Multimedia Tools and Applications (2021) 80:14137–14161
https://doi.org/10.1007/s11042-020-10284-y

PSO–Blockchain-based image steganography: towards a new method to secure updating and sharing COVID-19 data in decentralised hospitals intelligence architecture

A. H. Mohsin, et al. ***[full author details at the end of the article]***

Received: 29 May 2019 / Revised: 17 September 2020 / Accepted: 22 December 2020 /
Published online: 22 January 2021

Abstract

Secure updating and sharing for large amounts of healthcare information (such as medical data on coronavirus disease 2019 [COVID-19]) in efficient and secure transmission are important but challenging in communication channels amongst hospitals. In particular, in addressing the above challenges, two issues are faced, namely, those related to confidentiality and integrity of their health data and to network failure that may cause concerns about data availability. To the authors' knowledge, no study provides secure updating and sharing solution for large amounts of healthcare information in communication channels amongst hospitals. Therefore, this study proposes and discusses a novel steganography-based blockchain method in the spatial domain as a solution. The novelty of the proposed method is the removal and addition of new particles in the particle swarm optimisation (PSO) algorithm. In addition, hash function can hide secret medical COVID-19 data in hospital databases whilst providing confidentiality with high embedding capacity and high image quality. Moreover, stego images with hash data and blockchain technology are used in updating and sharing medical COVID-19 data between hospitals in the network to improve the level of confidentiality and protect the integrity of medical COVID-19 data in grey-scale images, achieve data availability if any connection failure occurs in a single point of the network and eliminate the central point (third party) in the network during transmission. The proposed method is discussed in three stages. Firstly, the pre-hiding stage estimates the embedding capacity of each host image. Secondly, the secret COVID-19 data hiding stage uses PSO algorithm and hash function. Thirdly, the transmission stage transfers the stego images based on blockchain technology and updates all nodes (hospitals) in the network. As proof of concept for the case study, the authors adopted the latest COVID-19 research published in the Computer Methods and Programs in Biomedicine journal, which presents a rescue framework within hospitals for the storage and transfusion of the best convalescent plasma to the most critical patients with COVID-19 on the basis of biological requirements. The validation and evaluation of the proposed method are discussed.

Keywords COVID-19 · Medical data · Steganography · Blockchain · Particle swarm optimisation · Integrity · Availability · High capacity · Spatial domain

1 Introduction

The World Health Organisation first reported a novel coronavirus on December 31, 2019 [16]. The coronavirus disease 2019 (COVID-19) pandemic is the largest shock to the world in recent decades and has caused an extraordinary impact on human lives [17, 84]. Different countries have contributed varying technologies that can help medical and healthcare providers stop this pandemic [18, 93]. These contributions describe several of the major threats to individual and collective human health, as well as the values and recommendations that need consideration to counteract such threats in the future [83]. Sustainable health systems and social care need improvements to satisfy the current needs [3, 6, 11–13, 25, 42, 49, 50, 54, 80, 85, 88, 114, 115, 119]. Considerable healthcare data for COVID-19 are generated daily from medical institutions, hospitals and individuals to enhance the understanding of the disease whilst considering environment and lifestyle when conducting disease treatment. Moreover, integration between hospitals is necessary to help doctors in the rapid delivery of COVID-19 treatment [19]. This integration should ensure secure full-field communication channels amongst hospitals. For a clear view of how to support the security of health system in integrating hospitals with considerable healthcare data for COVID-19 communication channels, five sequential questions are raised and answered as follows.

> First question: *What is the main challenge and issues in this study?*

Secure updating and sharing such large amounts of healthcare data in efficient and secure transmission are important but challenging. Potential contributors state that these issues have not been thoroughly investigated [32, 58]. In addition, challenges arise because more private health data of people with COVID-19 are collected and exchanged amongst hospitals and clinical laboratories. In particular, to settle the secure updating and sharing challenges, two issues are faced. Firstly, patients with COVID-19 and hospitals are becoming increasingly concerned about the integrity and confidentiality of their health data [28, 69]. Many state-of-the-art approaches focus on improving data providers' responsibilities to detect data disclosure activities [30]. However, protecting the access to patient data and providing immediate notifications of data disclosure risks are urgently needed. Secondly, hundreds of health systems are in use today, but most of these systems adopt a centralised architecture that suffers from a single point of failure that may cause concerns for data availability. Systems have little or even no communication and cooperation in securing data of patients with COVID-19 [55]. Moreover, health providers are supposed to follow rules or laws (such as the Health Insurance Portability and Accountability Act of 1996 [31]). However, many laws still do not cover different entities that may have access to patient data and therefore should be accountable for their data operations, which also need auditing [43, 46].

> Second question: '*What are the recommended technologies for such challenges and their issues*?'

Two technologies are recommended to address the updating and sharing challenges and their issues [65]. Firstly; steganography technology can be used to improve the confidentiality payload and robustness integrity of stenographic transactions in distributed hospitals. This technique can provide the confidentiality that represents high image quality, high embedding capacity and attack resistance [8, 20–22, 33, 36, 38–40, 47, 51, 56, 57, 62, 63, 71, 73–79, 81, 89, 90, 96, 100–111]. However, no study has yet focused on the integrity of secret data after retrieval from stego images and discovered tampering during data storage in the database. Therefore, essential improvements are needed for data protection regarding the data hiding method [122]. The channels used in conventional steganographic techniques are not secure and often result in privacy leakage on the part of the sender [4, 7, 9, 10, 29, 34, 41, 48, 72, 86, 98]. Therefore, hashes can be used to develop a new steganography method to achieve confidentiality and integrity during the transmissions between the communication channels. Secondly, blockchain technology can be used to maintain a continuous updating and sharing of all transactions across distributed hospital network for data-based decentralise communication, and to improve the level of confidentiality and maintain data availability despite network failure. That is, data availability is ensured regardless whether any single point of the network has a failure connection. Moreover, the central point (third party) in the network is eliminated during the transmission. In conclusion, the combination between the steganography and blockchain technology can ensure the updating and sharing of medical COVID-19 data with high level of security.

> Third question: '*What are the current scenarios for academic literature that attempt to use steganography based blockchain*?'

Literature has limited attempts to use steganography based on blockchain but not on COVID-19 frameworks or other medical data. For instance, a security system to secure digital documents, such as smart contracts, is proposed by relying on steganographic encoder and decoder for hidden messages and use the quick response (QR) code for user document validation [70]. Initially, the user document is inserted and subjected to a validation using the QR code. Subsequently, nodes are formed and finally stored in the blockchain before the normalisation phase. Another study proposed a blockchain-based technique for data hiding to ensure the protection of digital video data privacy [122]. Group encoding and multi-field embedding are also proposed to improve the payload and robustness of the steganography transaction [29]. However, the blockchain comprises hashes as signatures to achieve video integrity and retrieve video information in the destination; the proposed blockchain-based data hiding technique showed no remarkable improvement in data protection. A patient verification framework based on steganography and blockchain technique using finger vein biometrics [66] is also proposed. However, data hiding was only used in the database and not during data transmission. Thus, a steganography-based blockchain technique and covert communication that ensure secure updating and sharing of the communication channel with high confidentiality payload, integrity and availability of data during network failure remains a requirement.

Given the above discussion, two important questions are raised: '*What is the case study adopted as proof of concept that presents the medical COVID-19 data?*' and '*What is the contribution and novelty of the present study?'* A complete solution is needed to overcome the challenges cited above.

As proof of concept that presents the medical COVID-19 data for the case study, we adopted a previous rescue framework [19] within a hospital for the storage and transfusion of the best convalescent plasma (CP) to the most critical patients with COVID-19 on the basis of biological requirements data. Figure 1 shows the framework.

As shown in Fig. 1, the framework presented in [19] is adopted in one hospital. Firstly, ABO compatibility is achieved after classifying donors into the four blood types to indicate the suitability and safety of plasma for administration, and the list of tested CPs is refined using

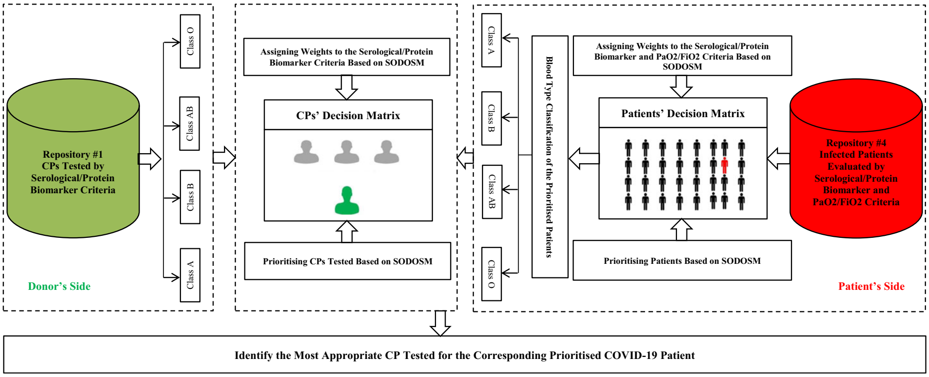

Repository #1
CPs Tested by
Serological/Protein
Biomarker Criteria
Donor's Side
Class O
Class AB
Class B
Class A
Assigning Weights to the Serological/Protein Biomarker Criteria Based on SODOSM
CPs' Decision Matrix
Prioritising CPs Tested Based on SODOSM
Class A
Class B
Class AB
Class O
Blood Type Classification of the Prioritised Patients
Assigning Weights to the Serological/Protein Biomarker and PaO2/FiO2 Criteria Based on SODOSM
Patients' Decision Matrix
Prioritising Patients Based on SODOSM
Repository #4
Infected Patients
Evaluated by
Serological/Protein
Biomarker and
PaO2/FiO2 Criteria
Patient's Side
Identify the Most Appropriate CP Tested for the Corresponding Prioritised COVID-19 Patient

Fig. 1 Intelligence-integrated concept to identify the most appropriate CP for a corresponding prioritised patient with COVID-19 [19]

machine learning techniques. Secondly, patient prioritisation is carried out using a constructed patient decision matrix via a novel multi-criteria decision-making (MCDM) method called subjective and objective decision by opinion score method (SODOSM). MCDM is an extension of the decision theory that covers any multi-objective decision and solves numerous problems either for healthcare or other domains. A decision matrix is constructed on the basis of an intersection between the evaluation criteria used and rank/prioritise a set of alternatives based on the evaluation criteria [1, 2, 5, 14, 15, 23, 24, 26, 37, 45, 52, 59–61, 87, 120, 121, 123]. Then, patients with emergency cases are classified based on their blood type to be matched with the list of tested donor CPs, which are prioritised using the constructed CP decision matrix (refer to [19] for more details). At present, each hospital should adopt this framework and the process needs generalisation across all hospitals in one platform to help doctors accelerate treatments. Thus, sharing and updating patient and donor data [44, 64, 68] in secure communication channels of hospital networks are now necessary. The reason behind using this framework is its possible adoption amongst distributed hospitals in decentralised telemedicine based on recommended blockchain technology [19].

