IMPROVING THE DIGITAL DATA PROTECTION BY EMBEDDING THE FEATURES OF DEEP LEARNING AND BLOCKCHAIN TECHNOLOGY IN STEGANOGRAPHIC PROCESS

Ms. Ayushi Chaudhary[1*],
GLA University,
ayushichaudhary11@gmail.com

Dr. Ashish Sharma[2],
GLA University,
ashish.sharma@gla.ac.in

Abstract:

With the advancement in technology, the amount of data produced has also been increased. So it is very difficult to maintain the huge quantity of data produced in the form of hard files. Keeping the data in the form of digital form helps in storing and maintaining large quantity of data. But securing data in any form is very challenging. Proper security techniques must be used to store and maintain the data. One of the approach to hide the information present in digital is called steganography. The digital forms of data considered for steganographic process are images, audios and videos. In the current methodology, encryption is used in the steganographic process to hide the information present in the images, audios and videos. The purpose of using encryption is to securely hide the information. But as we are moving forward in technological world, security using encryption is not sufficient. So the proposed method concentrates on improving the security techniques used in steganography by introducing the concept of blockchain technology. With the intention of automating the process of document classification into either image, video or audio; the features of deep learning have been embedded. Overall the proposed work aims to improve the data protection and appending the cognitive capacity into steganography framework. The proposed work is aiming to achieve the highest level of degree by adding the blockchain technology in addition to encryption, where encryption is treated as the first level of security and blockchain storage mechanism is treated as second level of security. Apart from security improvement, document identification is automated through the features of deep learning so that the system will work with less manual intervention.

Keywords: *Digital, Encryption, Steganography, Blockchain Technology, Deep Learning, Data Protection, security.*

DOI Number: 10.48047/NQ.2022.20.20.NQ109271 **NeuroQuantology2022;20(20): 2778-2791**

I. OUTLINE

The outline section of the article introduces the underlying technologies used in the proposed work of steganographic process such as deep learning, encryption and blockchain technology along with steganography technology itself.

The time period “safety” is a very vital which is worried with the secure guarding the gadgets. The object may be files of an organization, valuable metals belonging to someone, cash, and so forth. To at ease those valuable gadgets, human beings depend on hiding them. The term hiding is a common time period used in security for the protection cause. as an example, to secure the treasured metals people use the locker offerings so as to be hidden. in addition, groups depend upon cryptographic strategies to hide the report facts. in addition, if the statistics embedded with pictures and movies had to be hidden method a technique known as steganographic manner might be beneficial. Steganography alludes to records or else a report which desires to be hidden interior a computerized photo, audio-visible or sound report. in the event that a man or woman angle the object the individual in question will don't have any clue about that there are any mystery facts. Thusly, the character won't try to decode the information. The approach steganography is the maximum common way of concealing limited records in an unsuspicious cowl object. The approach is used for concealing, real incidence of correspondence the usage of the approach of implanting mystery messages into harmless looking cover records, like advanced photographs. Deep learning is

eISSN 1303-5150

utilized for data analysis purpose. Blockchain is works as a decentralized network used for secured transaction or storage. If each the technologies namely deep learning, encryption and blockchain are blended collectively in steganography, it can do wonders in security areas.

