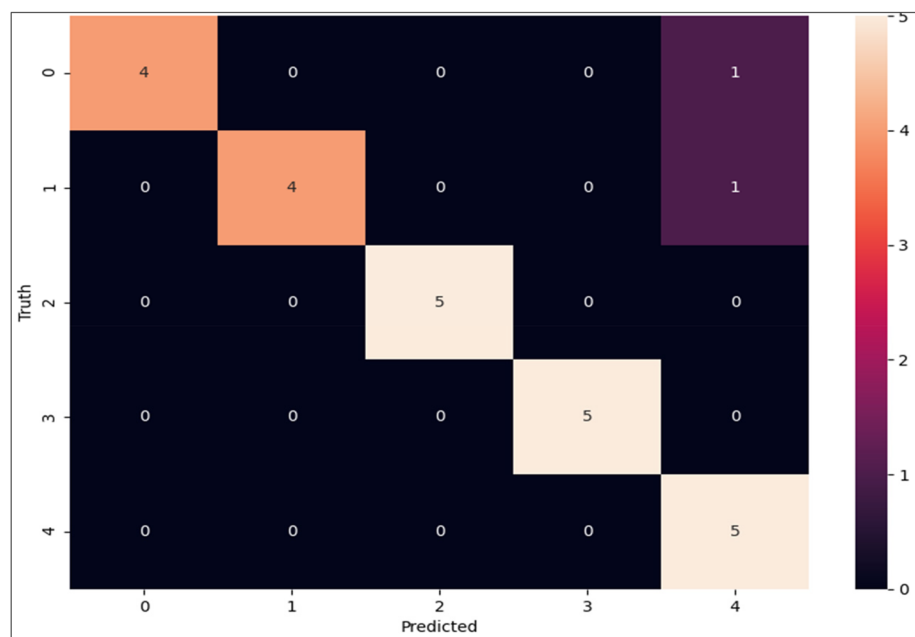


Fig. 10 Confusion matrix for 5-celebrities dataset

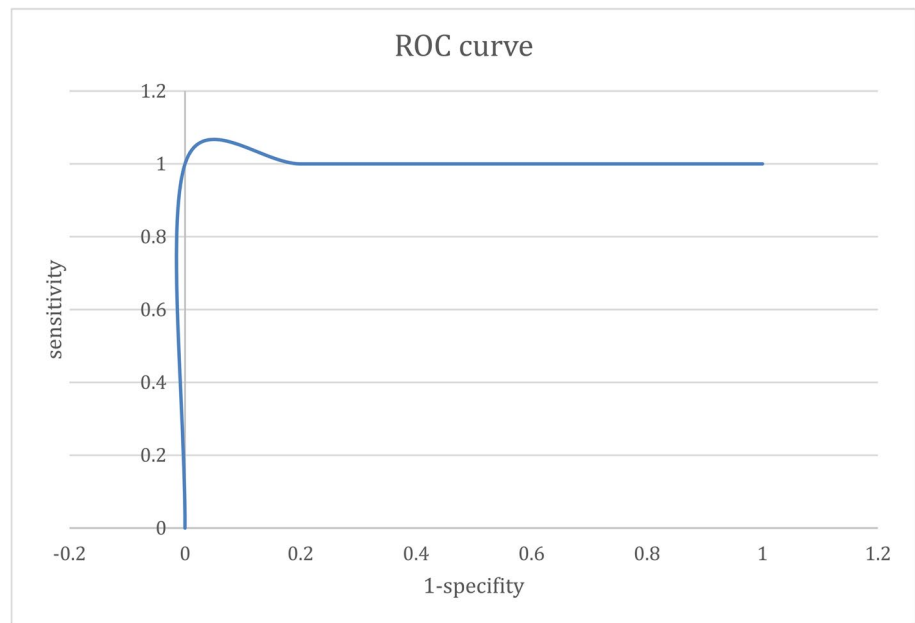