From the above points, the use of steganography-based blockchain can provide a complete solution for secure updating and sharing challenges with the integrity, availability, and confidentiality of patient and donor data when transactions between hospital nodes contain the information in stego images. This system can provide a secure communication channel for stegano-message delivery [82, 92] in two ways. (i) Channel security is ensured by using a distributed storage schema and an immutable chain of blocks. Thus, manipulating the communication history is virtually impossible. (ii) The blockchain network is a peer-to-peer network that does not require a third-party provider for message delivery to establish communication; hence, the network is not prone to any form of availability attack.

The main contribution of this study is a novel steganography-based blockchain method in the spatial domain. The novelty of the proposed method involves the removal and addition of new particles of the particle swarm optimisation (PSO) algorithm and hash function to hide secret medical COVID-19 data in hospital databases whilst providing confidentiality with high embedding capacity and high image quality. Moreover, stego images with hash data and blockchain technology are used in updating and sharing medical COVID-19 data between hospitals in the network, to improve the level of confidentiality and protect the integrity of medical COVID-19 data in grey-scale images, ensure data availability regardless whether any single point of the network has failure connection and eliminate the central point (third party) in the network during the transmission. The proposed method is discussed in three stages. Firstly, the pre-hiding stage estimates the embedding capacity of each host image. Secondly, the secret COVID-19 data hiding stage uses PSO algorithm and hash function. Thirdly, the secret medical COVID-19 data transmission transfers the stego images based on blockchain technology and updates all nodes (hospitals) in the network, as shown in Fig. 2. This proposed method also partitions data for a multicast delivery on better efficiency.

This paper is organised as follows. The proposed steganography method is presented in Section 2. The validation and evaluation tools used are illustrated in Section 3. The claims and limitation of this study are listed in Section 4. Finally, the conclusions and suggestions for future study are presented in Section 5.

2 Proposed steganography method based on blockchain and PSO algorithm

A new steganography method for concealing secret messages inside a host image based on PSO algorithm is previously proposed [65]. This algorithm is used to find the best bit locations for hiding secret data in host images [67]. The benefit of this method is to reduce the distortion of stego images. The best location refers to places where the secret data can be embedded with the least chances of distortion. This method determines the starting pixel, number of least significant bits (LSBs) used per pixel and the scanning image's pixel sequence for message bit embedment. The present study develops and proposes a new steganography method in the spatial domain by removing and adding new particles of the PSO algorithm and using blockchain technology to hide medical data of patients with COVID-19. Moreover, the

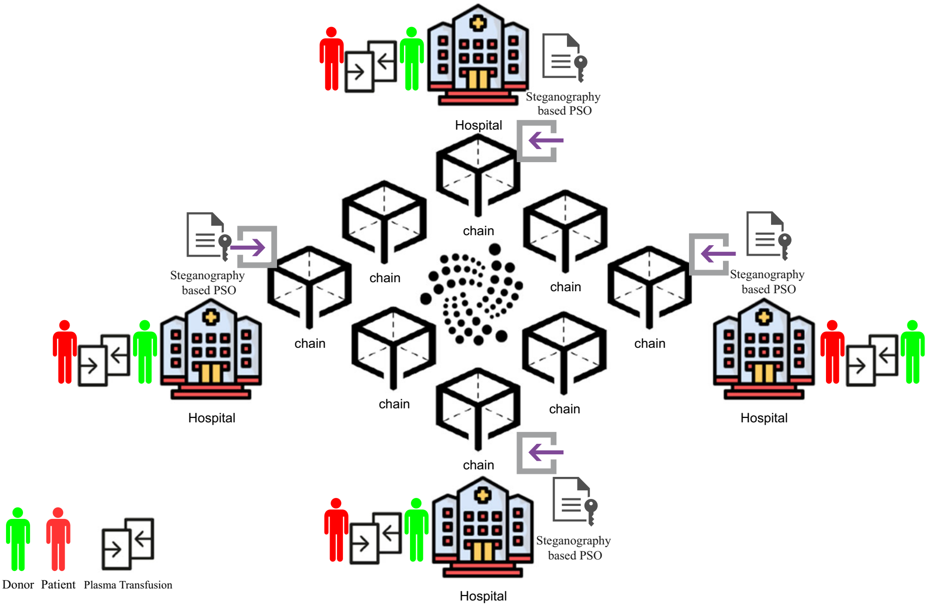


Fig. 2 Decentralised hospital architecture for the storage and exchange of the information of patients with COVID-19

proposed steganography method is classified into three stages: pre-hiding, secret data hiding, and secret COVID-19 medical data transmission. Generally, information-hiding schemes are evaluated based on the transparency, reliability and capacity of the hidden information, mainly its robustness to tampering and signal processing distortions and the computational speed of the scheme in secret data embedment and extraction [35, 53, 95, 97, 99, 112, 113, 116, 117]. However, the relevance of each of these measures depends on their intended application. Therefore, this study aims to achieve the aforementioned goals for secure updating and sharing as much as possible in addition to the information security requirements (confidentiality, integrity and availability) for the medical data of patients with COVID-19. The secret data hiding in each node (hospital) and medical data transmission to another node (hospital) in a decentralised architecture are explained in the following general procedure. Figure 3 shows the sequential steps of the new steganography method based on blockchain and PSO algorithm.

As shown in Fig. 3, the sequential steps start with the input of large-scale secret data and grey-scale host images. In the pre-hiding stage, Algorithm 1 (see Section 2.1) is proposed to estimate the embedding capacity of each host image. In the secret hiding stage, Algorithm 2 (see Section 2.2) is proposed to hide the secret medical data using PSO algorithm and hash function. The output of stages 1, 2 and 3 is a stego image that contains one part of the secret data with less distortion and high level of confidentiality. Moreover, stego images with hash data provide a level of benefits in terms of integrity when the stego images are transmitted to other nodes (hospitals) in the network. In the final stage, blockchain technology is used to update and share the medical data by transfer the stego images to all nodes (hospitals) in the network, to improve the level of confidentiality and protect the integrity medical COVID-19 data in grey-scale images, achieve data availability if any of a single point of network is failure connection and eliminate the central point (third party) in the network during the transmission process.

2.1 Pre-hiding stage

This stage will be discussed before starting the steganography process to:

1. Allow each node (server in decentralised hospital architecture) to estimate the host images (estimate the capacity of host images for hiding secret COVID-19 data) to reduce the time of hiding secret COVID-19 data;
2. Reduce the time consumed by the PSO algorithm in selecting the best bit locations in the host images for hiding secret COVID-19 data;

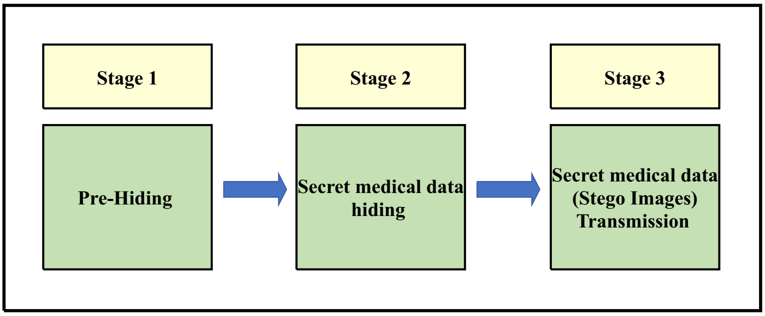

Stage 1
Stage 2
Stage 3
Pre-Hiding
Secret medical data hiding
Secret medical data (Stego Images) Transmission

Fig. 3 Sequential order of the new steganography method based on blockchain and PSO algorithm for COVID-19 data

3. Enhance the quality of stego images (reduce the distortion) by embedding the secret COVID-19 data according to the host images' capacity (no more, no less);
4. Label all host images in each node according to their capacity for hiding secret COVID-19 data.

Most of the recent technologies can utilise various forms of carrier messages, such as image, text and video. However, image file remains the most common form of carrier message because it can be easily sent during active communication between two parties. Images can exist in three different forms: binary (black and white), grey scale and red–green–blue (RGB) images. The study [65] that served as the benchmark of the current study used grey-scale images; therefore, the current study will adopt grey-scale images. The procedures defined in Algorithm 1 will be performed to estimate the host images' embedding capacity (Fig. 4).

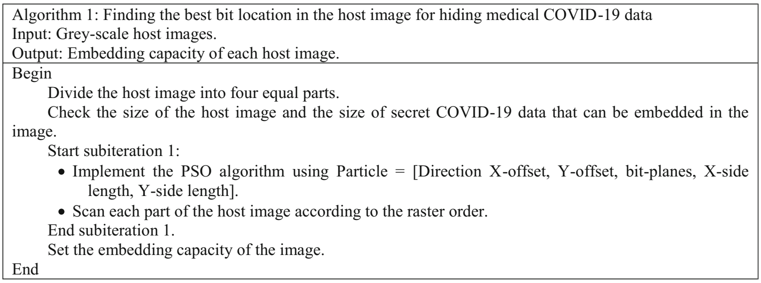
2.1.1 Finding the best bit location in the host image for hiding

The best bit location is the location where message bits could be embedded with the least chance of distortion. The start pixel, the number of LSB used in each pixel and the pixel sequence of the scanning image are determined using this method to conceal the message bits. The raster order of pixels in the LSB substitution method refers to the pixels' order in the cover image. These pixels are scanned from left to right and from the first row to the last row of the cover image. Assume an image with a 5 × 5 dimension, the raster order of the pixels will be as depicted in Fig. 5.

The major aim of this concept is to transform the steganography problem into a search and optimisation problem [27, 91, 118]. The order presented in Fig. 6a and b perhaps depicts a better order compared with the raster order. As a result, various positions and orders in the carrier image could serve as the ideal position for secret COVID-19 data embedment as they produce various peak signal-to-noise ratios (PSNRs). Hence, the problem of pixel scanning direction has 16 possible solutions. If a new method is designed to check all the possible orders and identify the best order for a given carrier image, then basic LSB steganography may be used to improve the result.