1.1. Introducing the steganography

Steganography is that the strong point of concealment the actual presence of correspondence with the aid of embedding mystery messages into risk free wanting cowl documents, as modernized pictures. the employment of steganography is gotten on the facet of encoding as a delivered stage of storage steadily or making sure information [1]. Steganalysis has simply were given a big quantity of idea every from law execution and also the media. There square measure different methods of coping with appropriate steganalysis – visual revelation, identification structured upon initial solicitation bits of facts (histogram assessment), twofold estimations systems that use abstraction institutions in footage and better-demand estimations (RS steganalysis), inevitable externally hindered area plans, and new cases, as an example, JPEG likeness steganalysis [2]. Steganography is accustomed conceal more often than not any type of modernized substance, in addition to message, picture, video or sound substance; the information to be hid is hidden inside for all intents and functions some other fairly leading facet substance [3] [38]. The substance to be useable via steganography - summoned stowed text - is systematically encoded before being combined into the risk free superficial cowl textual content document or information move [4]. If not mixed, the mysterious text is commonly pre-arranged in how or every other or an added to boom the difficulty of spotting the perplexing substance [5]. as an example, exploitation indiscernible ink to hide mystery messages regardless agreeable messages; concealment reviews recorded on exposure - which is probably absolutely similarly little or no as one millimetre in expansiveness - on or inside veritable superficial correspondence; or even by means of exploitation multiplayer play conditions to proportion records [6]. In present day stepped forward steganography, data is preliminary encoded or higgledy-piggledy in in an exceptional way and a short time later planted, exploitation partner degree uncommon estimation, into facts it's essential for a particular file association, for example, a JPEG photo, sound or video report [7]. The close message is embedded into ordinary records archives in numerous methods in which. One method is to cover data in bits that cope with a similar concealing pixels reiterated in development in a photograph file. by means of applying the combined information to the modern overabundance records in some unnoticeable approach, the result is {a photo} report that seems to be unclear from the foremost picture although that has "noise" times of traditional, decoded statistics. The demonstration of adding a watermark - a logo or alternative one-of-a-kind records disguised in amalgamated media or alternative substance reports - is one everyday use of steganography. Watermarking may be a technique frequently utilized by 8db290b6e1544acaffefb5f58daa9d83 distributers to apprehend the wellspring of media data which can be determined being shared whilst no longer assent [8]. whereas their square degree a large scope of vocations of steganography, as well as embedding fragile records into archive kinds, conceivably the foremost fantastic method is to introduce a textual content report into an image record. proper once this can be finished, everyone seeing the photograph record shouldn't have the selection to take a look at a differentiation among the primary image archive and additionally the encoded file; this can be refined via looking after the message with much less huge snack within the records report. This collaboration is completed in reality or with the use of a steganography appliance. Steganography paintings is used to cover a mysterious message in any media like message, image, sound and video. these rectangular measures are used in numerous calculations used for concealing the info. one in all the best and most up to date approaches is Least Crucial Bit (LSB). excessive restriction image steganography utilizing Least Critical Bit (LSB) alternative very impaires visible nature of the stego image. Likewise, the majority of steganographic plans ponder direct implanting of mystery message regardless of its safety concerns over open channel transmission. To clear up this issue, we have got conferred a totally precise stego-key coordinated LSB alternative plot that gives high implanting restrict further as robust against stego photograph injury. there

eISSN 1303-5150

are several photo steganography packages captivated with LSB square degree conferred. LSB steganography relies upon on the method that substitute at the least one in all of the final 1-4 items of cover photograph's pixels is not recognizable by means of human visual framework, but a few measurable assessments can also decide that they're supplanted in fitting areas. various structures square measure projected to regulate main conditions, however basics of LSB steganography square measure nitty gritty in. one in all of the strategies offers three substitution applicants and additionally the only that has the closest fee of the supply constituent, called best constituent, is used for substitution. A later LSB method gives a way, referred to as bit reversal, to similarly work at the PSNR (pinnacle sign commotion proportion). at some point of this reversal process, bound LSBs of the quilt photograph's pixel's square degree changed inside the event that they fit with a specific instance [9].

Steganography programming is utilized to play out a collection of capacities to conceal statistics, remembering encoding the information for request to set it as much as behind the internal another record, monitoring what pieces of the quilt textual content record incorporate stowed away facts, scrambling the data to be blanketed up and extricating stowed away statistics by way of its deliberate beneficiary. There are restrictive just as open supply and other allowed to-utilize applications accessible for doing steganography. Open Stego is an open source steganography application; exceptional initiatives can be portrayed with the aid of the styles of records that may be hid just as what types of facts that statistics may be concealed inside. some net based steganography programming devices contain Xiao Steganography, used to hide secret documents in BMP pictures or WAV facts; image Steganography, a JavaScript tool that conceals pictures interior different photo files; and Crypture, an order on line equipment that is utilized to perform steganography [1] [38].

1.2. Introducing deep learning in steganography

The purpose of using deep learning in steganography is to identify the type of input file. The proposed model can accept all the categories of multimedia files such as image, audio and video. The existing steganographic applications work for one category of media file either audio or video or image. Existing applications are designed to be dependent of input file type. So they can identify only either audio or video or image. Using deep learning it is possible accept all categories of multimedia files such as image, audio and video. The essential concept worried with inside the proposed approach is to automate the procedure of figuring out the enter class out of 3 types; photo, audio, or video. The principal goal is to expand a wise device on the way to paintings without or much less guide intervention. For this purpose, the deep mastering set of rules idea is proposed in order that the framework can paintings for all 3 classes of inputs; audio, video, and photo. The current structures paintings simplest on one form of enter and are depending on the form of enter. This method that the prevailing structures are designed particularly to the enter kind in one of these manner that they are able to procedure both simplest photo or audio or video. Not all of the 3 classes. The proposed device is embedded with synthetic intelligence generation wherein the implemented deep mastering set of rules will pick out and classify as both photo or audio or video. The recognized and categorised enter could be despatched to the procedure of steganography. Three unique deep mastering algorithms are used for evaluation purpose. The end result precision of CNN, RNN and LSTM are compared [30] [31] [36] [40].