Fig. 11 Roc curve for 5- celebrities dataset

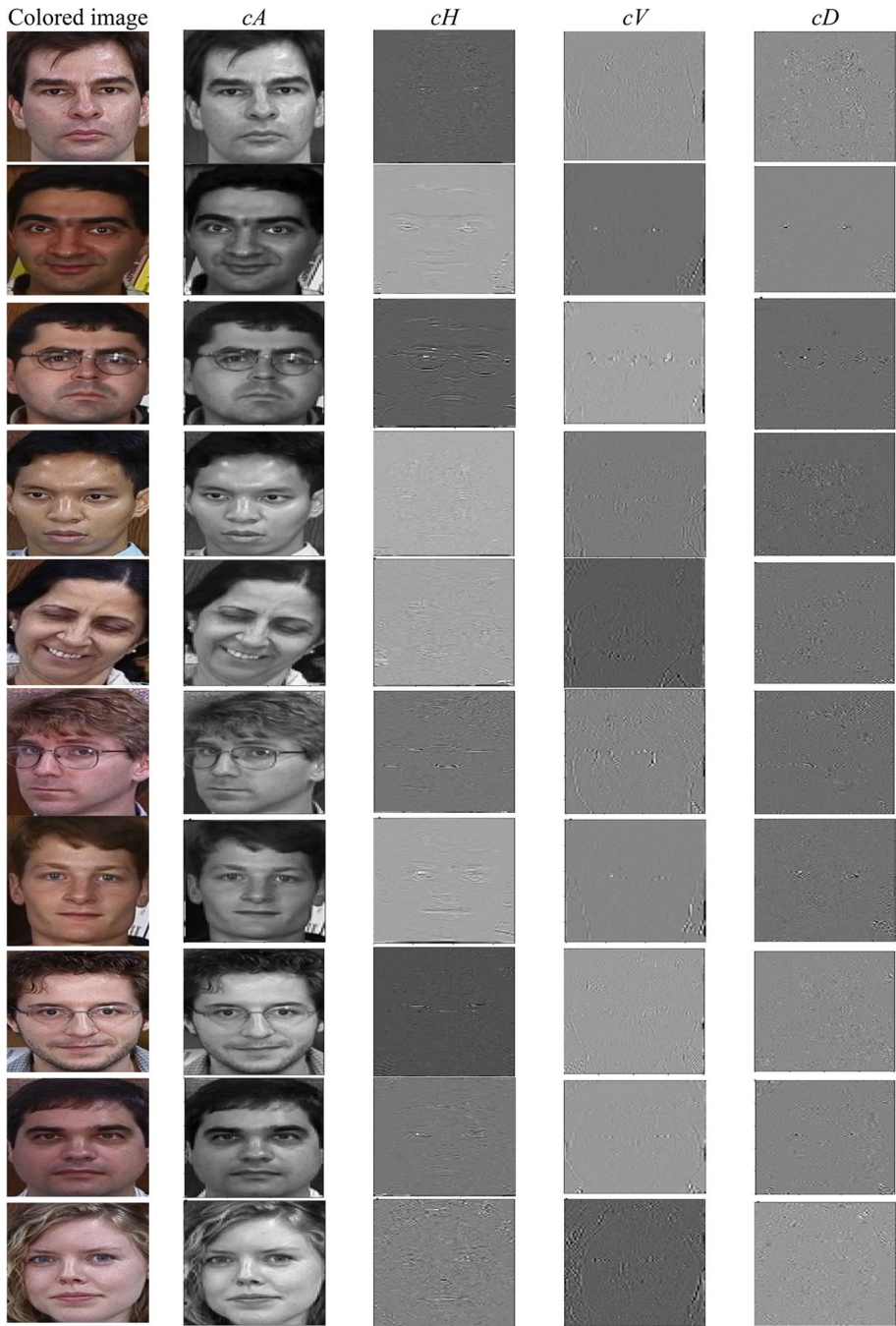
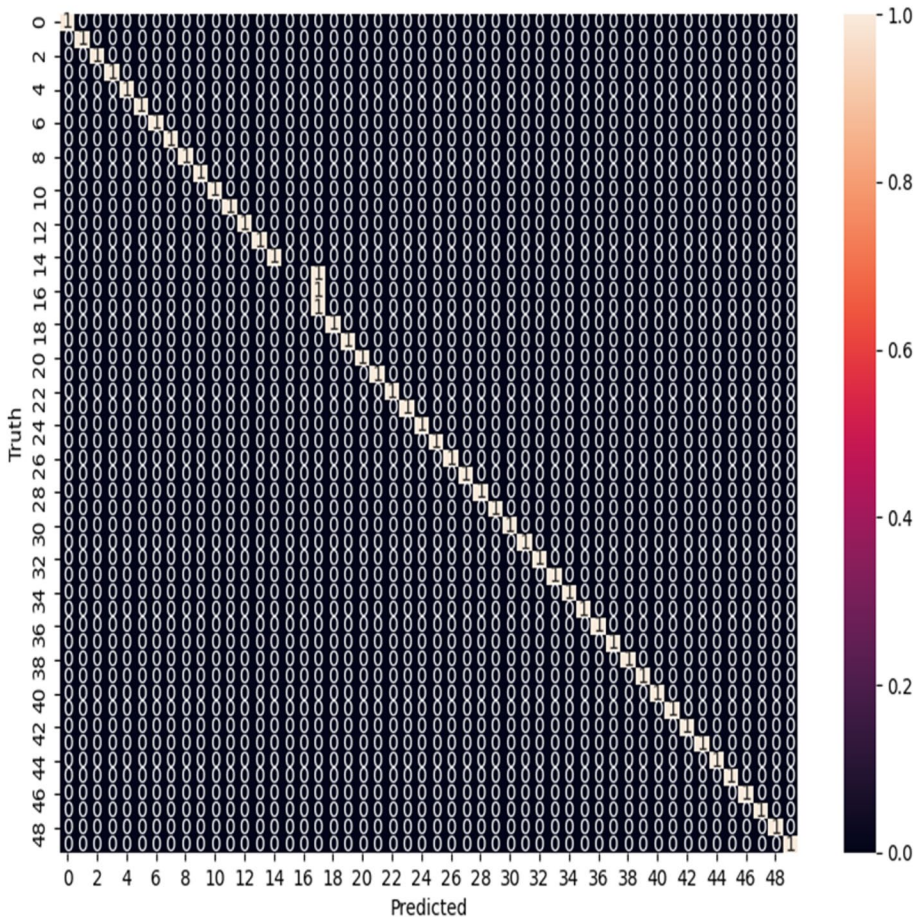