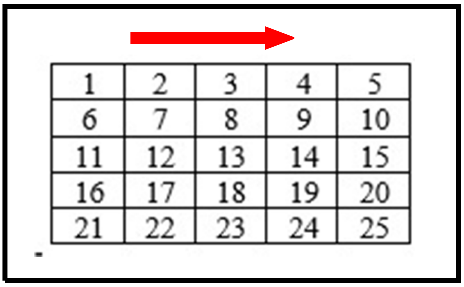
The host image is divided into four equal parts [11]; therefore, row-wise image pixel scanning is done from top to bottom or reverse, whereas column-wise scanning is done from right to left or reverse. The PSO particles for each part in the proposed method are as follows:

$$\text{Particle} = [\text{Direction X-offset, Y-offset, bit-planes, X-side length, Y-side length}].$$



```
Algorithm 1: Finding the best bit location in the host image for hiding medical COVID-19 data
Input: Grey-scale host images.
Output: Embedding capacity of each host image.
Begin
    Divide the host image into four equal parts.
    Check the size of the host image and the size of secret COVID-19 data that can be embedded in the image.
    Start subiteration 1:
        • Implement the PSO algorithm using Particle = [Direction X-offset, Y-offset, bit-planes, X-side length, Y-side length].
        • Scan each part of the host image according to the raster order.
    End subiteration 1.
    Set the embedding capacity of the image.
End
```

Fig. 4 Algorithm 1: Finding the best bit location in the host image for hiding medical COVID-19 data



1	2	3	4	5
6	7	8	9	10
11	12	13	14	15
16	17	18	19	20
21	22	23	24	25

Fig. 5 Raster order

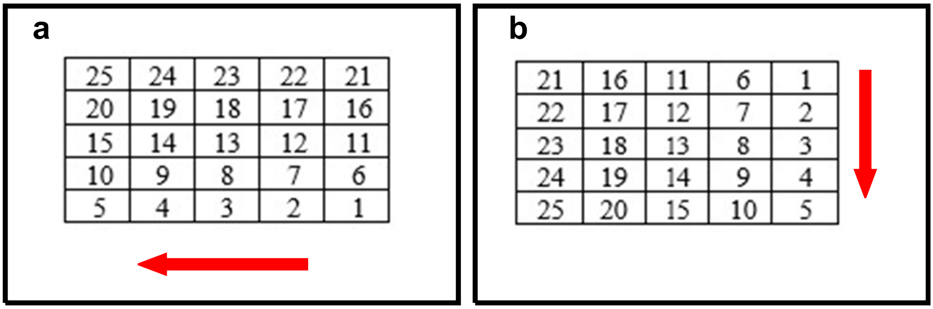
The particles' definitions are shown in Table 1, and all possible cases of host image scanning are shown in Table 2.

where the X-offset length ≤ the number of host columns and the Y-offset length < the number of host rows, because the last row is used for hiding all the particle bits as proposed in this study. Particle bits are embedded in the last row of the cover image for subsequent extraction during steganalysis. The pixels of the cover image can be scanned in 16 possible directions, but the particle representation in the proposed method has a length of 4 bits. The beginning of the scanning point can be represented as two particles (X-offset and Y-offset) with a length of 8 bits each. The LSB planes in the pixels of the cover image (bit-planes) are defined by showing all the possible bit-plane values as shown in Table 3.

Consequently, the proposed approach will classify the particles into three sets. The first set of particles includes those that point out secret bit insertion in the host image and is used to estimate the capacity of host images. The second set of particles is those used to effect changes in medical secret COVID-19 data to improve its adaptability with the host image. The third set of particles is used for the transmission of secret medical COVID-19 data (stego images) based on blockchain technology. The second and third sets of particles are used in secret COVID-19 data hiding and sego image transmission stages, respectively. The output of this first stage will be the host image's embedding capacity as shown in Fig. 7.

2.2 Secret medical data hiding stage

In this stage, the secret medical COVID-19 data is embedded in host images based on the finding from the pre-hiding stage, which determines the embedding capacity of each host image. All the procedures of this stage are defined in Algorithm 2 shown in Fig. 8. The time



25	24	23	22	21
20	19	18	17	16
15	14	13	12	11
10	9	8	7	6
5	4	3	2	1

21	16	11	6	1
22	17	12	7	2
23	18	13	8	3
24	19	14	9	4
25	20	15	10	5

Fig. 6 Two orders of pixel scanning. **a** Pixel scanning order 1. **b** Pixel scanning order 2

Table 1 Particle definitions

Particle name	Value range	Length	Description
Direction	0 to 15	4 Bits	Direction of the host image pixel scanning.
X-offset	0 to 225	8 Bits	X-offset of the starting point.
Y-offset	0 to 225	8 Bits	Y-offset of the starting point.
Bit-planes	0 to 15	4 Bits	Used LSBs for secret bit insertion.
X-side length	0 to 225	8 Bits	Dimension of the window in the X-axis.
Y-side length	0 to 225	8 Bits	Dimension of the window in the Y-axis.

consumption of the hiding process will be calculated only in this stage because the first stage will be performed before the COVID-19 data hiding process.

This stage can be divided into two steps:

2.2.1 Calculating the size of secret medical data (block of secret COVID-19 data)

In this step, the secret COVID-19 data is reduced to blocks according to the host images' size, which is the output of the previous stage (pre-hiding), and then the blocks of secret COVID-19 data are converted into binary data to prepare for embedding into the host image as explained in the next step. The advantages of this step are as follows:

- The secret COVID-19 data is hidden according to the embedding capacity of each host image.
- The secret COVID-19 data embeded in specific host images will be incomplete (distributed in many host images); therefore, the security level of steganography is enhanced compared with other steganography methods that embed secret COVID-19 data completely in one image. This complete embedment will increase the vulnerability of the image to attack. Moreover, the quality of the stego image will be high because the embedding will be done according to the capacity of host images. The output of this step is shown in Fig. 9.

Table 2 All possible cases of host image scanning

Direction	Row	Column	Type	Argument
0	Top to bottom	Left to right	Triangle	Columns then rows
1	Top to bottom	Right to left	Triangle	Columns then rows
2	Bottom to top	Left to right	Triangle	Columns then rows
3	Bottom to top	Right to left	Triangle	Columns then rows
4	Top to bottom	Left to right	Square	Columns then rows
5	Top to bottom	Right to left	Square	Columns then rows
6	Bottom to top	Left to right	Square	Columns then rows
7	Bottom to top	Right to left	Square	Columns then rows
8	Top to bottom	Left to right	Triangle	Rows then columns
9	Top to bottom	Right to left	Triangle	Rows then columns
10	Bottom to top	Left to right	Triangle	Rows then columns
11	Bottom to top	Right to left	Triangle	Rows then columns
12	Top to bottom	Left to right	Square	Rows then columns
13	Top to bottom	Right to left	Square	Rows then columns
14	Bottom to top	Left to right	Square	Rows then columns
15	Bottom to top	Right to left	Square	Rows then columns

Table 3 Possible values of bit-plane particles

Value	Description	Value	Description
0000	Use none of the LSB	1000	Use the fourth LSB
0001	Use the first LSB	1001	Use the first and fourth LSBs
0010	Use the second LSB	1010	Use the second and fourth LSBs
0011	Use the first and second LSBs	1011	Use the first, second and fourth LSBs
0100	Use the third LSB	1100	Use the third and fourth LSBs
0101	Use the first and third LSBs	1101	Use the first, third and fourth LSBs
0110	Use the second and third LSBs	1110	Use the second, third and fourth LSBs.
0111	Use the first, second and third LSBs	1111	Use the four LSBs

2.2.2 Hiding the block of secret medical COVID-19 data in host images

In this step, the blocks of secret COVID-19 data are hidden in the host images as mentioned in Algorithm 2. The particles of the PSO algorithm used in this stage are defined in Table 4. Direction X-offset, Y-offset, bit-planes, X-side length, Y-side length, data block number, host image number, Genesis image number, HC-SD. HN-SD, HL-SD.

The secret bit pole (SB-Pole) was determined by using the direction of secret bits (SB-Dire) to define the message bits' direction, whereas the last particle is determined by the bit plane's direction (BP-Dire) to show the direction of the LSB planes. The last three particles are illustrated in Table 5.

This stage hides the secret medical COVID-19 data in host images using the particles defined in this stage (Fig. 10).

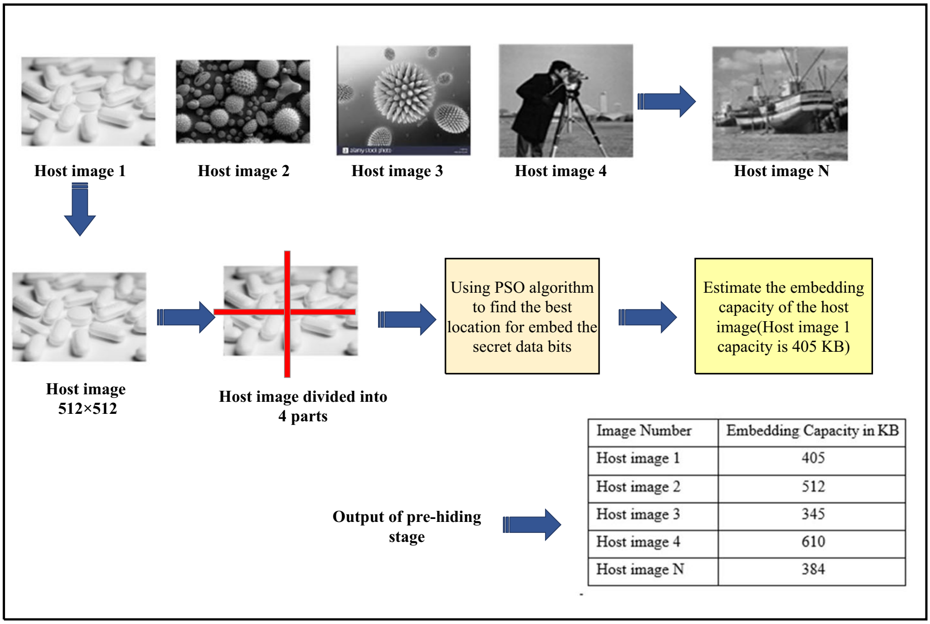

Host image 1
Host image 2
Host image 3
Host image 4
Host image N
Host image 512×512
Host image divided into 4 parts
Using PSO algorithm to find the best location for embed the secret data bits
Estimate the embedding capacity of the host image(Host image 1 capacity is 405 KB)
Output of pre-hiding stage

Image Number	Embedding Capacity in KB
Host image 1	405
Host image 2	512
Host image 3	345
Host image 4	610
Host image N	384

Fig. 7 Processing stages

```
Algorithm 2: Least Signified Bit (LBS) data hiding based on PSO algorithm and hash function
Input: Grey-scale host images, secret COVID-19 data.
Output: Stego images, hash for each block of secret COVID-19 data.
Begin
    Convert secret data into binary.
    Cut secret data into blocks according to the host images' size.
    Start subiteration 1:
      • Calculate the hashing for the block of secret COVID-19 data as the hash of the current secret data.
      • Set the hash of each next block of secret COVID-19 data.
      • Set the hash of the last block of secret COVID-19 data as N.
      • Set the number of blocks of secret COVID-19 data.
      • Set the number for each host image used for embedding this block of secret COVID-19 data.
      • Set the number of the first host image used for meddling this block of secret COVID-19 data as the
          Genesis image.
      • Implement the PSO algorithm using Particle = [Direction X-offset, Y-offset, bit-planes, X-side
          length, Y-side length, data block number, host image number, Genesis image number, HC-SD,
          HN-SD, HL-SD].
      • Scan each part of the host image based on the output of Algorithm 1 to hide the block of secret
          COVID-19 data.s
      • Hide the COVID-19 data of all particles in the last row of the host image.
    End subiteration 1.
    Save all the hashes (Genesis, 2, 3, …, N) in the ledger.
End
```

Fig. 8 Algorithm 2: LBS data COVID-19 hiding based on PSO algorithm and hash function

The output of this stage is shown in Fig. 11. All the stego images are stored in the node (hospital database) as chains of stego images. The hash for each secret medical COVID-19 data block is calculated and set as the particles as shown in Table 4 before embedding into the stego image to be used as the reference to point out the previous and next stego images during data retrieval.

