International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

A Novel Approach to Blockchain and Deep Learning in the field of Steganography

Ms. Ayushi Chaudhary[1*], Prof. Ashish Sharma[2], Dr. Neeraj Gupta[3]

Submitted: 18/10/2022 **Revised:** 20/12/2022 **Accepted:** 22/01/2023

Abstract: Our daily lives have been changed by electronic technology. To maintain cybersecurity, secure and reliable connection is necessary, to improve the robustness and effectiveness of these techniques Securing a large amount of data is a major challenge during the communication of data over the network. Confidentiality and integrity play an important role while transferring the data in the field of health, defence, and conference meetings. As a result, this study suggests using Blockchain and Deep Learning in addition to innovative steganography. Along with this the hash function is used to hide the secret data which provides high entrenching capability and high eminence data input images. Stego images along with hash function generating datasets, along with Blockchain technology are used to improve the efficiency of securing the data during communication over network. In the proposed model the deep learning algorithms adds the more security to the data that is stored in the Blockchain. The data extracted using deep learning is stored in the Blockchain which is free from null values, and duplicate values. Thus the proposed model helps in achieving securing the data in more efficient way by avoiding third party to hack the data.

Keywords*: Steganography, Deep Learning, Blockchain, confidentiality, cyber security*

1. Introduction

With the invention of 6G technology, huge data are communicated over public channels. This leads to huge security challenges on the information shared on the network. Hence significant to securely transmit the information which can be in the form of images, audio, or video must be provided. There exist many security approaches such as encryption, watermarking, steganography, and many more. In the encryption approach, the full information is encoded by using the secret keys, and the hidden information is decoded at the receiver end using the secret keys. Encrypting the information may be insecure because attackers can easily trace the information that is hidden information. To overcome this disadvantage, the information is hidden with some images, video, or audio using the concept called steganography. In steganography, the information is transmitted by hiding in the images, audio, or video, without changing any patterns. The secret information is hidden in the cover image and transmitted through the network. The hidden information on the cover page is not noticeable to the attackers. The hidden information inside the cover image is called the stego image. However, the main apprehension is in integrating the information inside the cover page so as to protect it from intruders. To address the security of information, the Blockchain framework can be applied for transforming information in a more efficient way. But Blockchain technology also faces majority attacks such as double-spending. In a decentralized system like Blockchain, the bulk of attacks are conducted by a group of people or groups that work together to seize control of the ledger and profit from it. To overcome these attacks machine learning algorithm can be used and avoid the majority of attacks that may take place by using Blockchain technologies[1].

1.1 Steganography:

Since the practice of steganography is one of disguising information without raising suspicion, the word steganography literally translates as "Covered writing" and has Greek origins. It consists of a wide variety of covert communication methods that mask the mere existence of the message. The term "steganography" originally appeared in 1499 in the book Steganographia by Johannes Trithemius [2]. Despite the title's explicit reference, the book focused mostly on esoteric topics and cryptography procedures. In the fifth century BC, when people used to write messages on wax-coated tablets, Herodotus described the earliest known use of steganography. The message remained hidden behind the wax layer in this manner. Herodotus also recorded that Histiaeus, the ruler of Miletus under Darius I of Persia, wished to speak with his Greek son-in-law [3]. In order to accomplish this, had tattooed the message onto the slave's

ayushichaudhary11@gmail.com
ashish.sharma@gla.ac.in
neeraj.gupta@gla.ac.in

GLA University,

scalp after shaving the skull of one of his most dependable slaves. He sent the slave with the concealed message when his hair had grown back, and when the slave arrived at the destination once more, he shaved his head and retrieved the message.

Steganography is primarily employed today to safeguard private data. As a result of the effective growth in demand for digital communication, the internet has permanently evolved into the most potent and quick method of digital communication. Simultaneously, as data on the internet has developed into a target for copyright violations, hacking, and eavesdropping, the demand for secure and trustworthy communication has grown. In steganography the communication is carried out as, the recipient receives the stego object x(m), which was created by the sender using a cover object x to embed a secret message m. To increase security, the sender might use an optional key (k). The recipient uses the corresponding key to extract the object's concealed information after it has been communicated using stego.

1.2 Features of steganography:

Since steganography has been explored within the context of informatics and computer science, several methods have been devised to embed messages in data that appears innocent, but their primary goal is the development of secure and reliable steganographic protocols. So imperceptibility and robustness are characteristics of a stego-medium that are anticipated. Robustness is a key feature to prevent secret messages from being known to anybody but the intended receiver [4]. However, the stego object should be unable to defend against intruder attacks. The Figure 1.1 depicts the Stegnography.

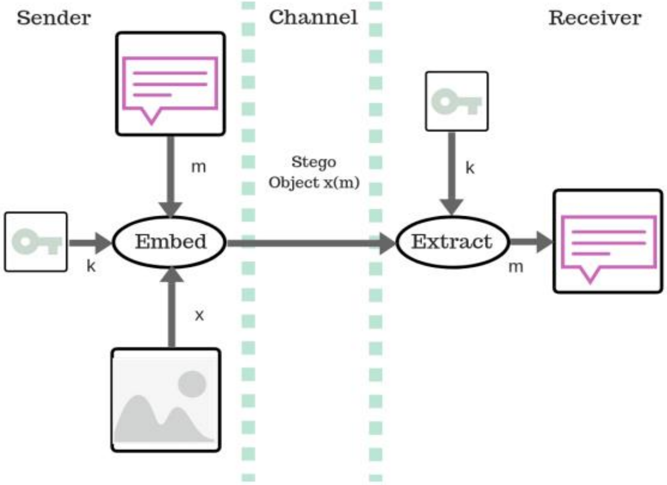


Fig. 1.1 The Steganography Scheme

Taking into account everything mentioned above, it is simple to list the three crucial characteristics [5] of a steganographic method: imperceptibility, embedding ability, and robustness. The term "imperceptibility" describes the incapacity of a person to tell the cover from the stego item and, as a result, to recognize the existence of hidden information. Additionally, the embedding or payload capacity is the maximum quantity of secret data that may be inserted into a cover item without lowering the object's quality. The payload capacity in picture steganography is expressed in bits per second.