Fig. 12 Wavelet transforms for 10 sample images of GTdb\_crop dataset





**Fig. 13** Confusion matrix for GTdb\_crop dataset

The results in Table 3 shows that best accuracy; 93% was obtained by 128 dense neurons, 5 steps, 30 epocs. However, it takes much more time than haar cascade classifier; 51 s. While haar cascade classifier reaches 96% accuracy in only 13 s.

For cancelable techniques, wavelet transform was compared with Cartesian and multiplicative transforms. Table 4 shows a comparison between the three methods for the sample image of Gtdb\_crop. Wavelet transform is an acceptable method for cancelability in the case of processing time. Wavelet transform provides 4 transformations “cA, cH, cV, cD” which gives more security options, however, it takes more storage.



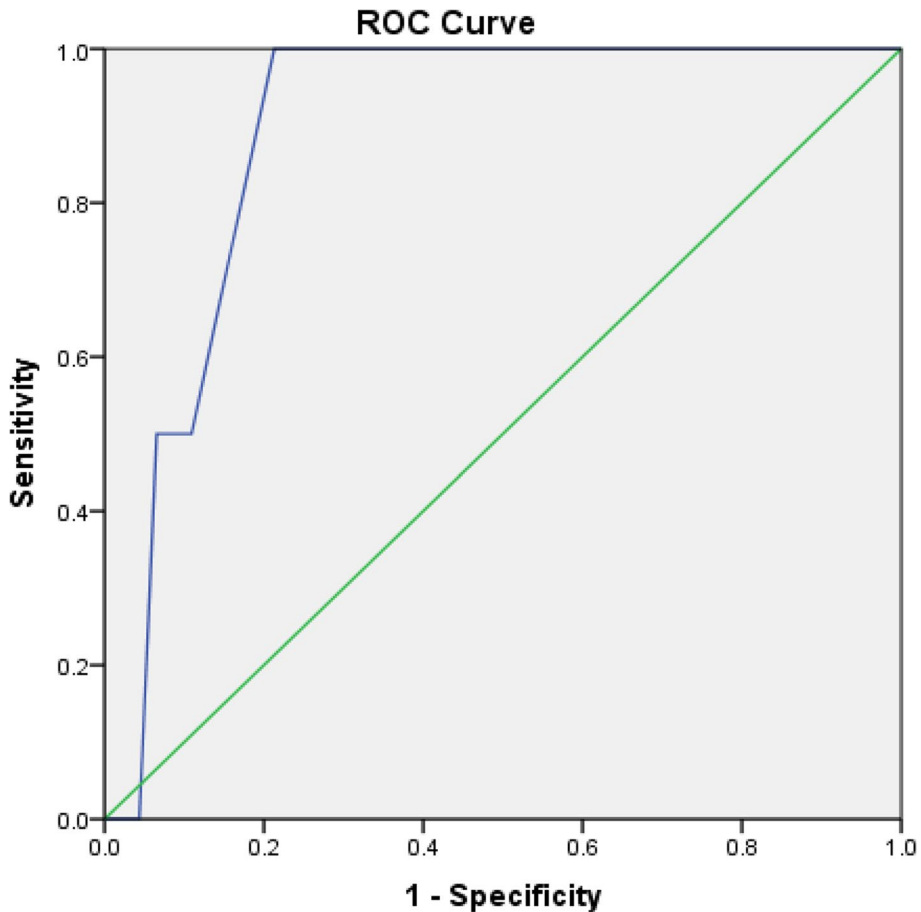


Fig. 14 Roc curve for GTdb\_crop dataset

## 6 Conclusion and future scope

This paper presents a cancelable biometric framework for face recognition based on blockchain. In this framework, the source image is hashed, face features are extracted from the image. The image then is composed via wavelet transform to hide the face details of the person. Source image, hash value, wavelet transformations are stored in the ledger of the permissioned blockchain via a Raspberry Pi 3. For authentication, the test image is hashed, face features are extracted from the image and compared to the stored values and files. The decision and files are stored again in the blockchain. The experimental results from evaluation the proposed framework with two common datasets namely 5-celebrities, and the GTdb\_crop. It shows reliable performance. For comparison, 2 face recognition techniques were applied for GTdb\_crop dataset; CNN and haar cascade classifier. The results show that haar cascade classifier is higher in accuracy and lower in consumed time (96%, 13 s) than CNN (93%, 51 s). For cancelable, 3 techniques were applied for comparison; Cartesian, Multiplicative, Wavelet transforms. Results show that wavelet transform is better in cancelability, however it needs more disk storage. The accuracy of