As shown in Fig. 11, this stage has two directions. The black arrow refers to the hiding direction, in which each block of secret medical COVID-19 data is embedded in one host image (according to the embedding capacity of the host image). In this case, the secret COVID-19 data is randomly distributed in many stego images to

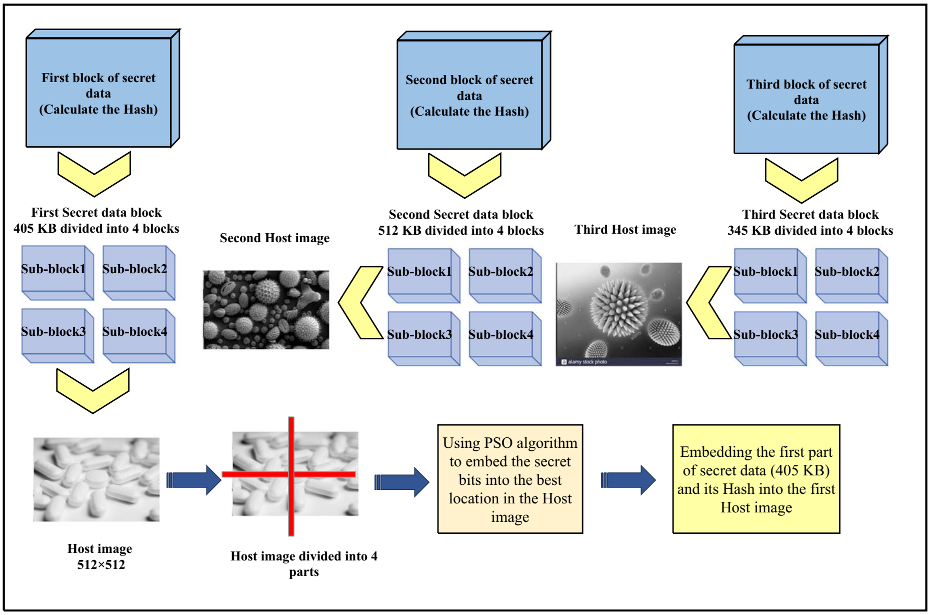

First block of secret data (Calculate the Hash)
Second block of secret data (Calculate the Hash)
Third block of secret data (Calculate the Hash)
First Secret data block 405 KB divided into 4 blocks
Second Host image
Second Secret data block 512 KB divided into 4 blocks
Third Host image
Third Secret data block 345 KB divided into 4 blocks
Sub-block1
Sub-block2
Sub-block3
Sub-block4
Sub-block1
Sub-block2
Sub-block3
Sub-block4
Sub-block1
Sub-block2
Sub-block3
Sub-block4
Host image 512×512
Host image divided into 4 parts
Using PSO algorithm to embed the secret bits into the best location in the Host image
Embedding the first part of secret data (405 KB) and its Hash into the first Host image

Fig. 9 Dividing the secret COVID-19 data into blocks according to the host images' embedding capacity

Table 4 Particle definitions

Particle name	Value range	Length	Description
SB-Pole	0 to 1	1 Bit	Pole of secret bits.
SB-Dire	0 to 1	1 Bit	Direction of secret bits.
BP-Dire	0 to 1	1 Bit	Direction of bit planes.
Data block number	0 to 225	8 Bits	Number of secret COVID-19 data blocks embedded in one host image.
Host image number	0 to 225	8 Bits	Number of host image used for embedding one block of secret COVID-19 data.
Genesis image number	0 to 225	8 Bits	Number of host image used for embedding the first block of secret COVID-19 data.
HC-SD	Any value	256	Hash of current block of secret COVID-19 data
HN-SD	Any value	256	Hash of next block of secret COVID-19 data
HL-SD	Any value	256	Hash of last block of secret COVID-19 data

complicate hiding and increase security against any attempt to steganalysis by any attacker (extracting the secret medical COVID-19 data from one stego image will be not useful, because the extracted secret COVID-19 data is incomplete). Each node (hospital) has its own record called ledger, which stores all the hashes for the blocks of the secret COVID-19 data (Fig. 12). This ledger is used during the retrieval of secret COVID-19 data from stego images (to extract the complete secret medical COVID-19 data) and the transmission of stego images to all nodes in the network, which is explained in the next section.

2.3 Secret medical COVID-19 data (stego images) transmission stage

Covert communication refers to a secret and secure form of communication that can only be detected by the participants. Such communication is performed in a manner that keeps outsiders from sniffing or realising the existence of conversations. However, conventional steganography approaches normally rely on nonsecure channels, which are associated with privacy leakage on the part of the sender, because of their reliance on a third-party provider for the delivery of the stegano-message. This third-party provider can easily interfere with the communication process, especially when the information or message is wrongly classified or filtered. Another problem of the conventional steganography technique is that it exposes the identity of the sender (such as IP or email addresses) to the public, and such information could be used by an outsider to further analyse the communication pattern or interrupt the propagation of the stegano-message. Although the secrecy of the content may still be retained because of encryption, the

Table 5 Possible values for SB-Pole, SB-Dire and BP-Dire particles

Particle name	Value	Description
SB-Pole	0	In this case, the secret bits are unchanged.
	1	In this case, the secret bits are changed to be opposite.
SB-Dire	0	In this case, no change is made to the secret bits.
	1	In this case, the secret bits are reversed from end to beginning.
BP-Dire	0	In this case, bit-planes are used from most significant bit (MSB) to LSB.
	1	In this case, bit-planes are used from LSB to MSB.

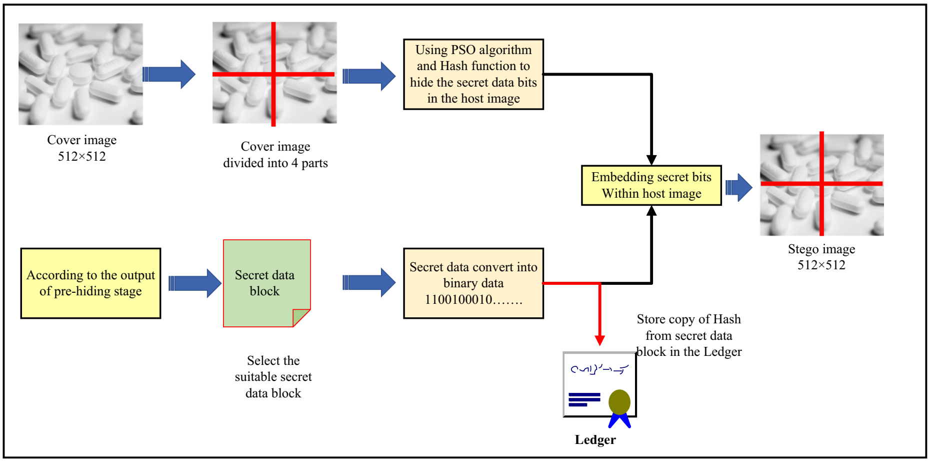

Cover image
512×512
Cover image
divided into 4 parts
Using PSO algorithm and Hash function to hide the secret data bits in the host image
Embedding secret bits Within host image
Stego image
512×512
According to the output of pre-hiding stage
Secret data block
Secret data convert into binary data 1100100010…….
Select the suitable secret data block
Store copy of Hash from secret data block in the Ledger
Ledger

Fig. 10 Hiding secret medical COVID-19 data in host image

identity of the sender and the communication time can easily be recognised [29]. Therefore, blockchain technology was used in the proposed steganography method to enhance the security level during the stego image transmission stage, as well as during the COVID-19 data hiding process. Hashing was used to hide the secret COVID-19

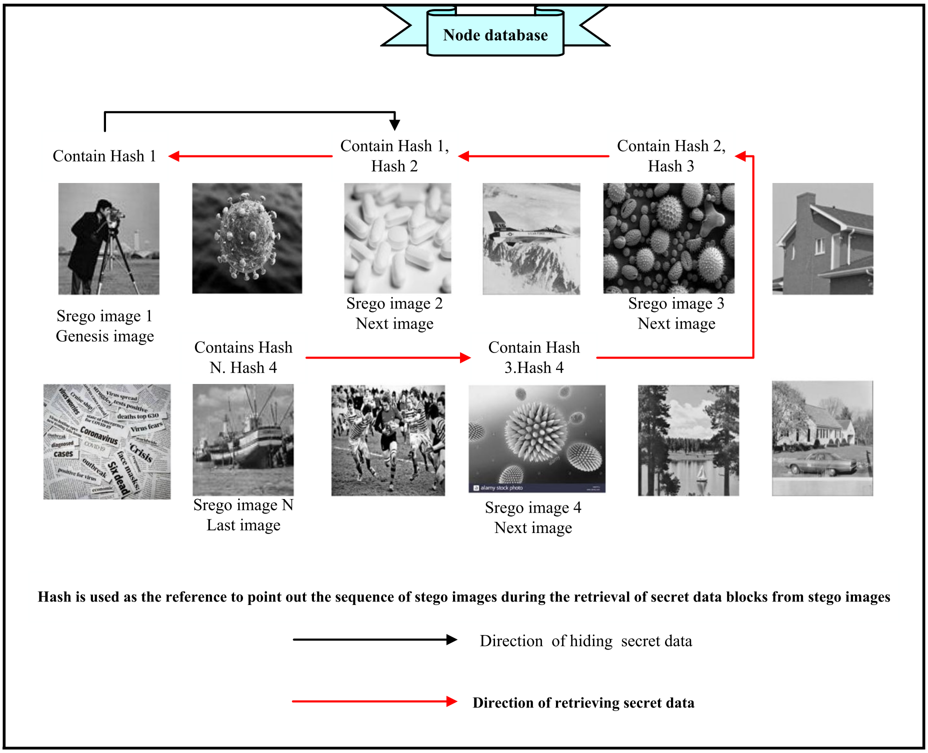


Fig. 11 Storage and retrieval of stego images in the node database

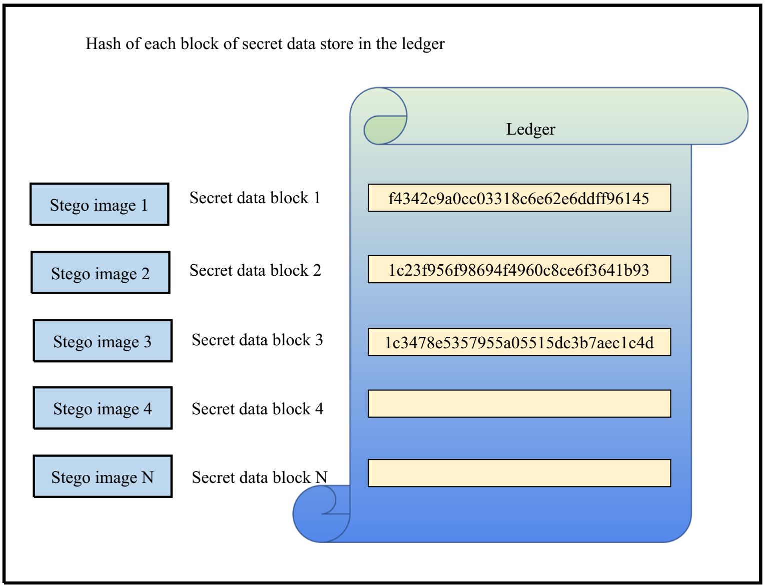


Fig. 12 Ledger for each node (hospital) in the network

data as explained in the previous section, and blockchain was used in stego image transmission in the decentralised architecture as explained in the following procedures:

1. The decentralised architecture based on blockchain technology has no central point (third party) that verifies the transaction between any nodes (hospitals) in the network as the connection will be by pair.
2. Based on blockchain technology, all nodes (hospitals) in the network will receive the COVID-19 data immediately without the need to verify the transaction from any third party when any node transfers any secret COVID-19 data to any node in the network. The validity of the transaction needs to be verified by at least 50% of the nodes in the network; this procedure will make tampering the transaction hard for any attacker.
3. The transmission will proceed as a chain of COVID-19 data blocks that contain the secret medical COVID-19 data when any node (hospital) sends the medical secret COVID-19 data (stego image) to all nodes (hospitals) in the network based on blockchain technology. Each block contains the payload (stego image of COVID-19 data), the hash of this image (current stego image) and the hash of the previous stego image except the first block called the Genesis block, which contains only the payload (stego image of COVID-19 data) and the hash of the first stego image.
4. The hash of the Genesis block will be stored in the ledger of the nodes (each node in the network) that received the block of COVID-19 data.
5. The node will check the value of the hash of the Genesis block, which has been stored in the ledger with the hash of the Genesis block coming with this block, when the second block of COVID-19 data reaches the node (each node in the network), which contains the hash of the second block, the previous block (Genesis block) and payload.