1.3. Introducing encryption in steganography

Encryption [39] is employed for concealment the essential records to buy it from change of state or stealing. Its miles proven in things within which articulation is mounted among activities over AN insecure medium which can be while not troubles eavesdropped delineated in recognize one. coding frameworks area unit wont to regulate adventure story messages into marked-up formats to AN unauthorized man or girl while decipherment frameworks area unit wont to decrypt the disorganized message via somebody who`s crime to learn this. A scientific discipline hash feature is AN example of AN integrity take a glance at feature. It`s miles a relation wont to acknowledge tiny quantities of data which can be wont to notably become aware of immense virtual objects. There are a unit specific hash values for splendid objects; thence, it is not computationally potential to possess AN object with the equal hash fee as that of an up-to-date object. Hash competencies perform a yardstick for the verification of the integrity of a message when transmission [10].

eISSN 1303-5150

Figure 1: General representation of encryption method

Information safety consists of activity mystery pictures, text, audio or video documents inner each special documents which will be wont to keep the choice of the sport statistics from being theft through means of technique of the 1/3 party. secret writing algorithms play essential roles to protect actual statistics from unauthorized access [11] [32] [33].

1.4. Introducing blockchain in steganography

In the prevailing steganographic device, the very best stage of safety is supplied via the encryption technique. In the proposed method, encryption is handled because the 1st stage of safety and as a further and 2nd stage of safety, blockchain era has been introduced. In steganography, the facts are transmitted with the aid of using hiding with inside the images, audio, or video, without converting any patterns [39] [40]. The mystery facts are hidden with inside the cowl photo and transmitted via the network. The hidden facts on the duvet web page isn't major to the attackers. The hidden facts with inside the photo is referred to as the stego photo. However, the primary apprehension is in integrating the facts with inside the cowl web page to be able to guard it from intruders. To cope with the safety of facts, the Blockchain framework may be implemented for reworking facts in a greater green way. But Blockchain era additionally faces majority assaults including double-spending. In a decentralized device like Blockchain, the majority of assaults are performed with the aid of using a collection of humans or businesses that paintings collectively to capture manage of the ledger and take advantage of it. To triumph over those assaults gadget mastering set of rules may be used and keep away from the bulk of assaults that can take area with the aid of using the usage of Blockchain technologies [34] [35].

II. BACKGROUND WORK

The section explains about the works carried related to steganographic process in terms of deep learning, encryption and blockchain technology. Also a deep survey on the existing underlying technologies used in the steganographic process.

In internet technology, security is turning into a significant issue within the world as internet shoppers are evolving quickly over time. If consumer has to use a social application to transfer its own knowledge to a different web consumer, then the technologist will override these social applications and hack all the individual knowledge regarding the net consumer. Therefore, a security element is required to guard all individual knowledge from unauthorized persons. a widely known privacy-protected data processing technique is organization. Over time, the employment of steganography and its fields has distended. within the current digitisation amount, digital steganography has become a replacement device for subtly activity knowledge. Scripts, advanced image process, digital audio, and computerised video became host protests against info activity [36] [40].

Since the exercise of steganography is one in all disguising data without elevating suspicion, the phrase steganography actually interprets as "Covered writing" and has Greek origins. It includes an extensive type of covert communique techniques that masks the mere life of the message. The term "steganography" at the start seemed in 1499 with inside the book Steganographic through Johannes Trithemius [12]. Despite the title`s specific reference, the book targeted totally on esoteric subjects and cryptography procedures. In the 5th century BC, while human beings used to write down messages on wax-lined tablets, Herodotus defined the earliest regarded use of steganography. The message remained hidden in the back of the wax layer on this manner. Herodotus additionally recorded that Histiaeus, the ruler of Miletus below Darius I of Persia, wanted to talk together along with his Greek son-in-law [13]. In order to perform this, had tattooed the message onto the slave's scalp after shaving the cranium of one in all his maximum reliable slaves. He despatched the slave with the hid message while his hair had grown back, and while the slave arrived on

eISSN 1303-5150

the vacation spot as soon as more, he shaved his head and retrieved the message [40].