Fig. 15 The practical testing of the proposed system for face detection



Fig. 16 The proposed system detects a test image as an authorized user

**Table 1** A comparison between and proposed framework and existing work

Work	BC	Data Integrity	Storage Preservation	Face Recognition	Cancelable Biometric
[34]	×	×	✓	✓	✓
[3]	×	×	×	✓	✓
[33]	×	×	×	✓	✓
[18]	×	×	✓	✓	✓
[19]	✓	✓	×	×	×
[30]	✓	✓	×	×	×
[32]	✓	✓	×	×	×
[13]	✓	✓	×	×	×
[17]	×	×	×	✓	×
[10]	×	×	×	✓	×
[1]	✓	✓	×	✓	×
[2]	✓	✓	×	✓	×
Proposed framework	✓	✓	✓	✓	✓




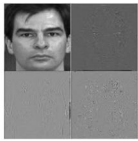
**Table 2** A comparison between haar cascade classifier and CNN for face recognition

Technique	Pros	Cons
Haar cascade classifier	1-Works almost real-time on CPU 2-Simple Architecture 3-Detects faces at different scales	1- False predictions 2-Not work on non-frontal images 3-Not work under occlusion
CNN	1-Works for different face orientations 2-Robust to occlusion 3-Works very fast on GPU 4- Easy training process	1-Very slow on CPU 2-Not detect small faces 3-The bounding box is small

**Table 3** The results of CNN face recognition

No. of dense neurons	Steps	Epocs	Time in seconds	Accuracy (%)
64	5	15	26	36
64	5	20	34	22
128	5	15	26	29
128	5	20	35	43
<u>128</u>	<u>5</u>	<u>30</u>	<u>51</u>	<u>93</u>
128	8	30	70	87

**Table 4** The results of the wavelet transform method

	Original	Cartesian	Multiplicative	Wavelet
Image				
Time		0 sec	2sec	0sec
Image size	14KB	30KB	38KB	45KB

the projected framework was 92%, 95% for 5-celebrities, and GTdb\_crop datasets respectively. Also, the proposed system provided more features compared to existing work through the utilization of both cancelable face recognition and blockchain for securing the C-IoT applications. In the future, we plan to apply the proposed system with evaluating its performance using different biometrics datasets such as iris, fingerprint to generate a multi-biometric model-based cancellable system with blockchain. Likewise, apply it in real-life Cognitive-IoT applications.