6. If the hashes are similar, then the COVID-19 data content is not tampered.
7. The same process will be implemented with each block of COVID-19 data to check the integrity of the stego images.
8. After finishing all the transactions, the ledger in each node will contain all the hashes of the stego image to ensure the integrity of the transmitted COVID-19 data and will use this hash during the retrieval of the secret COVID-19 data from the stego images.

The benefits of using blockchain technology in stego image transmission are to:

1. Enhance the level of security when hiding secret COVID-19 data during steganography by distributing the secret COVID-19 data in multi-host images and using hashes as pointers during the retrieval of the secret COVID-19 data (see secret COVID-19 data hiding stage);
2. Ensure the integrity of COVID-19 data during the transmission and retrieval of secret COVID-19 data from stego images;
3. Ensure the availability of the secret COVID-19 data in all the nodes in the network.

The diagram of the peer-to-peer transmission in a decentralised architecture is illustrated in Fig. 13, which depicts the transmission of the stego images with COVID-19 data from one node to all nodes in the network.

The transmission in decentralised hospital architecture is illustrated in Fig. 14, which shows that all nodes (hospitals) are connected with each other as peers without a central point. The data is received and updated in real time. The network will not be affected in case of network failure and node failure as other nodes will still provide the services.

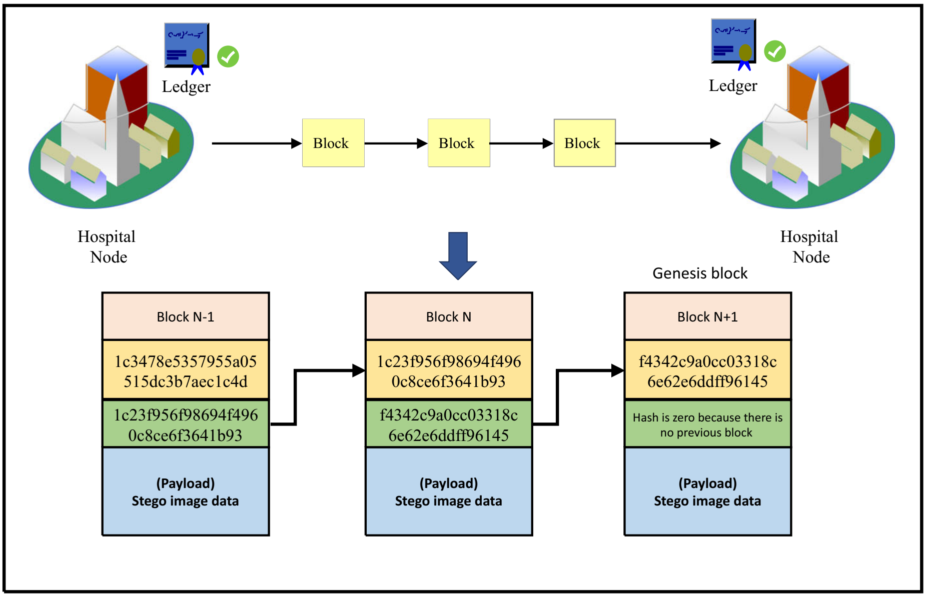

Ledger
Ledger
Block
Block
Block
Hospital Node
Hospital Node
Genesis block
Block N-1
1c3478e5357955a05 515dc3b7aec1c4d
1c23f956f98694f496 0c8ce6f3641b93
(Payload) Stego image data
Block N
1c23f956f98694f496 0c8ce6f3641b93
f4342c9a0cc03318c 6e62e6ddff96145
(Payload) Stego image data
Block N+1
f4342c9a0cc03318c 6e62e6ddff96145
Hash is zero because there is no previous block
(Payload) Stego image data

Fig. 13 Peer-to-peer transmission based on blockchain technology

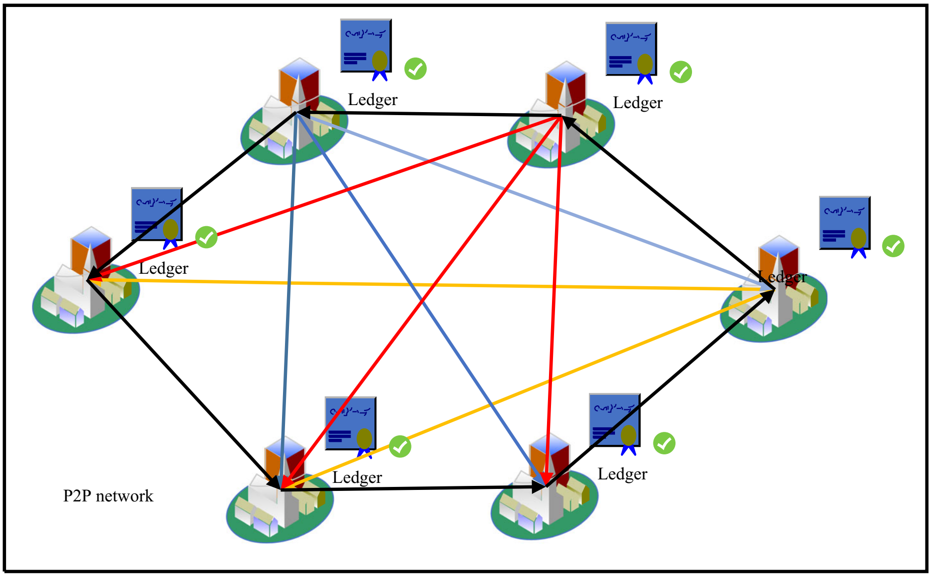


Fig. 14 Peer-to-peer architecture of COVID-19 data transmission based on blockchain technology

2.4 Secret COVID-19 data retrieval

The embedded secret COVID-19 data can be extracted by the reverse process as shown in Fig. 15. The information is extracted from the last row of the stego image. The procedure of retrieving the secret COVID-19 data can be summarise as follows:

1. Extract the information from the last row in the last stego image (the last stego image contains the last part of the secret COVID-19 data).
2. Check the hash of the last stego image extracted in 1 with the last stego image in the ledger. If the result matches, then no tampering happened in the stego image content during its storage in the database.
3. Implement stenography method based on PSO algorithm in reverse to obtain the secret COVID-19 data from the stego image.
4. Check the hash of the next stego image (N−1) extracted in 1 to know the next stego image that contains the second block of secret COVID-19 data (see secret COVID-19 data hiding stage).
5. Repeat 2, 3 and 4 until the next stego image has no Hash.
6. Aggregate all the parts of the secret COVID-19 data blocks to obtain the final secret COVID-19 data.

3 Validation and evaluation of the proposed method

The findings of the proposed method in this study should be validated to check whether the proposed method is appropriate for the purpose of securing the hiding and transmission of secret COVID-19 data, as well as overcoming the identified limitations and producing the

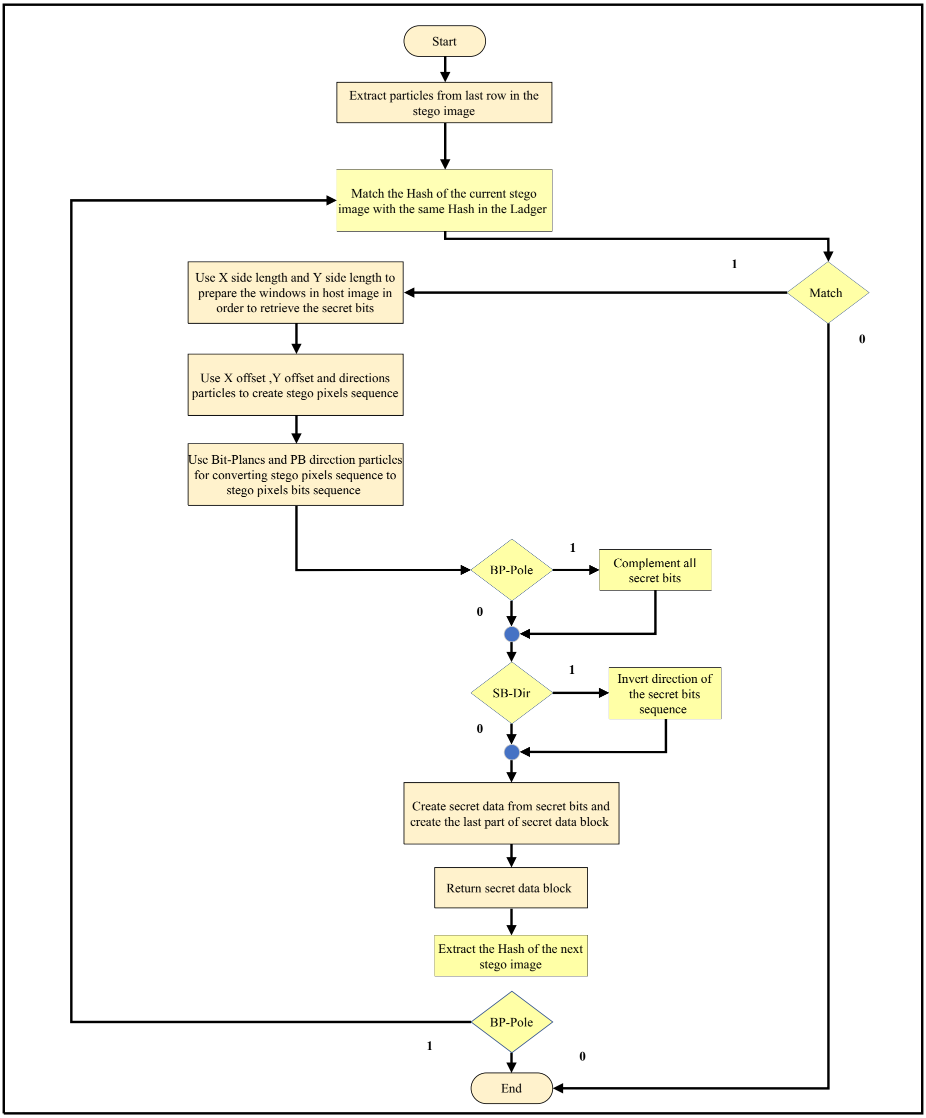

Start
Extract particles from last row in the stego image
Match the Hash of the current stego image with the same Hash in the Ladger
Match
1
0
Use X side length and Y side length to prepare the windows in host image in order to retrieve the secret bits
Use X offset ,Y offset and directions particles to create stego pixels sequence
Use Bit-Planes and PB direction particles for converting stego pixels sequence to stego pixels bits sequence
BP-Pole
1
Complement all secret bits
0
SB-Dir
1
Invert direction of the secret bits sequence
0
Create secret data from secret bits and create the last part of secret data block
Return secret data block
Extract the Hash of the next stego image
BP-Pole
1
0
End

Fig. 15 Flowchart of the secret image extraction process

expected performance. Moreover, the validation process will determine whether the proposed method has achieved all the requirements in relation to the goals of this study.