Steganography is generally hired these days to shield personal facts. As an end result of the powerful increase in call for virtual communique, the net has completely advanced into the maximum mighty and short approach of virtual communique. Simultaneously, as facts at the net has evolved right into a goal for copyright violations, hacking, and eavesdropping, the call for stable and sincere communique has grown. In steganography the communique is achieved as, the recipient gets the stego item x(m), which become created through the sender the usage of a cowl item x to embed a mystery message m. To growth security, the sender would possibly use an optionally available key (k). The recipient makes use of the corresponding key to extract the item's hid data after it's been communicated the usage of stego.

The author named Elisa et.al.[14] of their look at gives a framework for a decentralized e-authorities peer-to-peer (p2p) gadget primarily based totally on Blockchain generation which could shield information protection and privatizes at the same time as additionally improving public region trust. Blockchain generation is used to make sure excessive protection and privatizes via way of means of keeping decentralized structures in which transactions aren't beneath the third-birthday birthday celebration control. To keep away from cyber-assault consisting of malware, denial of carrier (DoS), and dispensed denial of carrier attacks (DDoS) because of the failure with inside the centralized control and gadget validation, Blockchain generation is proposed. The creator proposes the prototype with theoretical guide and a quantitative evaluation of privatizes and protection.

An author called Liu, Si et.al. [15] of their look at explores the functions of Blockchain that gain steganography. To guard the privatizes of Blockchain transaction information, this look at first separates every transaction into parts: touchy information and primary information, after which encrypts and hides the touchy information in HEVC video. The outcomes of the experiments monitor that this HEVC video steganography set of rules correctly will increase the privatizes information embedding potential at the same time as keeping excessive visible quality.

One more author named Mustafa Muneeb Taher et.al. proposed the Robustness and normalized cross-correlation (NCC) are key additives of steganography [16]. In this context, Digital steganography has gone through good sized studies advancements. Meanwhile, the blanketed and privacy-maintaining communique thru the WWW (World Wide Web) has been seriously threatened via way of means of such unfettered get entry to one of these big quantity of statistics and Punidha et al. applied the integer wavelet remodel and the famous wavelet method to hide messages. The look at defines, Steganography is a smart records hiding era in which the name of the game records is implanted in a cowl media in one of these manner that the aim of each cryptography and steganography is to keep and store the name of the game message and steady it from hackers or attackers. Authors added the term "computational intricacy" in steganographic strategies correlates to the accuracy of the embedding algorithms, and a few system trying to examine strategies name for an excessive stage of computational skill. The reviewers use the integer wavelet, remodel idea to loss of standardization switch audio speech signals.

Another author called Indrajit et al. [17] proposed, addressing a couple of assault kinds is now an important precondition. The essential definition of Automated teller system (ATMs) are the gadgets which are maximum often used in recent times for monetary transactions, and PINs are normally utilized in those gadgets. According to PINs which might be used for identification documents, are easy but is despite the fact that powerless with inside the face of the diverse forms of use an assault (Phishing assault, spoofing assault, Sniffing etc.). The researchers have referred to that safety of the only of vein authentication device`s statistics change has finally been the situation of studies via way of means of diverse researchers throughout the globe. The aim is likewise approximately a biometrics authentication device and a blended method of cryptography and steganography are proposed for the switch of banking transaction statistics reliably thru ATMs.

The author named Boughaci D et al. has proposed a famous set of rules referred to as unmarried bit LSB [18] substitute lets in for the substitute of an unmarried bit from a photo pixel in every service pixel. The researchers additionally say that, common victim's lifestyles are now being threatened via way of means of the increasing, awful incidents of assaults on personal statistics, Park K R et al. have supplied with inside the context of capital transactions and banking-associated sports at computerized teller machines (ATMs) approximately Finger vein identity via way of means of combining international and neighbourhood functions primarily based totally on SVM [18].

Another author called Inas et al. [19] have researched with inside the discipline of

eISSN 1303-5150

cryptography, which offers with diverse techniques of records encryption, became most of the maximum thrilling ones with inside the records control discipline. Its aim is to encrypt mystery statistics the usage of special tactics after which remodel it right into a written form. H. Wang et al. have proposed that any steganographic device must have 3 matters specifically, imperceptibility, safety, Payload, Robustness and the functionality of hiding statistics, a few applications, such as Smart stegano transportable gadgets encrypting multisensory biometric statistics, securing IP (Intellectual Properties), and encoding non-public information in clever identification cards.