**Data Availability** Data available on request from the authors.

## Declarations

**Ethical approval** All procedures performed in studies involving human participants were in accordance with the ethical standards of the institutional and/or national research committee and with the 1964 Helsinki declaration and its later amendments or comparable ethical standards.

**Informed consent** Informed consent was obtained from all individual participants included in the study.

**Conflict of interest** The authors declare that they have no conflict of interest.

## References

1. Abdellatef E et al (2019) Cancelable fusion-based face recognition. *Multimed Tools Appl* 78(22):31557–31580
2. Ashiba HI (2021) Proposed framework for cancelable face recognition system. *Multimed Tools Appl* 80(9):13677–13705
3. Ashiba HI, Abd El-Samie FE (2020) Implementation face based cancelable multi-biometric system. *Multimed Tools Appl* 79(41):30813–30838
4. Atlam HF et al (2020) Internet of things forensics: a review. *Internet Things* 11:100220
5. Danko D, Mercan S, Cebe M, Akkaya K (2019) Assuring the integrity of videos from wireless-based IoT devices using blockchain. In: 2019 IEEE 16th International Conference on Mobile Ad Hoc and Sensor Systems Workshops (MASSW), Nov, pp 48–52
6. Dirgantoro KP, Lee JM, Kim DS (2020) Generative adversarial networks based on edge computing with blockchain architecture for security system. In: 2020 International Conference on Artificial Intelligence in Information and Communication (ICAIC). IEEE, pp 039–042
7. El-Din HE, Manjaiah DH (2017) Internet of things in cloud computing. *Internet of things: novel advances and envisioned applications*, pp 299–311
8. El-Din HE, Manjaiah DH (2017) Internet of nano things and industrial internet of things. *Internet of things: novel advances and envisioned applications*. Springer, Cham, pp 109–123

9. El-Shafai W, Hemdan EE-D (2021) Robust and efficient multi-level security framework for color medical images in telehealthcare services. *J Ambient Intell Humaniz Comput*:1–16
10. Gao J et al (2020) A wavelet transform-based image segmentation method. *Optik* 208:164123
11. Hemdan EE-D, Manjaiah DH (2020) Digital investigation of cybercrimes based on big data analytics using deep learning. *Deep learning and neural networks: concepts, methodologies, tools, and applications*. IGI Global, pp 615–632
12. Hu J et al (2021) Detecting compressed deepfake videos in social networks using frame-temporality two-stream convolutional network. *IEEE Trans Circuits Syst Video Technol* 32:1089–1102
13. Ibrahim S et al (2020) Cancelable face and fingerprint recognition based on the 3D jigsaw transform and optical encryption. *Multimed Tools Appl*:1–26
14. Kak SF, Mustafa FM (2019) Smart home management system based on face recognition index in real-time. In: 2019 International Conference on Advanced Science and Engineering (ICOASE). IEEE, pp 40–45
15. Kamal R, Hemdan EE-D, El-Fishway N (2021) Video integrity verification based on blockchain. 2021 International Conference on Electronic Engineering (ICEEM). IEEE
16. Khan PW, Byun Y-C, Park N (2020) A data verification system for CCTV surveillance cameras using blockchain technology in smart cities. *Electronics* 9(3):484
17. Kortli Y, Jridi M, Al Falou A, Atri M (2020) Face recognition systems: a survey. *Sensors* 20(2):342
18. Kumar N (2020) Cancelable biometrics: a comprehensive survey. *Artif Intell Rev* 53(5):3403–3446
19. Li X, Jiang P, Chen T, Luo X, Wen Q (2020) A survey on the security of blockchain systems. *Futur Gener Comput Syst* 107:841–853
20. Liao X, Wen Q, Zhang J (2012) A novel steganographic method with four-pixel differencing and exploiting modification direction. *IEICE Trans Fundam Electron Commun Comput Sci* 95(7):1189–1192
21. Liao X et al (2020) Robust detection of image operator chain with two-stream convolutional neural network. *IEEE J Sel Top Signal Process* 14(5):955–968
22. Mercan Suat et al (2021) Blockchain-based video forensics and integrity verification framework for wireless Internet-of-Things devices. *Secur Privacy* 4(2):e143
23. Michelin RA, Ahmed N, Kanhere SS, Seneviratne A, Jha S (2020) Leveraging lightweight blockchain to establish data integrity for surveillance cameras. In: 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC). IEEE, pp 1–3
24. Munir A, Ehsan SK, Raza SM, Mudassir M (2019) Face and speech recognition based smart home. In: 2019 International Conference on Engineering and Emerging Technologies (ICEET). IEEE, pp 1–5
25. Raspberry Pi Foundation (2020) Raspberry Pi 2. Available at <https://www.raspberrypi.org/products/raspberry-pi-2-model-b/>. Accessed July 2021
26. Shalaby AS et al (2021) An efficient CNN based encrypted Iris recognition approach in cognitive-IoT system. *Multimed Tools Appl*:1–24
27. Shankar S, Madarkar J, Sharma P (2020) Securing face recognition system using blockchain technology. In: International conference on machine learning, image processing, network security and data sciences. Springer, Singapore, pp 449–460
28. Shetty AB, Bhoomika D, Rebeiro J, Ramyashree (2021) Facial recognition using Haar cascade and LBP classifiers. *Global Trans Proc* 2:330–335
29. Surve M, Joshi P, Jamadar S, Vharkate M (2020) Automatic attendance system using face recognition technique. *Int J Recent Technol Eng (IJRTE) IEEE* 9(1):2134–2138
30. Tseng L, Yao X, Otoum S, Aloqaily M, Jararweh Y (2020) Blockchain-based database in an IoT environment: challenges, opportunities, and analysis. *Clust Comput* 23(3):2151–2165
31. Wang S, Deng G, Hu J (2017) A partial Hadamard transform approach to the design of cancelable fingerprint templates containing binary biometric representations. *Proc Pattern Recognit* 61:447–458
32. Wang Q, Huang J, Wang S, Chen Y, Zhang P, He L (2020) A comparative study of blockchain consensus algorithms. In: *Journal of physics: conference series*, vol 1437, no 1. IOP Publishing, pp 012007
33. Yang W, Wang S, Hu J, Zheng G, Valli C (2018) A fingerprint and finger-vein based cancelable multi-biometric system. *Pattern Recognit* 78:242–251
34. Zakaria Y et al (2019) Cancelable multi-biometric security system based on double random phase encoding and cepstral analysis. *Multimed Tools Appl* 78(22):32333–32355