The validation stage for the proposed steganography method can be achieved by discussing security analysis using two types of attack; most biometric systems are prone to two types of attack, namely, spoofing and brute-force attacks [94]. For spoofing, we consider that an attacker spoofs the user via phishing or a similar method to access the node and then analyse the resistance of the proposed steganography method against this type of attack. For brute-force attacks, we assume that an attacker is attempting to guess the hash via brute-force attack.

The stego image (hidden secret COVID-19 data inside a host image) is evaluated through existing methods using PSNR value, mean square error (MSE) and histogram following the same evaluation method of the benchmark methods to prove its effectiveness over the other steganography methods referred in literature.

1. The PSNR value between the cover and stego images is calculated using the following equation

$$PSNR = 10 \times log_{10} \frac{(255)^2}{\mathrm{MSE}} \tag{1}$$

where MSE is the mean square error between the cover and stego images.

2. The MSE value is calculated using Eq. 2

$$MSE = \frac{1}{W \times H} \sum_{i=1}^{w} \sum_{j=1}^{H} \left(x_{ij} - y_{ij} \right)^2 \tag{2}$$

where x_{ij} *and* y_{ij} are the value of each pixel in the host image and stego image, respectively.

4 Claims and limitation of study

The general claims of this study is proposed and a novel steganography-based block chain method in spatial domain for secure updating and sharing the data of donors and patients with COVID-19 during the transmission channels is discussed. The main claims of this study are briefly stated as follows:

1. The use of hashes when hiding secret COVID-19 data can secure the integrity of the data after retrieval from stego images. This steganography method is state-of-the-art given that no other has focused on the integrity of secret COVID-19 information within distributed hospitals after retrieval.
2. According to literature, all the previous steganography methods hide secret data in one host image (complete secret data); the proposed method divides secret COVID-19 data into several parts and hides them in multi-host images, then uses the hash as a pointer between stego images amongst hospitals. This manner of hiding makes the proposed method very difficult to break by any attacker. Moreover, the expected stego image has a high level of quality because the host image's embedding capacity is estimated before hiding the secret data (not more or less than the embedding capacity). This step provides a high level of confidentiality.
3. According to literature, stego image transmission is challenging; therefore, blockchain is used for stego image transmission in distributed hospitals to increase the security of transmission of COVID-19 data and to eliminate the third party. Moreover, the secret data has a high level of confidentiality.
4. The proposed method has the ability to avoid network failure during disasters on the basis of used the blockchain technology. This ability ensures data availability regardless

whether any single point of network has failure connection. This feature is important in terms of providing medical care services during the COVID-19 pandemic.

The limitation of this study is that the proposed method in this study has not been tested on real data of infected cases due to the lockdown and global pandemic. Collecting real datasets of patients with COVID-19 and recovered donors is difficult during these times.

5 Conclusion and future work

This study presents a novel method of secret medical data hiding, which can be adopted as a new framework and covert communication between hospitals with decentralised architecture when transmitting healthcare information of patients with COVID-19. This method can classify plasma donors and determine priority patients (SODOSM) according to the highest emergency and plasma data to be matched with the data of tested donor CPs based on the decision matrix. In terms of secure updating and sharing, the proposed steganography method based on PSO algorithm and hash function can hide secret medical COVID-19 data in hospital databases whilst providing confidentiality with high embedding capacity and high image quality. Moreover, stego images with hash data and blockchain technology are used in updating and sharing medical COVID-19 data between hospitals in the network, to improve the level of confidentiality and ensure the protection of the integrity medical COVID-19 data in grey-scale images, ensure data availability regardless whether any single point of the network has a failure connection and eliminate the central point (third party) in the network during the transmission. Overall, blockchain technology can be used to develop future electronic voting systems, which can be deployed to fulfil the principles of democratic elections. However, the privacy of public blockchains remains a critical issue because of long-term privacy concerns. The proposed method to secure the recently published framework within a hospital for the storage and transfusion of the best CP to the most critical patients with COVID-19 on the basis of biological requirements can be simulated and implemented in the future to serve as a guide for providing healthcare services with secret COVID-19 data during the abovementioned challenges and issues.

References

1. Abdulkareem KH et al (2020) A novel multi-perspective benchmarking framework for selecting image Dehazing intelligent algorithms based on BWM and group VIKOR techniques. Int J Inf Technol Decis Mak 19(3):909–957
2. Abdulkareem KH, Arbaiy N, Zaidan AA et al (2020) A new standardisation and selection framework for real-time image dehazing algorithms from multi-foggy scenes based on fuzzy Delphi and hybrid multi-criteria decision analysis methods. Neural Comput & Applic. https://doi.org/10.1007/s00521-020-05020-4
3. Abdulnabi M, Al-Haiqi A, Kiah MLM, Zaidan AA, Zaidan BB, Hussain M (2017) A distributed framework for health information exchange using smartphone technologies. J Biomed Inform 69:230–250
4. Ahmed MA et al (2010) A novel embedding method to increase capacity and robustness of low-bit encoding audio steganography technique using noise gate software logic algorithm. J Appl Sci 10(1):59–64
5. Alaa M, Albakri ISMA, Singh CKS, Hammed H, Zaidan AA, Zaidan BB, Albahri OS, Alsalem MA, Salih MM, Almahdi EM, Baqer MJ, Jalood NS, Nidhal S, Shareef AH, Jasim AN (2019) Assessment and ranking framework for the English skills of pre-service teachers based on fuzzy Delphi and TOPSIS methods. IEEE Access 7:126201–126223

6. Albahri AS, Alwan JK, Taha ZK, Ismail SF, Hamid RA, Zaidan AA, … Alsalem MA (2020) IoT-based telemedicine for disease prevention and health promotion: State-of-the-Art. J Netw Comput Appl 173:102873
7. Alanazi HO (2010) Using the features of mosaic image and AES cryptosystem to implement an extremely high rate and high secure data hidden : analytical study. Sci Res Essays 5(21):3254–3260
8. Alanazi HO et al (2010) Secure topology for electronic medical record transmissions. Int J Pharmacol 6(6): 954–958
9. Alanazi H, Zaidan AA, Zaidan BB, Jalab HA, Al-Ani ZK (2010) New classification methods for hiding information into two parts: Multimedia files and non multimedia files. arXiv preprint arXiv: 1003.4084
10. Al-Ani ZK, Zaidan AA, Zaidan BB, Alanazi H (2010) Overview: Main fundamentals for steganography. arXiv preprint arXiv: 1003.4086
11. Albahri AS et al (2018) Real-Time Fault-Tolerant mHealth System: Comprehensive Review of Healthcare Services, Opens Issues, Challenges and Methodological Aspects. J Med Syst 42(8) Springer US:137
12. Albahri OS et al (2018) Real-Time Remote Health-Monitoring Systems in a Medical Centre: A Review of the Provision of Healthcare Services-Based Body Sensor Information, Open Challenges and Methodological Aspects. J Med Syst 42(9):164
13. Albahri OS, Albahri AS, Mohammed KI, Zaidan AA, Zaidan BB, Hashim M, Salman OH (2018) Systematic review of real-time remote health monitoring system in triage and priority-based sensor technology: Taxonomy, open challenges, motivation and recommendations. J Med Syst 42(5):80
14. Albahri AS, Albahri OS, Zaidan AA, Zaidan BB, Hashim M, Alsalem MA, … Nidhal S (2019) Based multiple heterogeneous wearable sensors: A smart real-time health monitoring structured for hospitals distributor. IEEE Access 7:37269–37323
15. Albahri OS, Albahri AS, Zaidan AA, Zaidan BB, Alsalem MA, Mohsin AH, Mohammed KI, Alamoodi AH, Nidhal S, Enaizan O, Chyad MA, Abdulkareem KH, Almahdi EM, Al-Shafeey GA, Baqer MJ, Jasim AN, Jalood NS, Shareef AH (2019) Fault-tolerant mHealth framework in the context of IoT-based real-time wearable health data sensors. IEEE Access 7:50052–50080
16. Albahri AS et al (2020) Role of biological Data Mining and Machine Learning Techniques in Detecting and Diagnosing the Novel Coronavirus (COVID-19): A Systematic Review. J Med Syst 44(7):122
17. Albahri AS, Al-Obaidi JR, Zaidan AA, Albahri OS, Hamid RA, Zaidan BB, … Hashim M (2020) Multi-biological laboratory examination framework for the prioritization of patients with COVID-19 based on integrated AHP and group VIKOR methods. Int J Inf Technol Decis Mak 19(05):1247–1269
18. Albahri OS et al (2020) Systematic review of artificial intelligence techniques in the detection and classification of COVID-19 medical images in terms of evaluation and benchmarking: taxonomy analysis, challenges, future solutions and methodological aspects. J Infect Public Health 13(10):1381–1396
19. Albahri OS et al (2020) Helping doctors hasten COVID-19 treatment: towards a rescue framework for the transfusion of best convalescent plasma to the most critical patients based on biological requirements via ML and novel MCDM methods. Comput Methods Prog Biomed 196:105617
20. Al-Frajat AK et al (2010) Hiding data in video file: an overview. J Appl Sci 10(15):1644–1649
21. Ali AH, George LE, Zaidan AA, Mokhtar MR (2018) High capacity, transparent and secure audio steganography model based on fractal coding and chaotic map in temporal domain. Multimed Tools Appl 77(23):31487–31516
22. Al-khateeb WF, Hameed SA (2009) New approach of hidden data in the portable executable file without change the size of carrier file using statistical technique. Int J Comput Sci Netw Secur 9(7):218–224
23. Almahdi EM, Zaidan AA, Zaidan BB, Alsalem MA, Albahri OS, Albahri AS (2019) Mobile-based patient monitoring systems: a prioritisation framework using multi-criteria decision-making techniques. J Med Syst 43(7):219
24. Almahdi EM et al (2019) Mobile patient monitoring systems from a benchmarking aspect: challenges, open issues and recommended solutions. J Med Syst 43(7):207
25. Alsalem MA et al (2018) Systematic review of an automated multiclass detection and classification system for acute leukaemia in terms of evaluation and benchmarking, open challenges, issues and methodological aspects. J Med Syst 42(11):204
26. Alsalem MA et al (2019) Multiclass benchmarking framework for automated acute leukaemia detection and classification based on BWM and Group-VIKOR. J Med Syst 43(7):212
27. Alsattar HA, Zaidan AA, Zaidan BB (2020) Novel meta-heuristic bald eagle search optimisation algorithm. Artif Intell Rev 53(3):2237–2264
28. Bai Y, Yao L, Wei T, Tian F, Jin DY, Chen L, Wang M (2020) Presumed asymptomatic carrier transmission of COVID-19. JAMA 323(14):1406–1407
29. Basuki AI, Rosiyadi D (2019) Joint Transaction-Image Steganography for High Capacity Covert Communication. In 2019 International Conference on Computer, Control, Informatics and its Applications (IC3INA). IEEE, pp 41–46