One more author named A.K. Sahu et al. [20] additionally said that many metrics are implemented to assess the diverse elements of steganographic strategies. According to famous measures have covered 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 shows that structures having suitable mastering schemes have powerful photo steganography structures, and research can be cantered on deep trying to examine schemes for more photo steganography device applications. A. Miri et al. exact the photo adaption steganography in which it has relied upon remodel area thru genetic strategies.

Digital photo steganalysis recognition algorithms on inter-pixel dependencies, this is the inspiration of herbal images. While virtual audio analysis algorithms are primarily based quite truly on the functional components of the file, which include the degree of distortion of the audio character and its excessive records. Steganalysis algorithms for virtual video cause “spatial and temporal redundancy on the inside, symptoms and symptoms on the inside of character frames and on the inter body level” [21].

The reason behind audio steganalysis is to discover any alternative in the sign due to record embedding. There are key domain names for embedding records, each using a spatial or occasionally 'temporal' or 'temporal' location, and which in most cases is transmitted by translating the least significant bit (LSB) of the record pattern on the internal side of the audio. file, or the inner side to redecorate the place thanks to the improvement of the remarkable parameters of the character. Additionally, audio steganalysis is classified primarily entirely based on layout into steganalysis strategies for compressed codecs, which include MP3 and AAC, and steganalysis strategies for uncompressed codecs [22]. Regarding compressed codecs, Jin et al. [23] proposed a causal steganalysis approach for MP3Stego steganography detection. The authors determined that MP3Stego changes the quantized altered discrete cosine redecorate coefficients of the QMDCT for the duration of the compression, which affects the correlations between adjacent QMDCTs of the audio cover. Markov capabilities are therefore extracted from the cover and stego sound to provide a rationale for the QMDCT correlations. These features are then crossed using pre-processing steps to select the most pleasing features for training the SVM classifier. According to the experiments, the proposed approach achieves excessive detection accuracy on the inner side in the case of low insertion speed.

Another steganalytic approach for Mp3 is proposed by Wang et al. [24] where the QMDCT MP3 coefficient matrix is calculated to extract steganalysis capabilities. A rich way of skipping skip filtering is ultimately done to increase sensitivity in their approach in opposition to noise symptoms and symptoms. The authors argued that the unreal 1 coefficient of QMDCT has implications for the conversion of 1 Huffman codeword on the inside. For this reason, they approved the correlation degree module to discover any viable change of the inner side of the QMDCT coefficient matrix in points, 2 × 2 by blocks, and four × four by blocks, separately. An empirical threshold is made to reduce the dimensions of abilities and choose the most pleasant one. For the task of elegance, the file classifier [25] is ultimately the expert.

For uncompressed codecs, it consists of strategies: collaborative approach and non-collaborative approach. In the primary approach, the strategy depends on the evaluation of some expected covering element and stego element. There are many strategies to estimate a quilt that includes demolition, which is primarily based on a very real basis of lining, re-inserting, and more. However, stego signature estimation for calibration is also viable, it is kilometers performed using Ghasemzadeh et al. [26], where the authors proposed a well-known steganalysis approach primarily based entirely on calibration. In their approach, the re-embedding approach used to embed a character with a random message ended up. The energy abilities were extracted, with each sign and re-inserted sign divided into many parts and the energy for each one calculated. The energy of each chew is then subtracted from the sign and its reinserted counterpart. Finally, without delay, the statistical homes of the energy capabilities, which include mean, skewness, standard deviation, and kurtosis, are decided upon to educate the SVM

eISSN 1303-5150

classifier. Their approach was evaluated using an extensive method of numerous steganographic strategies. Experimental results confirmed its effectiveness in detecting the inner side of concentrated and known times.

On the other hand, the non-cooperative approach extracts its own capabilities far from the sound character normal with the embedding function. Han et al. [27] promoted a linear prediction approach where LP linear prediction capabilities are extracted from a segmented audio file. Based on the experiments, the authors concluded that the LP can greatly distinguish between the blanket and the stego. Therefore, the capabilities of LP coefficients, LP residuals, LP spectrum and LP cepstral coefficients are extracted from time space and frequency space. The SVM classifier is an expert that is primarily based on the extracted capabilities from mask and stego features and features. A large vogue of experiments is complemented by numerous ratio embeddings and are explored in opposition to remarkable steganographic strategies. The results demonstrated the effectiveness of the proposed strategies in evaluation with known and current steganalysis strategies, where the accuracy above 96% is completed.