2. Applications of Steganography

Advanced data structures in medical images where the patient's record is embedded into the image enabling information protection and decreasing transmission time, and powerful watermarks are only a few examples of the wide range of applications for steganography. military organizations document tracking tools document authentication intelligence agencies general communication online elections smart identity cards radar systems, modern printers, and remote sensing.

Blockchain: In Bitcoin (Nakamoto, 2018), Blockchain technology is introduced as the core mechanism for crypto-currency as an open, decentralised method of establishing trust. Blockchain is a decentralised platform for information exchange between nodes that acts as a public record of data gathered through a network and represented as a chain of blocks [31]. The use of cryptographic hashing connects these blocks to one another. By maintaining integrity, it makes it possible for the data to be tamper-proof. For individuals or groups of individuals who do not trust one another to coordinate and participate in a cogent decision-making process but desire to come to a common platform to share information among them, blockchain technology is useful. Blocks, nodes, and miners are three key ideas.

Key Terminologies related to Blockchain:

A hash algorithm [6] is a function that transforms data into a fixed-length, numeric string output known as a hash value. In the proof of work algorithm, for example, this hash value is frequently used to check the accuracy of the data. These hash values are intended to be collision-resistant, making it unlikely for separate pieces of data to produce the same hash value and making it challenging to locate. A Blockchain's block contains the hash value of the data it contains. Additionally, hashes of an owner's private key and the required data are frequently used to create signatures that confirm transactions. Blocks, nodes, and miners are three key ideas.

Proof of work (POW) [7] is a zero-knowledge proof system based on cryptography that demonstrates both the existence of some data and the existence of some computing work supporting the data's authenticity. Any node that wishes to create a new block in a blockchain system must write all transactions to the blockchain and solve a proof-of-work challenge. Users are rewarded for mining and validating blockchain transactions. The blockchain underpins the network, with the majority of the effort being done to verify and broadcast block information to other network nodes.

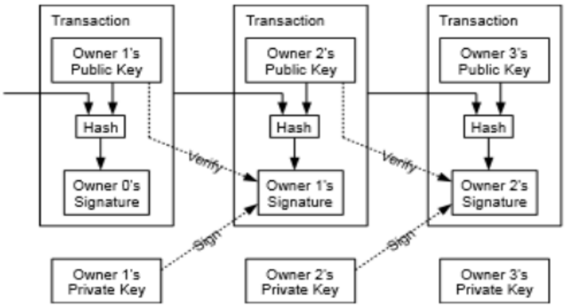


Fig. 1.2: Proof of work (POW)

Timestamp: To combat the problem of double spending, timestamps are utilised. The ownership of the money involved in a transaction cannot be transferred again because the blockchain system publishes the hash block of things together with a timestamp server and uses the timestamp network [8] to verify that the data must have existed at the time.Each hash contains the timestamp from the previous block, creating a chain in which each block reinforces the ones that came before it.

Machine Learning

Machine Learning techniques are often used to build, train, and evaluate the steno images. Machine learning is a branch of artificial intelligence research that uses computers to mimic human learning abilities [9]. The three main subcategories of machine learning are reinforcement learning, unsupervised learning, and supervised learning. The process of supervised learning, which is frequently used in speech recognition, spam detection, and object recognition, involves learning a function that maps an input to an output by receiving input-output pairs. Unsupervised learning refers to the process of gaining knowledge from test data that has not been labelled, categorised, or classified. Principal component analysis, cluster analysis, vector quantization, and self-organization are the main fields in which unsupervised learning is used. How to act in order to maximise a hypothetical cumulative reward is the focus of reinforcement learning [10]. The goal of reinforcement learning is to choose the best course of action to maximize a hypothetical cumulative reward. Robotics, investment analysis, and inventory management all use reinforcement learning to teach their systems what actions to take. Machine learning, which is focused on learning data representations, includes deep learning as one of its subfields.

Figure 1.4 illustrates the procedure for using machine learning for steganography analysis. Data collection, model construction, training, and evaluation are its four stages.

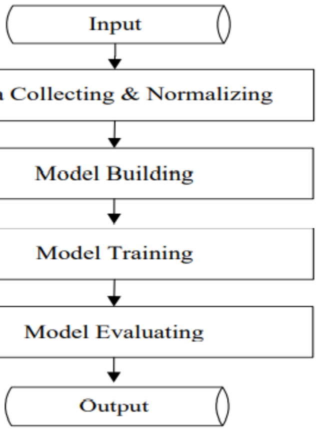


Fig.1.3: Stenography using Machine Learning

To improve accuracy, a lot of training and test data should be gathered and homogenised. Since images are employed in steganography and steganalysis in general, it is necessary to do vectorization in particular by feature extraction from photos. Depending on the machine learning framework, different algorithms can be used throughout the model creation, training, and assessment phases.

3. Literature Survey

Mustafa Muneeb Taher et.al.proposed the Robustness and normalized cross-correlation (NCC) are two key components of steganography [12]. In this context, Digital steganography has undergone significant research advancements. Meanwhile, the protected and privacy-preserving communication through the WWW (World Wide Web) has been severely threatened by such unfettered access to such a massive amount of information and *Punidha et al.* utilized the integer wavelet transform and the well-known Haar wavelet approach to conceal messages. The study defines, Steganography is an intelligent data hiding technology where the secret data is implanted in a cover media in such a way that the goal of both cryptography and steganography is to hold and save the secret message and secure it from hackers or attackers. Authors introduced the term "computational intricacy" in steganographic techniques correlates to the accuracy of the embedding algorithms, and some machine attempting to learn techniques call for a high level of computational skill. The reviewers use the integer wavelet, transform concept to lack of standardization transfer audio speech signals.

Indrajit et al. [13] proposed, addressing multiple attack types is now a necessary precondition. The main definition of Automated teller machine (ATMs) are the devices that are most regularly used nowadays for financial transactions, and PINs are typically used in these devices . According to PINs which are used for identity documents, are simple yet is nevertheless powerless in the face of the various types of use an assault (Phishing attack, Spoofing attack, Sniffing etc.). The researchers have mentioned that security of the one of vein authentication system's information exchange has subsequently been the subject of research by various researchers across the globe . The study's goal is also about a biometrics authentication system and a combined approach of cryptography and steganography are proposed for the transfer of banking transaction information reliably through ATMs.