30. Bonino D, Ciaramella A, Corno F (2010) Review of the state-of-the-art in patent information and forthcoming evolutions in intelligent patent informatics. World Patent Inf 32(1):30–38
31. Caplan RM (2003) HIPAA. Health insurance portability and accountability act of 1996. Dent Assist 72(2):6–8
32. Chang MC, Park D (2020) How can Blockchain help people in the event of pandemics such as the COVID-19? J Med Syst 44(5):1–2
33. Cheddad A, Condell J, Curran K, Kevitt PM (2010) Digital image steganography: survey and analysis of current methods. Signal Process 90(3):727–752
34. Elnajjar M, Zaidan AA, Zaidan BB, Sharif MEM, Alanazi H (2010) Optimization digital image watermarking technique for patent protection. arXiv preprint arXiv: 1002.4049
35. Elshoura SM, Megherbi DB (2013) A secure high capacity full-gray-scale-level multi-image information hiding and secret image authentication scheme via Tchebichef moments. Signal Process Image Commun 28(5):531–552
36. Eltahir ME, Kiah LM, Zaidan BB, Zaidan AA (2009) High rate video streaming steganography. In 2009 International Conference on Information Management and Engineering. IEEE, pp 550–553
37. Enaizan O, Zaidan AA, Alwi NM, Zaidan BB, Alsalem MA, Albahri OS, Albahri AS (2020) Electronic medical record systems: Decision support examination framework for individual, security and privacy concerns using multi-perspective analysis. Heal Technol 10(3):795–822
38. Hamdan A et al (2010) New frame work of hidden data with in non multimedia file. Int J Comput Netw Secur 2(1):46–54
39. Hmood AK, Zaidan BB, Zaidan AA, Jalab HA (2010) An overview on hiding information technique in images. J Appl Sci 10(18):2094–2100
40. Hmood AK, Jalab HA, Kasirun ZM, Zaidan BB, Zaidan AA (2010) On the capacity and security of steganography approaches: an overview. J Appl Sci 10(16):1825–1833
41. Hmood AK et al (2010) On the accuracy of hiding information metrics: counterfeit protection for education and important certificates. Int J Phys Sci 5(7):1054–1062
42. Hussain M, Zaidan AA, Zidan BB, Iqbal S, Ahmed MM, Albahri OS, Albahri AS (2018) Conceptual framework for the security of mobile health applications on android platform. Telematics Inform 35(5): 1335–1354
43. Hussain M, Al-Haiqi A, Zaidan AA, Zaidan BB, Kiah M, Iqbal S, Iqbal S, Abdulnabi M (2018) A security framework for mHealth apps on android platform. Comput Secur 75:191–217
44. Hussien HM, Yasin SM, Udzir SNI, Zaidan AA, Zaidan BB (2019) A systematic review for enabling of develop a blockchain technology in healthcare application: taxonomy, substantially analysis, motivations, challenges, recommendations and future direction. J Med Syst 43(10):320
45. Ibrahim NK, Jalood NS, Baqer MJ, Nidhal S, Almahdi EM, Alaa M, Hammed H, Zaidan AA, Zaidan BB, Albahri OS, Alsalem MA, Mohammed RT, Jasim AN, Shareef AH (2019) Multi-criteria evaluation and benchmarking for young learners' English language Mobile applications in terms of LSRW skills. IEEE Access 7:146620–146651
46. Iqbal S, Kiah MLM, Zaidan AA, Zaidan BB, Albahri OS, Albahri AS, Alsalem MA (2019) Real-time-based E-health systems: Design and implementation of a lightweight key management protocol for securing sensitive information of patients. Heal Technol 9(2):93–111
47. Jalab HA, Zaidan AA, Zaidan BB (2009) Frame selected approach for hiding data within MPEG video using bit plane complexity segmentation. J Comput 1(1):108–113
48. Jalab HA et al. (2010) New Design for Information Hiding with in Steganography Using Distortion Techniques. 2(1). https://www.ijetch.org
49. Kalid N et al (2018) Based Real Time Remote Health Monitoring Systems: A Review on Patients Prioritization and Related "Big Data" Using Body Sensors information and Communication Technology. J Med Syst 42(2):30
50. Kalid N, Zaidan AA, Zaidan BB, Salman OH, Hashim M, Albahri OS, Albahri AS (2018) Based on real time remote health monitoring systems: a new approach for prioritization "large scales data" patients with chronic heart diseases using body sensors and communication technology. J Med Syst 42(4):69
51. Khalifa OO et al (2010) Novel approach of hidden data in the (unused area 2 within EXE file) using computation between cryptography and steganography. Int J Comput Sci Netw Secur 9(5):294–300
52. Khatari M, Zaidan AA, Zaidan BB, Albahri OS, Alsalem MA (2019) Multi-criteria evaluation and benchmarking for active queue management methods: Open issues, challenges and recommended pathway solutions. Int J Inf Technol Decis Mak 18(04):1187–1242
53. Kiah MLM et al (2011) A review of audio based steganography and digital watermarking. Int J Phys Sci 6(16):3837–3850
54. Kiah MLM et al (2014) Design and Develop a Video Conferencing Framework for Real-Time Telemedicine Applications Using Secure Group-Based Communication Architecture. J Med Syst 38(10):133

55. Liang X, Shetty S, Zhao J, Bowden D, Li D, Liu J (2018) Towards decentralized accountability and self-sovereignty in healthcare systems. Lect Notes Comput Sci 10631 LNCS: 387–398
56. Majeed A et al (2009) Novel approach for high secure and high rate data hidden in the image using image texture analysis. J Eng Technol 1(2):63–69
57. Malik A, Sikka G, Verma HK (2017) A high capacity text steganography scheme based on LZW compression and color coding. Eng Sci Technol Int J 20(1):72–79
58. Mashamba-Thompson TP, Crayton ED (2020) Blockchain and Artificial Intelligence Technology for Novel Coronavirus Disease 2019 Self-Testing. Diagnostics (10):198
59. Mohammed KI et al (2019) Real-time remote-health monitoring systems: a review on patients prioritisation for multiple-chronic diseases, taxonomy analysis, concerns and solution procedure. J Med Syst 43(7):223
60. Mohammed KI et al (2019) Novel technique for reorganisation of opinion order to interval levels for solving several instances representing prioritisation in patients with multiple chronic diseases. Comput Methods Prog Biomed 105151
61. Mohammed KI, Jaafar J, Zaidan AA, Albahri OS, Zaidan BB, Abdulkareem KH, Jasim AN, Shareef AH, Baqer MJ, Albahri AS, Alsalem MA, Alamoodi AH (2020) A uniform intelligent prioritisation for solving diverse and big data generated from multiple chronic diseases patients based on hybrid decision-making and voting method. IEEE Access 8:91521–91530
62. Mohsin AH et al (2018) Real-time medical systems based on human biometric steganography: a systematic review. J Med Syst 42(12):245
63. Mohsin AH et al (2018) Real-time remote health monitoring systems using body sensor information and finger vein biometric verification: a multi-layer systematic review. J Med Syst 42(12):238
64. Mohsin AH, Zaidan AA, Zaidan BB, Albahri OS, Albahri AS, Alsalem MA, Mohammed KI (2019) Blockchain authentication of network applications: Taxonomy, classification, capabilities, open challenges, motivations, recommendations and future directions. Comput Stand Interfaces 64:41–60
65. Mohsin AH, Jasim AN, Shareef AH, Zaidan AA, Zaidan BB, Albahri OS, Albahri AS, Alsalem MA, Mohammed KI, Nidhal S, Jalood NS (2019) New method of image steganography based on particle swarm optimization algorithm in spatial domain for high embedding capacity. IEEE Access 7:168994–169010
66. Mohsin AH, Zaidan AA, Zaidan BB, Albahri OS, Albahri AS, Alsalem MA, Mohammed KI (2019) Based medical systems for patient's authentication: Towards a new verification secure framework using CIA standard. J Med Syst 43(7):192
67. Mohsin AH, Zaidan AA, Zaidan BB, Albahri OS, Albahri AS, Alsalem MA, Mohammed KI (2019) Based blockchain-PSO-AES techniques in finger vein biometrics: A novel verification secure framework for patient authentication. Comput Stand Interfaces 66:103343
68. Mohsin AH, Jalood NS, Baqer MJ, Alamoodi AH, Almahdi EM, Albahri AS, Alsalem MA, Mohammed KI, Ameen HA, Garfan S, Zaidan AA, Zaidan BB, Albahri OS, Bin Ariffin SA, Alemran A, Enaizan O, Shareef AH, Jasim AN (2020) Finger vein biometrics: taxonomy analysis, open challenges, future directions, and recommended solution for decentralised network architectures. IEEE Access 8:9821–9845
69. Murthy S, Gomersall CD, Fowler RA (2020) Care for Critically ill Patients with COVID-19. JAMA 323(15):1499–1500
70. Muthamilselvan S, Praveen N, Suresh S, Sanjana V (2018) E-DOC Wallet Using Blockchain. In 2018 3rd International Conference on Communication and Electronics Systems (ICCES). IEEE, pp 989–993
71. Nabi MSA, Kiah MLM, Zaidan BB, Zaidan AA, Alam GM (2010) Suitability of using SOAP protocol to secure electronic medical record databases transmission. Int J Pharmacol 6(6):959–964
72. Naji AW (2009) New system for secure cover file of hidden data in the image page within executable file using statistical steganography techniques. Int J Comput Sci Inf Secur 7(1):273–279
73. Naji AW, Hameed SA, Islam MR, Zaidan BB, Gunawan TS, Zaidan AA (2009) "Stego-Analysis Chain, Session Two" Novel Approach of Stego-Analysis System for Image File. In 2009 International Association of Computer Science and Information Technology-Spring Conference. IEEE, pp 410–413
74. Naji AW, Hameed SA, Al-Khateeb WF, Khalifa OO, Gunawan TS (2009) Novel framework for hidden data in the image page within executable file using computation between advanced encryption standard and distortion techniques. Int J Comput Sci Inf Secur 3(1):1–6
75. Naji AW et al (2009) Novel approach for secure cover file of hidden data in the unused area within EXE file using computation between cryptography and steganography. J Comput Sci 9(5):294–300
76. Naji AW et al (2009) New approach of hidden data in the portable executable file without change the size of carrier file using distortion techniques. Proc World Acad Sci Eng Technol 56:493–497
77. Naji AW et al (2009) Challenges of hidden data in the unused area two within executable files. J Comput Sci 5(11):890–897
78. Naji AW, Gunawan TS, Hameed SA, Zaidan BB, Zaidan AA (2009) "Stego-Analysis Chain, Session One" Investigations on Steganography Weakness vs Stego-Analysis System for Multimedia File. In 2009