**Publisher's note** Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Springer Nature or its licensor (e.g. a society or other partner) holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.

**Randa Kamal Soltan** has received her B.Sc. from The Department of Computers and Control, Faculty of Engineering, Tanta University, Tanta, Egypt, in 2001. She received her M.Sc. from The Department of Computers and Control, Faculty of Engineering, Tanta University, Tanta, Egypt, in 2017. She is currently studying for a Ph.D. degree in computer science from the Department of Computer Science and Engineering, Faculty of Electronic Engineering, Menoufia University, Egypt. She is currently the Head of the IT support sector in Telecom Egypt “WE”, Egypt. Her current research interests include the Internet of Things (IoT), Blockchain, Digital Forensics, Cyber security.



**Ezz El-Din Hemdan** has received his B.Sc from the Department of Computer Science and Engineering, Faculty of Electronic Engineering, Menoufia University, Egypt, in 2009. He received his M.Sc. From the Department of Computer Science and Engineering, Faculty of Electronic Engineering, Menoufia University, Egypt, in 2013. He received his Ph.D. degree in the Department of Computer Science, Mangalore University, India in 2018. He has several publications in national/international conferences and journals. His research area of interest includes; Canacelable Biometric, Blockchain, Digital Twins, Image Processing, Virtualization, Cloud Computing, Internet of Things/Nano-Things, Cryptography, Data Hiding, Digital Forensics, Cloud Forensics, Big Data Forensics, Data Science and Big Data Analytics.



**Nawal El-Fishawy** received a Ph.D. degree in mobile communications from, Faculty of Electronic Eng., Menoufia University, Menouf, Egypt, in collaboration with Southampton University in 1991. Her research interest includes computer communication networks with emphasis on protocol design, traffic modeling, and performance evaluation of broadband networks and multiple access control protocols for wireless communications systems and networks. Now she directed her research interests to the developments of security over wireless communications networks (mobile communications, WLAN, Bluetooth), VOIP, and encryption algorithms. She has served as a reviewer for many national and international journals and conferences.