Boughaci D et al. has proposed a well-known algorithm called single bit LSB [14] replacement allows for the replacement of a single bit from an image pixel in each carrier pixel. The researchers also say that, average victim's life is now being threatened by the increasing, horrific incidents of attacks on private information, *Park K R et al.* have presented in the context of capital transactions and banking-related activities at automated teller machines (ATMs) about Finger vein identification by combining global and local features based on SVM [18].

Inas et al. [15] have researched in the field of cryptography, which deals with various methods of data encryption, was among the most interesting ones in the data management field . Its goal is to encrypt secret information using different approaches and then transform it into a written form. *H. Wang et al.* have proposed that any steganographic system ought to have three things specifically, imperceptibility, security, Payload, Robustness and the capability of hiding information, some applications, including Smart stegno portable devices encrypting multisensory biometric information , securing IP (Intellectual Properties), and encoding personal details in smart identity cards .

A.K. Sahu et al. [16] also stated that many metrics are applied to evaluate the various aspects of steganographic techniques. According to popular measures have included Peak Signal to Noise Ratio, Correlation Analysis, Histogram Compare, the Structure Similarity Index Measure (SSIM), and Payload Capacity. *S. Bhatt et al*. article paper outlines the survey indicates that systems having appropriate learning schemes have effective image steganography systems, and studies may be focused on deep attempting to learn schemes for greater image steganography system applications. *A. Miri et al*. detailed the image adaption steganography where it has relied upon transform domain through genetic techniques.

The challenge for author *Płachta, Mikołaj et al.* [17] of identifying Image files that have been lack of standardization manipulated is covered in this article. Based on analysis is done about how well different shallow and computational model strategies operate when used to discern visual steganography. According *Yang, Z et al.* defined about the wide availability of this file format, multiple data-hiding techniques as well as distinct identification strategies have been offered, nsF5, JPEG universal wavelet relative distortion (J-Uniward), and uniform embedding revisited distortion (UERD) are a few examples of the algorithms we chose. Therefore, in this part, we first go through the properties that are most frequently employed with steganographic algorithms before going over some standard instances of superficial and deep attempting to learn detection algorithms in brief. *Huang G et al*. mentioned the image features DCTR, GFR, and PHARM, tests were conducted. In order to train our systems, we used couples of photos with and without steganographically disguised data.In this article study, we analyzed the performance of shallower, intermediate, and supervised learning methods for finding hidden information in Jpeg format. Although the nsF5 approach can almost perfectly confirm the presence of information concealed at a concentration of 0.4 bpnzac, J-Uniward cannot be used to identify information concealed at a concentration of 0.1 bpnzac .

The accurate assessment done by *Eng-Jon Ong et al*. [18] of videos at the snippet stage using an extensive word of keywords is indeed a difficult task. This essay focuses on the research on the above mentioned Kaggle challenge. Applying DNNs, has there already emerged substantial advancement in picture diagnosis and characterization . The GAP20 accuracy range for DNN is similar, falling between 82 and 83 percent. It's unclear when additional training samples will help to solve this. *A. Guzman-Rivera et al*. have discovered that the solitary parameter aggregation of 13 different base DNNs provides us with the most cutting-edge GAP20 efficiency, which is 85.12%. On the UCF101 and HMDB51 databases, we also executed classification technique on the already-existing DNNs from the abovementioned and showed that, not with standing the employing features vectors that are significantly more compacted than full RGB frames, *S. Zhao et al.* methodologies execute on par with jurisdiction strategies. Additionally, assembling has been shown to significantly boost these collections.

Ilhan et al.[19] put forth majority of research have been carried on a modest number of digital sets. This gives no obvious indication of how well the data points performed. The effectiveness of three classifiers—SVM, KNN, and DT—that are often used in the research has been evaluated for the five large datasets used in this work. Section 3 provides public IDS datasets. The classifiers employed in the study are described in Section 4 of the report. In Sections 5 and 6, respectively, the suggested approach and experimental findings are described. To choose the optimal subset of features for the malware detection, they used multilayer multiple linear regression based on an evolutionary algorithm. Several data points that are routinely used for malware detection, including *Sharafaldin et al.* [11] created CSE-CIC IDS-2018.*Moustafa et al.* [19] set up UNSW-NB15, ISCX-2012 , NSL-KDD were employed in this work. In terms of different classifiers, it has also been noted that the DT classifiers performs better than the other ones that have been employed. For the CSE-CIC IDS-2018, ISCX-2012, NSL-KDD, and CIDDS-001 data sets, DT's success rates of between 99 and 100 percent are comparable to those reported in the literature .

On December 31, 2019, the World Health Organization [20] became aware of a new coronavirus. *A.H Mohsin et al.* have researched on the coronavirus infection 2019 (COVID-19) epidemic has had a profound impact on people's lives and is the biggest revelation toward the world in recent memory . *Jasmin AN et al*. have proposed new steganalysis technique based on the PSO algorithm was previously published for hiding hidden message inside a host image. According to, the most effective bit positions for concealing sensitive data in hosted images are discovered using this technique . The optimal bit position is where there is the least danger of message bits being distorted when they are inserted. Detailed covering the section of private COVID-19 health information in host pictures, Classified healthcare COVID-19 transmitting data level (stego pictures) etc. This technique may categorize platelet donors, management concepts patients (SODOSM) dependent on the level of emergency, and correlate plasma statistics with the information of validated donor CPs. It is possible to replicate the way that has been suggested for securing the recent publication structure in a medical for the preservation and donation of the optimum CP to the most vulnerable COVID-19 patients based on the biological criteria.

Satoshi Nakamoto [21] impacted the market when launched the software known as Bitcoin. As additional companies participate in this extraction and processing, "miners pools" are created, and when a bitcoin mining has 51 percent of the computational power. To maintain the suspect's achievement (twice expenditure) at a study by *Rosenfeld* , baseline of 10%, 1%, and 0.10%. Author suggests to make use of some modifications of the Confirmation suggested in this employment in order to stop such nefarious conduct in the consensus based Blockchain systems. The likelihood that the decision makers/reviewer will launch a takeover attack is based on the actual valuation of the service or good getting sold in the present agreement.

Souvik et al. [22] technique of disguising knowledge by enclosing communications in other, seemingly inconsequential communications is known as steganography. This type of mechanism a cryptic information that is virtually impossible for the naked eye to distinguish into an image as noise. The several visual image steganography methods include: (i)Substitution in the Spatial Domain, (ii)Transform domain technique: Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), and Fast Fourier Transform (FFT) are some of the transform domain techniques etc.