International Association of Computer Science and Information Technology-Spring Conference. IEEE, pp 405–409

79. Naji AW, Zaidan AA, Zaidan BB, Hameed SA, Khalifa OO (2009) Novel approach for secure cover file of hidden data in the unused area within exe file using computation between cryptography and steganography. J Comput Sci 9(5):294–300 Chicago
80. Napi NM, Zaidan AA, Zaidan BB et al (2019) Medical emergency triage and patient prioritisation in a telemedicine environment: a systematic review. Heal Technol 9:679–700. https://doi.org/10.1007/s12553-019-00357-w
81. Othman F, Maktom L, Taqa AY, Zaidan BB, Zaidan AA (2009) An extensive empirical study for the impact of increasing data hidden on the images texture. In 2009 International Conference on Future Computer and Communication. IEEE, pp 477–481
82. Partala J (2018) Provably secure covert communication on blockchain. Cryptography 2(3):18
83. Ranney ML, Griffeth V, Jha AK (2020) Critical supply shortages - The need for ventilators and personal protective equipment during the Covid-19 pandemic. N Engl J Med 382(18):E41
84. Richardson S, Hirsch JS, Narasimhan M et al (2020) Presenting Characteristics, Comorbidities, and Outcomes Among 5700 Patients Hospitalized With COVID-19 in the New York City Area. JAMA. 323(20):2052–2059. https://doi.org/10.1001/jama.2020.6775
85. Salman OH et al (2017) Novel Methodology for Triage and Prioritizing Using 'Big Data' Patients with Chronic Heart Diseases Through Telemedicine Environmental. Int J Inf Technol Decis Mak 16(05):1211–1245
86. Shuwandy ML et al (2019) Sensor-based mhealth authentication for real-time remote healthcare monitoring system: a multilayer systematic review. J Med Syst 43(2):33
87. Talal M, Zaidan AA, Zaidan BB, Albahri OS, Alsalem MA, Albahri AS, … Alaa M (2019) Comprehensive review and analysis of antimalware apps for smartphones. Telecommun Syst 72(2):285–337
88. Talal M et al (2019) Smart Home-based IoT for Real-time and Secure Remote Health Monitoring of Triage and Priority System using Body Sensors: Multidriven Systematic Review. J Med Syst 43(3):42
89. Tang M, Song W, Chen X, Hu J (2015) An image information hiding using adaptation and radix. Optik (Stuttg) 126(23):4136–4141
90. Taqa A et al (2009) New framework for high secure data hidden in the MPEG using AES encryption algorithm. Citeseer 1(5):8163
91. Tariq I et al (2018) MOGSABAT: a metaheuristic hybrid algorithm for solving multi-objective optimisation problems. Neural Comput & Applic 30:1–15
92. Wang J, Cheng M, Wu P, Chen B (2019) A Survey on Digital Image Steganography. J Info Hiding Privacy Protect 1(2):87
93. Wang CJ, Ng CY, Brook RH (2020) Response to COVID-19 in Taiwan: big data analytics, new technology, and proactive testing. JAMA 323(14):1341–1342
94. Wu Z, Tian L, Li P, Wu T, Jiang M, Wu C (2018) Generating stable biometric keys for flexible cloud computing authentication using finger vein. Inf Sci 433:431–447
95. Yahya AN, Zaidan AA, Zaidan BB, Jalab HA, Alanazi HO (2010) A new system for hidden data within header space for EXE-File using object oriented technique. In: 2010 3rd International Conference on Computer Science and Information Technology, vol 7. IEEE, pp 9–13
96. Zaidan AA, Zaidan BB (2009) Novel approach for high secure data hidden in MPEG video using public key infrastructure. Int J Comput Netw Secur 1(1):1553–1985
97. Zaidan BB, Zaidan AA (2017) Software and hardware FPGA-based digital watermarking and steganography approaches: toward new methodology for evaluation and benchmarking using multi-criteria decision-making techniques. J Circ Syst Comput 26(07):1750116
98. Zaidan BB, Zaidan AA (2018) Comparative study on the evaluation and benchmarking information hiding approaches based multi-measurement analysis using TOPSIS method with different normalisation, separation and context techniques. Measurement 117:277–294
99. Zaidan AA, Zaidan BB, Jalab HA (2010) A new system for hiding data within (unused area two+ image page) of portable executable file using statistical technique and advance encryption Standared. Int J Comput Theory Eng 2(2):218
100. Zaidan AA, Zaidan BB, Alanazi OH, Gani A, Zakaria O, Alam GM (2010) Novel approach for high (secure and rate) data hidden within triplex space for executable file. Sci Res Essays 5(15):1965–1977
101. Zaidan BB, Zaidan AA, Othman F (2008) Enhancement of the amount of hidden data and the quality of image. Faculty of Computer Science and Information Technology. University of Malaya, Kuala Lumpur, Malaysia
102. Zaidan AA, Othman F, Zaidan BB, Raji RZ, Hasan AK, Naji AW (2009) Securing cover-file without limitation of hidden data size using computation between cryptography and steganography. In: Proceedings of the World Congress on Engineering, vol 1, pp 1–7

103. Zaidan AA, Zaidan BB, Majeed A (2009) High securing cover-file of hidden data using statistical technique and AES encryption algorithm. World Academy of Science Engineering and Technology (WASET) 54:468–479
104. Aos AZ, Naji AW, Hameed SA, Othman F, Zaidan BB (2009) Approved undetectable-antivirus steganography for multimedia information in PE-file. In: 2009 International Association of Computer Science and Information Technology-Spring Conference. IEEE, pp 437–441
105. Zaidan B et al (2009) Stego-image vs stego-analysis system. Citeseer 1(5):1793–8163
106. Zaidan AA et al (2009) New technique of hidden data in PE-file with in unused area one. Int J Comput Electr Eng 1(5):642–650
107. Zaidan B et al (2009) Quality of image vs. quantity of data hidden in the image. IPCV 6:343–350
108. Zaidan AA et al (2009) High securing cover-file of hidden data using statistical technique and AES encryption algorithm. World Acad Sci Eng Technol 54:463–474
109. Zaidan BB, Zaidan AA, Taqa AY, Othman F (2009) An empirical study for impact of the increment the size of hidden data on the image texture. ICFCC09
110. Zaidan BB, Zaidan AA, Al-Frajat AK, Jalab HA (2010) On the differences between hiding information and cryptography techniques: an overview. J Appl Sci 10(15):1650–1655
111. Zaidan AA, Zaidan BB, Al-Fraja AK, Jalab HA (2010) Investigate the capability of applying hidden data in text file: an overview. J Appl Sci 10(17):1916–1922
112. Zaidan AA, Zaidan BB, Taqa YA, Sami MK, Alam GM, Jalab AH (2010) Novel multi-cover steganography using remote sensing image and general recursion neural cryptosystem. Int J Phys Sci 5(11):1776–1786
113. Zaidan BB et al (2010) StegoMos: a secure novel approach of high rate data hidden using mosaic image and ANN-BMP cryptosystem. Int J Phys Sci 5(11):1796–1806
114. Zaidan BB et al (2015) A Security Framework for Nationwide Health Information Exchange based on Telehealth Strategy. J Med Syst 39(5):51
115. Zaidan AA et al (2015) Challenges, Alternatives, and Paths to Sustainability: Better Public Health Promotion Using Social Networking Pages as Key Tools. J Med Syst 39(2):7
116. Zaidan BB, Zaidan AA, Karim HA, Ahmad NN (2017) A new digital watermarking evaluation and benchmarking methodology using an external group of evaluators and multi-criteria analysis based on 'large-scale data. Softw Pract Exp 47(10):1365–1392
117. Zaidan BB et al (2017) A new approach based on multi-dimensional evaluation and benchmarking for data hiding techniques. Int J Inf Technol Decis Mak:1–42. https://doi.org/10.1142/S0219622017500183
118. Zaidan AA, Atiya B, Bakar MA, Zaidan BB (2019) A new hybrid algorithm of simulated annealing and simplex downhill for solving multipleobjective aggregate production planning on fuzzy environment. Neural Comput & Applic 31(6):1823–1834
119. Zaidan AA, Zaidan BB, Albahri OS, Alsalem MA, Albahri AS, Yas QM, Hashim M (2018) A review on smartphone skin cancer diagnosis apps in evaluation and benchmarking: coherent taxonomy, open issues and recommendation pathway solution. Heal Technol 8(4):223–238
120. Zaidan AA, Zaidan BB, Alsalem MA, Albahri OS, Albahri AS, Qahtan MY (2020) Multi-agent learning neural network and Bayesian model for real-time IoT skin detectors: a new evaluation and benchmarking methodology. Neural Comput & Applic 32(12):8315–8366
121. Zaidan AA, Zaidan BB, Alsalem MA, Momani F, Zughoul O (2020) Novel Multiperspective Hiring Framework for the Selection of Software Programmer Applicants Based on AHP and Group TOPSIS Techniques. Int J Inf Technol Decis Mak 19(3):775–847
122. Zhao H, Liu Y, Wang Y, Wang X, Li J (2018) A Blockchain-Based Data Hiding Method for Data Protection in Digital Video. In: Qiu M (ed) Smart Blockchain. SmartBlock 2018. Lecture Notes in Computer Science, vol 11373. Springer, Cham. https://doi.org/10.1007/978-3-030-05764-0_11
123. Zughoul O, Momani F, Almasri OH, Zaidan AA, Zaidan BB, Alsalem MA, … Hashim M (2018) Comprehensive insights into the criteria of student performance in various educational domains. IEEE Access 6:73245–73264

Affiliations

A. H. Mohsin[1,2] • A. A. Zaidan[1] • B. B. Zaidan[1] • K. I. Mohammed[1] • O. S. Albahri[1] • A. S. Albahri[1,3] • M. A. Alsalem[1]

✉ A. A. Zaidan
aws.alaa@fskik.upsi.edu.my

A. H. Mohsin
ali_hadi182@yahoo.com

B. B. Zaidan
bilalbahaa@fskik.upsi.edu.my

K. I. Mohammed
khalid_ib1@fskik.upsi.edu.my

O. S. Albahri
osamah@fskik.upsi.edu.my

A. S. Albahri
ahmed.bahri1978@gmail.com

M. A. Alsalem
mohammed.asum@gmail.com

[1] Department of Computing, Universiti Pendidikan Sultan Idris, Tanjong Malim, Perak, Malaysia

[2] Republic of Iraq-Presidency of Ministries - Establishment of Martyrs, Baghdad, Iraq

[3] Informatics Institute for Postgraduate Studies (IIPS), Iraqi Commission for Computers and Informatics (ICCI), Baghdad, Iraq