Authors also presented data hiding by MBNS, Data hiding by QIM, etc. Particular stego techniques depend on the specific steganography technique employed and are based on the bitmap image type (such as GIF, BMP, and JPEG formats). The information incorporation in the speech signals causes fluctuations in its defining characteristics, which the aural steganography systems take advantage of. This article paper summarizes steganography and steganalysis techniques land in four similar cover areas.

Andres et al. [23] in their research explored if and how that is able to exchange information from sensory input and accurate 3D audio, specifically acoustic pictures, in an attempt to optimize audio categorization using a solitary microphone. In order to achieve this, we make use of a unique sensor called Dual Cam proposed by *A. Zunino et al*., a sound waves camera that produces spatially and temporally synchronized audio information. By using this technology, we were able to collect an experience and new of acoustic conveyed behavior in three different circumstances. We want to use this information to extract information that will be helpful for audio categorization. Here, we want to draw attention to the fact that the suggested classroom architecture is the first to be able to turn 2D visual data and acoustic images into a model that uses a 1D paradigm, specifically audio waves, as data. *A. Owens* et al. study will focus on investigating the potential of this identity acquisition, identification, and classification bridge retrieval and sound source mapping.

Doaa et al. [24] had begun putting a lot of effort into image steganography to identify and prevent fraudulent application because of the risky and illegal uses of data encryption in the background . In addition to extraction of features, human brains may also be employed as classifiers. According to, acoustic sentiment analysis seeks to identify any shift in a waveform brought on by embedded information. for semi files and steganalysis methods for condensed files as MP3 and AAC [24]. *Li et al* computational complexity reduction effort relies on no foreknowledge of the amount of frequency hopping bearers. Once that was done, the enhanced NPELO (Near-Perfect Estimation for Local Optimality) and MVRBR (Motion Vector Reversion-Based Steganalysis Revisited) characteristics were collected from every classification and given to a separate SVM Classification model.

Sherif et al. [25] in their study presents a review of steganography methods from the perspective of picture formats, keeping in mind the most widely used image formats, JPEG, BMP, GIF, and PNG [2]. Due of JPEG images fading encoding, most steganalysis methods for them operate in the spectral domain in order to ensure the survival of the hidden data . However, the majority of steganography methods for BMP, GIF, and PNG pictures are spatial domain methods. When comparison to the subspace, the sine wave is more durable. The visual processing system cannot detect cryptographic primitives in grayscale photos , but its steganography approaches are simpler than those for colored images. *H.B Kekre et al*. research paper comparison to colorful images, monochromatic images have a 100 % detection prediction performance, according on the findings of previous literature research. The majority of BMP steganography procedures created their individual databases rather than using demonized ones for their tests .

It is normal practice of *Christian et al.* [26] in their study paper to divide steganalytical approaches into distinct and general subcategories when analyzing them. Steganography methods by combining already known methods, as mentioned by *Kharrazi et al* . The auditory cryptographic methodology described provides the foundation for this study provided in this study. The VoIP steganography-related introduction of the audio steganalysis tool (AAST; AMSL Audio Steganography Toolset). Accordingly, Type I and II mistakes, and discriminating power. These assessments assess the AAST's functionality as a general steganography tool, as well as its particular efficiency on a range of techniques and the VoIP asymmetric encryption implementation case. The detailed flexibility of the taught classification algorithm being employed as well as the prevalence of erroneous data are also addressed in these queries.

In the research paper of *Barani et al.* [27] Steganalysis essentially takes care of hiding the secret material in a disseminated means so that its presence cannot be detected. Steganography of hiding information in a distributed medium for secret and private communication.The obtained extraction is applied in 3D reconstruction, motion, recognition, image enhancement and reconstructing, photograph membership, picture pressures, and other activities . Above that the boundary quantity and slope values of this gradient vector (G) can then be juxtaposed, and these numbers are referred to as gray levels.

Nedumaran, A et al. [28] study paper based on these colors contrast with the hues of the object's cell edge. The maximum severe error that really can occur in AER is 7, therefore the aforementioned requirement becomes the condition for AER strategy and yields an estimate of 30.069 dB. However, this value is obviously ahead of the PSNR for the MER tool's utmost severe scenario by 6 dB, which really is a substantial increase.

Yuanyuan et al [29] in their study explores rapid advancement of industrial model and the emergence of new Automation applications, such as intelligent cars the researchers. had published this paper. According to 6G's theoretical goals, maximum data rates must be at least a single Tb/s, latency must be 10–100 s, velocity must exceed 1000 km/h, and viewer data rates must be at least 1 Gb/s . The 6G generation will end the knowledge stranglehold and develop a sizable economy for information exchange and trade. Enormous private information and easier access to data may increase the need for security protocols, complicate regulatory concerns, and possibly even lead to incidents involving data. The latest ML patterns, unresolved questions, and legal implications were properly covered. Intelligence and information preservation are unquestionably important aspects of the 6G agenda. *Quo.L et al.* could use ML fully while keeping security protected, rather than only adopting it for that purpose. The benefits of Intelligence and strong privacy equipment can be integrated in this place to create the upcoming 6G era safer and more efficient.

4. Proposed Model: Steganography with Blockchain and Deep Learning

Securing the data especially in the areas like the medical field, defence, and online conferences and communication via a network. Recent technology like steganography along with machine learning and Blockchain can be used to overcome the security challenges that are faced in today's 6G communication.

In the proposed model secret data are taken and hidden using the cover pages such as text images, audio, or videos during communication securely via network. This input is considered as the cover image and later original information is hidden which is called the stegano image. During the analysis of diseases, the input which are in the audio sound form for example in medical field such as coughing sound, heartbeat sound, the medical reports from doctors plays an important role. The AI techniques [32] helps in automating these diagnostics by identifying sounds, classifying them, and listening to the audio spectrum. Once the diseases are identified, these medical related data are stored for further analysis. This is one application where Blockchain can be applied to secure the medical reports through a network. Thus for securing the data, most emerging technology called Blockchain with the deep learning technique to extract the relevant data is applied in the proposed model. The architecture for the proposed model is shown in figure 4.1

The proposed steganography method using Blockchain and Deep Learning is given below:

Deep Learning is used to store the data which is to be analysed and predicted in the Blockchain network. The data stored in the Blockchain helps in improving the efficiency during the analysis and prediction process by Deep Learning algorithms used such as CNN with LSTM. This is possible since data stored in the network will not have null values, duplicates, missing values, or noise which is very much important to remove all this in order to get the more accurate results of the proposed model.

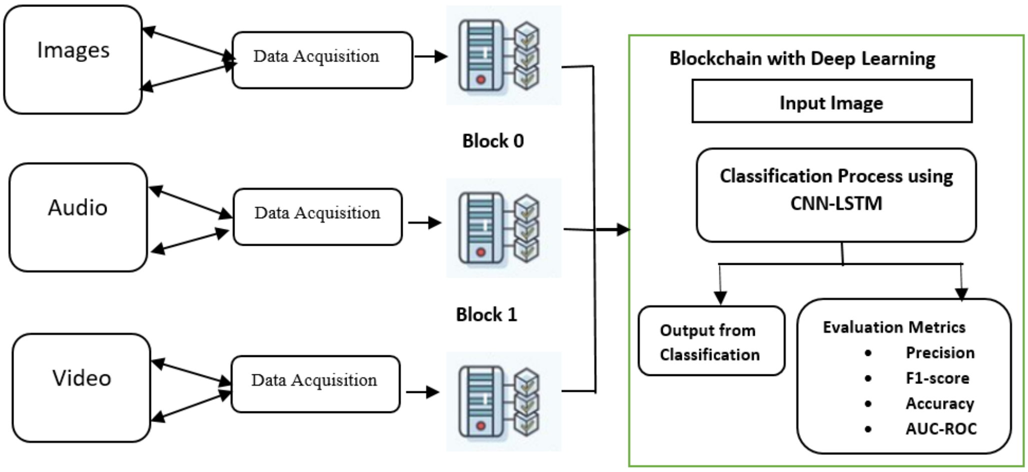


Fig. 4.1: Blockchain with Deep Learning

Figure 4.2 and 4.3sheds on the various steps necessary for the successful deployment of the Deep Learning model. Data collection is the first step, after which it is prepared for training by being screened for bias or labelled. Then, a classifier is either created or chosen from an existing set based on the requirements of the application.

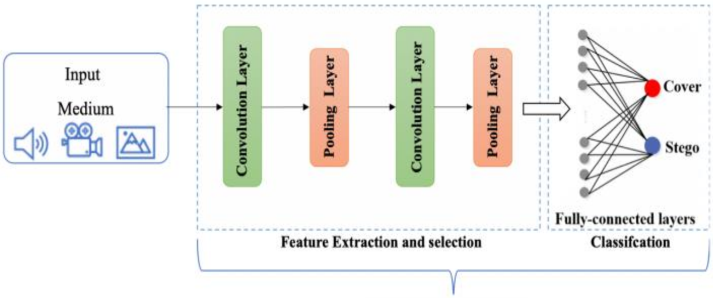


Fig. 4.2: Steganalysis using CNN

For the gathered dataset, a classifier is trained, and its performance can be increased by changing certain parameters. The deployed trained model will then begin retraining in preparation for future improvement.

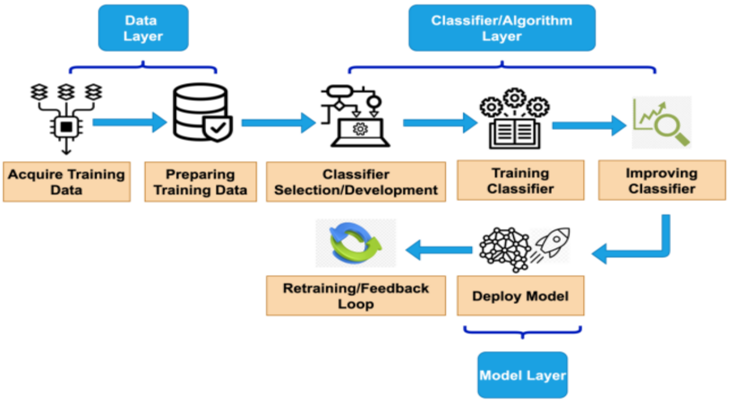
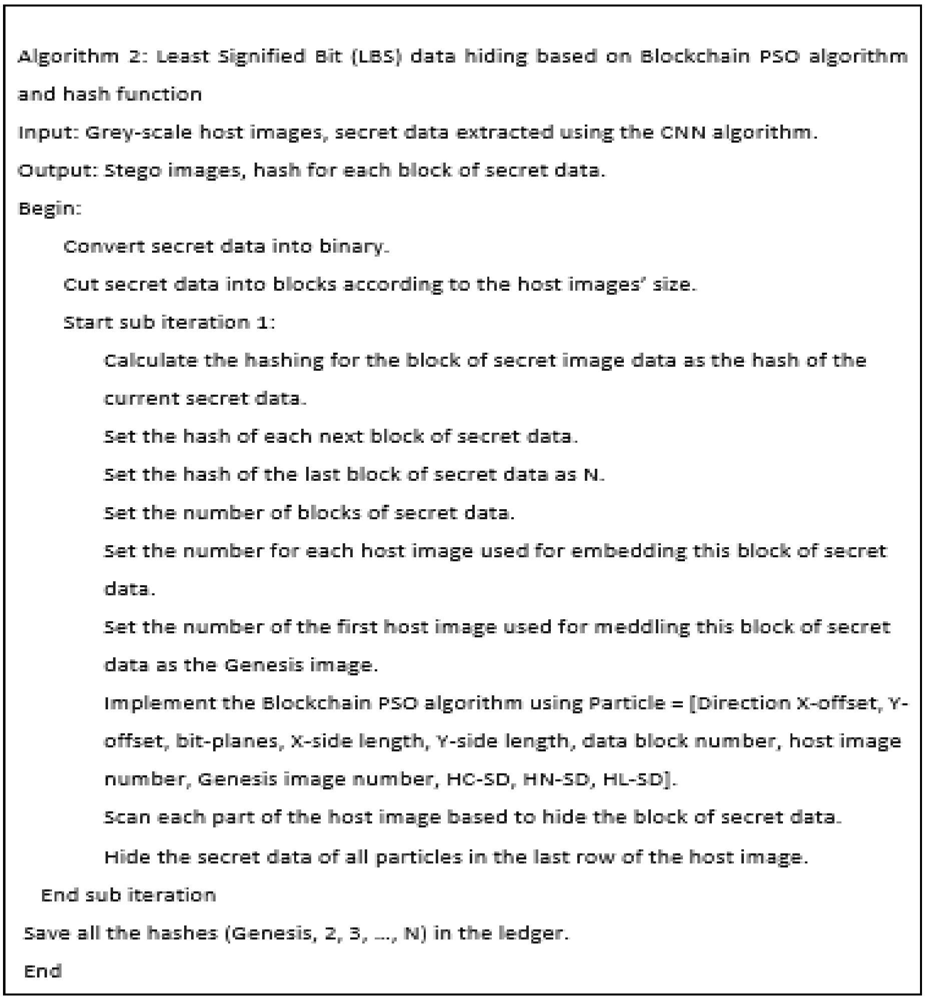


Fig. 4.3: Stages involved in the deploying the Deep Learning Algorithms

Blockchain technology[30] can be used to secure this training process, as depicted in Figure 4.2The retrieved features from the trained model will be saved in the Blockchain for further reference in a feature vector.

```
Algorithm 1:
        Finding the best bit location in the host image for a secret data set.
        Input: Images selected from different sources.
        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 data extracted using
            the CNN algorithm embedded in the image.
            Start sub iteration
                Implement the CNN-LSTM algorithm to Scan each part of the
                host image.
            End sub iteration
        Set the embedding capacity of the image.
End
```



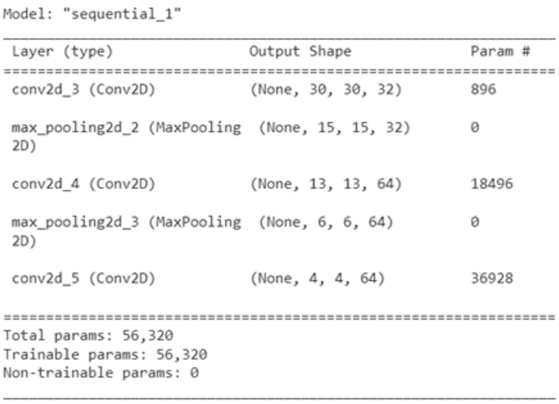
```
Algorithm 2: Least Signified Bit (LBS) data hiding based on Blockchain PSO algorithm
and hash function
Input: Grey-scale host images, secret data extracted using the CNN algorithm.
Output: Stego images, hash for each block of secret data.
Begin:
    Convert secret data into binary.
    Cut secret data into blocks according to the host images' size.
    Start sub iteration 1:
        Calculate the hashing for the block of secret image data as the hash of the
        current secret data.
        Set the hash of each next block of secret data.
        Set the hash of the last block of secret data as N.
        Set the number of blocks of secret data.
        Set the number for each host image used for embedding this block of secret
        data.
        Set the number of the first host image used for meddling this block of secret
        data as the Genesis image.
        Implement the Blockchain 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 to hide the block of secret data.
        Hide the secret data of all particles in the last row of the host image.
  End sub iteration
Save all the hashes (Genesis, 2, 3, ..., N) in the ledger.
End
```

Fig. 4.4: Algorithm for the proposed model

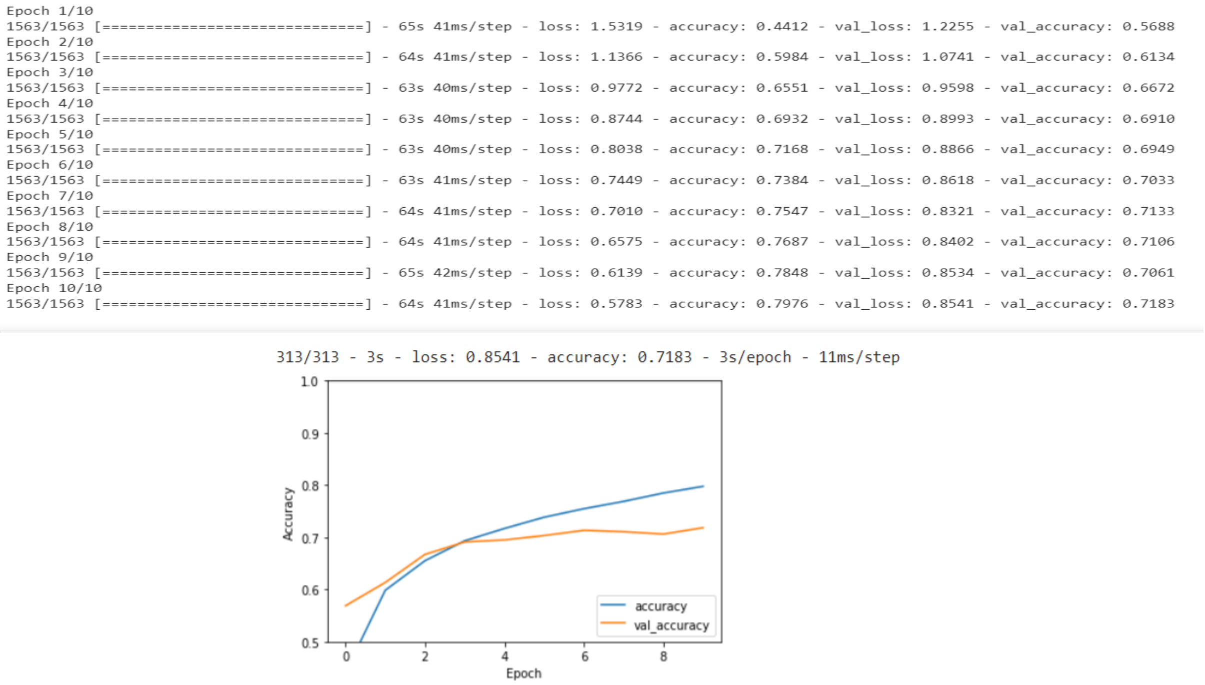
The steps involved in embedding the stego image after extracting from using Deep Learning Algorithm are shown in Figure 4.4.

Evaluation and Validation of the proposed model using the Blockchain with a Deep learning algorithm can be done as:

The evaluation of the proposed model using the CNN-LSTM is done by using the evaluation metrics. The first metric used is accuracy, which gives the correct or the true classification of the entire data set used. The second metric is precision, which gives the proportion of the results indicating the actual inclusion of the given data set. The recall another metric classifies the subset of the classification results detected by the proposed model. The metric F1-score is used to analyse the harmonic mean of recall and the precision. The effectiveness of the proposed model is determined using AUC-ROC curve. Figure 4.5 shows the image classier and effectiveness of the proposed model using the Data Set collected from online images in the form of text, video or audio.



```
Model: "sequential_1"
_________________________________________________________________
 Layer (type)                Output Shape              Param #
=================================================================
 conv2d_3 (Conv2D)           (None, 30, 30, 32)        896

 max_pooling2d_2 (MaxPooling  (None, 15, 15, 32)       0
 2D)

 conv2d_4 (Conv2D)           (None, 13, 13, 64)        18496

 max_pooling2d_3 (MaxPooling  (None, 6, 6, 64)         0
 2D)

 conv2d_5 (Conv2D)           (None, 4, 4, 64)          36928

=================================================================
Total params: 56,320
Trainable params: 56,320
Non-trainable params: 0
_________________________________________________________________
```



```
Epoch 1/10
1563/1563 [==============================] - 65s 41ms/step - loss: 1.5319 - accuracy: 0.4412 - val_loss: 1.2255 - val_accuracy: 0.5688
Epoch 2/10
1563/1563 [==============================] - 64s 41ms/step - loss: 1.1366 - accuracy: 0.5984 - val_loss: 1.0741 - val_accuracy: 0.6134
Epoch 3/10
1563/1563 [==============================] - 63s 40ms/step - loss: 0.9772 - accuracy: 0.6551 - val_loss: 0.9598 - val_accuracy: 0.6672
Epoch 4/10
1563/1563 [==============================] - 63s 40ms/step - loss: 0.8744 - accuracy: 0.6932 - val_loss: 0.8993 - val_accuracy: 0.6910
Epoch 5/10
1563/1563 [==============================] - 63s 40ms/step - loss: 0.8038 - accuracy: 0.7168 - val_loss: 0.8866 - val_accuracy: 0.6949
Epoch 6/10
1563/1563 [==============================] - 63s 41ms/step - loss: 0.7449 - accuracy: 0.7384 - val_loss: 0.8618 - val_accuracy: 0.7033
Epoch 7/10
1563/1563 [==============================] - 64s 41ms/step - loss: 0.7010 - accuracy: 0.7547 - val_loss: 0.8321 - val_accuracy: 0.7133
Epoch 8/10
1563/1563 [==============================] - 64s 41ms/step - loss: 0.6575 - accuracy: 0.7687 - val_loss: 0.8402 - val_accuracy: 0.7106
Epoch 9/10
1563/1563 [==============================] - 65s 42ms/step - loss: 0.6139 - accuracy: 0.7848 - val_loss: 0.8534 - val_accuracy: 0.7061
Epoch 10/10
1563/1563 [==============================] - 64s 41ms/step - loss: 0.5783 - accuracy: 0.7976 - val_loss: 0.8541 - val_accuracy: 0.7183
```

```
313/313 - 3s - loss: 0.8541 - accuracy: 0.7183 - 3s/epoch - 11ms/step
```

Fig. 4.5: Image classifier using the proposed algorithm CNN-LSTM

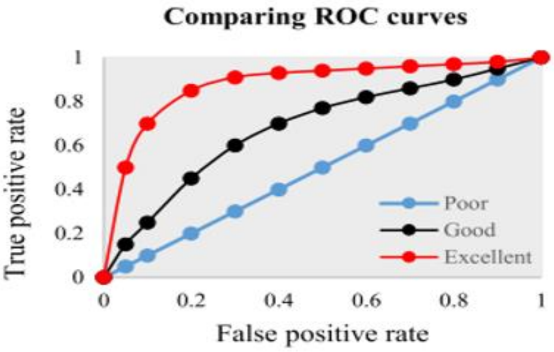


Fig. 4.6: AUC-ROC curve representing for sample dataset

Since most biometric systems are vulnerable to two forms of attack, spoofing and brute-force attacks, the validation stage for the proposed steganography approach can be accomplished by conducting security analysis utilising two types of attack. To test the proposed steganography method's resilience to spoofing, that an attacker will pose as the user and access the node using phishing or a similar technique is assumed.

5. Conclusion

The use of hash-generated value in Blockchain and applying deep learning in the proposed model increases the security level in the steganography. Because the proposed technique makes use of Blockchain technology, network breakdown during emergencies can be avoided. This capability guarantees data availability regardless of whether a network connection fails at any one point. The use of CNN with the Blockchain increase the security level during the transmission of the data or information via network.

References

[1] Zheng, Zibin, Shaoan Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang. "An overview of blockchain technology: Architecture, consensus, and future trends." In 2017 IEEE international congress on big data (BigData congress), pp. 557-564. Ieee, 2017.

[2] Prayagi, Harsh, Tushar Srivastava, Gyanendra Ojha, and Sunil Chaurasia. "Information Hiding in an Image File: Steganography." IJCSIT) International Journal of Computer Science and Information Technologies 3, no. 3 (2012): 4216-4217.

[3] Evans, J. A. S. "Histiaeus and Aristagoras: Notes on the Ionian Revolt." *The American Journal of Philology* 84, no. 2 (1963): 113-128.

[4] Sumathi, C. P., T. Santanam, and G. Umamaheswari. "A study of various steganographic techniques used for information hiding." *arXiv preprint arXiv:1401.5561* (2014).

[5] Agarwal, Namita, Amit Kumar Singh, and Pradeep Kumar Singh. "Survey of robust and imperceptible

watermarking." *Multimedia Tools and Applications* 78, no. 7 (2019): 8603-8633.

[6] Hamamreh, Rushdi A., and Mohammed A. Jamoos. "Hash algorithm for data integrity based on matrix combination." In *The 14th International Arab Conference on Information Technology (ACIT'2013)*. 2014.

[7] Hill, Brenn, Samanyu Chopra, and Paul Valencourt. *Blockchain Quick Reference: A guide to exploring decentralized blockchain application development*. Packt Publishing Ltd, 2018.

[8] Hyla, Tomasz, and Jerzy Pejaś. "Long-term verification of signatures based on a blockchain." *Computers & Electrical Engineering* 81 (2020): 106523.

[9] Mohammed, Mohssen, Muhammad Badruddin Khan, and Eihab Bashier Mohammed Bashier. *Machine learning: algorithms and applications*. Crc Press, 2016.

[10] Laskov, Pavel, Patrick Düssel, Christin Schäfer, and Konrad Rieck. "Learning intrusion detection: supervised or unsupervised?." In *International Conference on Image Analysis and Processing*, pp. 50-57. Springer, Berlin, Heidelberg, 2005.

[11] Shinde, Rucha, Shruti Patil, Ketan Kotecha, Vidyasagar Potdar, Ganeshsree Selvachandran, and Ajith Abraham."Securing AI-based Healthcare Systems using Blockchain Technology: A State-of-the-Art Systematic Literature Review and Future Research Directions." *arXiv preprint arXiv:2206.04793* (2022).

[12] Hameed, Rana Sami, Bin Hj Ahmad Abd Rahim, Mustafa Muneeb Taher, And Siti Salasiah Mokri. "A Literature Review Of Various Steganography Methods." *Journal of Theoretical and Applied Information Technology* 100, no. 5 (2022).

[13]Das, Indrajit, Shalini Singh, Sonali Gupta, Amogh Banerjee, Md Golam Mohiuddin, and Shubham Tiwary. "Design and implementation of secure ATM system using machine learning and crypto–stego methodology." SN Applied Sciences 1, no. 9 (2019): 1-14.

[14] Boughaci, Dalila, and Hanane Douah. "A Variable Neighborhood Search-Based Method with Learning for Image Steganography." In *Sustainable Development and Social Responsibility—Volume 2*, pp. 7-18. Springer, Cham, 2020.

[15] Kadhim, Inas Jawad, Prashan Premaratne, Peter James Vial, and Brendan Halloran. "Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research." *Neurocomputing* 335 (2019): 299-326.

[16] Sahu, Aditya Kumar, and Monalisa Sahu. "Digital image steganography and steganalysis: A journey of the past three decades." *Open Computer Science* 10, no. 1 (2020): 296-342.

[17] Płachta, Mikołaj, Marek Krzemień, Krzysztof Szczypiorski, and Artur Janicki. "Detection of Image Steganography Using Deep Learning and Ensemble Classifiers." *Electronics* 11, no. 10 (2022): 1565.

[18] Ong, Eng-Jon, Syed Sameed Husain, Mikel Bober-Irizar, and Miroslaw Bober. "Deep architectures and ensembles for semantic video classification." *IEEE Transactions on Circuits and Systems for Video Technology* 29, no. 12 (2018): 3568-3582.

[19] Kilincer, Ilhan Firat, Fatih Ertam, and Abdulkadir Sengur. "Machine learning methods for cyber security intrusion detection: Datasets and comparative study." *Computer Networks* 188 (2021): 107840.

[20] Mohsin, Ali H., A. A. Zaidan, B. B. Zaidan, K. I. Mohammed, Osamah Shihab Albahri, Ahmed Shihab Albahri, and M. A. Alsalem. "PSO–Blockchain-based image steganography: towards a new method to secure updating and sharing COVID-19 data in decentralised hospitals intelligence architecture." *Multimedia tools and applications* 80, no. 9 (2021): 14137-14161.

[21] Dey, Somdip. "Securing majority-attack in blockchain using machine learning and algorithmic game theory: A proof of work." In *2018 10th computer science and electronic engineering (CEEC)*, pp. 7-10. IEEE, 2018.

[22] Bhattacharyya, Souvik. "A survey of steganography and steganalysis technique in image, text, audio and video as cover carrier." *Journal of global research in computer science* 2, no. 4 (2011).

[23] Perez, Andres, Valentina Sanguineti, Pietro Morerio, and Vittorio Murino. "Audio-visual model distillation using acoustic images." In *Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision*, pp. 2854-2863. 2020.

[24] Badr, Sherif M., Goada Ismaial, and Ashgan H. Khalil. "A review on steganalysis techniques: from image format point of view." *International Journal of Computer Applications* 102, no. 4 (2014).

[25] Kraetzer, Christian, and Jana Dittmann. "Pros and cons of mel-cepstrum based audio steganalysis using SVM classification." In *International Workshop on Information Hiding*, pp. 359-377. Springer, Berlin, Heidelberg, 2007.

[26] Sarkar, Proton, Sudipta Kumar Ghosal, and Madhulina Sarkar. "Stego-chain: A framework to mine encoded stego-block in a decentralized network." *Journal of King Saud University-Computer and Information Sciences* (2020).

[27] Sundaram, B. Barani, Sudhanshu Maurya, P. Karthika, and P. Vidhya Saraswathi. "Enhanced the Data Hiding in Geometrical image using stego-Crypto techniques with machine laerning." In *2021 6th International Conference on Inventive Computation Technologies (ICICT)*, pp. 1141-1144. IEEE, 2021.

[28] Sun, Yuanyuan, Jiajia Liu, Jiadai Wang, Yurui Cao, and Nei Kato. "When machine learning meets privacy in 6G: A survey." *IEEE Communications Surveys & Tutorials* 22, no. 4 (2020): 2694-2724.

[29] Takaoğlu, Mustafa, Adem Özyavaş, Naim Ajlouni, Ali Alshahrani, and Basil Alkasasbeh. "A Novel and Robust Hybrid Blockchain and Steganography Scheme." *Applied Sciences* 11, no. 22 (2021): 10698.

[30] Madhura, K., and R. Mahalakshmi. "Designing an optimized confidential-data management system using preeminent access-control and block-chain." International Journal of Intelligent Computing and Cybernetics (2022).

[31] Madhura, K., and R. Mahalakshmi. "Survey on Technologies, Benefits, Challenges and Future Suggestions to Improvise the Data Security of Confidential Academic Records in India." In 2021 9th International Conference on Cyber and IT Service Management (CITSM), pp. 1-9. IEEE, 2021.

[32] Manjula, H. M., and S. P. AnandaRaj. "Ayurvedic Diagnosis using Machine Learning Techniques to examine the diseases by extracting the data stored in AyurDataMart." In 2021 3rd International Conference on Advances in Computing, Communication Control and Networking (ICAC3N), pp. 239-244. IEEE, 2021.