Recently, deep reading has generated more interest and completed advanced implications within the field of steganalysis. Lin et al [28] proposed an advanced approach that is primarily completely based on CNN to discover the inner side of audio steganalysis and place time. First, a high-pass filter layer is used to extract the residual character from the input audio. Then, hierarchical representations of the enter are obtained using six numerous layer gadgets, with the primary set consisting only of the activation of the primary convolutional layer and the final gadgets containing the convolutional layer and pooling layer. A nonlinear activation is performed after each convolution operation. By giving up these layers, the audio character is converted to 215-abilities. For steganography discovery, the extracted capabilities are fed into a binary classifier, which consists of a Softmax layer and a fully related layer. This approach has been shown to be effective in detecting remarkable levels of entrainment [29].

Ren et al. [30] proposed a well-known steganalysis approach where ResNet is performed for feature extraction. The spectrogram of the audio feature is finally used as input to a neural network known as a spectrogram deep residual network (S-ResNet). Figure 9 illustrates how a spectrogram can form the energy facts of many frequency bands over the years, in addition to which valuable time-frequency facts are included on the inside of the audio signature.

III. EXISTING MODEL

The proposed studies paintings method steps are indexed below:

1. Collect the records set like pics and videos.
2. Randomly pick out the enter no matter it layout both a picture or a video.
3. Covert the enter into its binary equivalent.
4. Determine LSB of each pixel of safety portrait.
5. Extract the name of the game data and carry out encryption on it.
6. Using the encryption key write the stegano picture for every random enter.

The proposed paintings method is depicted with inside the diagram below in figure 2:

eISSN 1303-5150

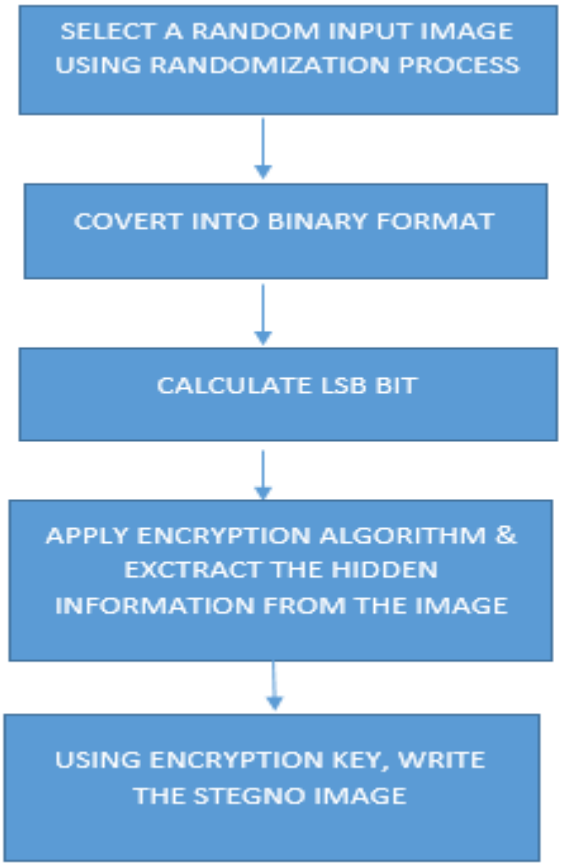


Figure 2: Steps involved in the existing model of steganography

IV. PROPOSED WORK

The basic concept that the proposed approach deals with is the automation of the input class determination system from 3 types; photo, sound or video. The most important goal is to extend the wise machine to be able to paint without or much less wizard intervention. To this end, a deep understanding of the ruleset idea is designed so that the framework can paint for all 3 classes of inputs; audio, video and photos. Current painting structures are best suited to one type of input and are dependent on the type of input. This approach is that the current structures are designed especially for the input type in any way that they could systematize both the most convenient photo and audio or video. Not all 3 classes. The designed machine is equipped with synthetic intelligence generation in which the implemented deep knowledge acquisition of rule set selects and classifies as photo or audio or video. The recognized and categorized record could be sent to a steganography system. Three specific in-depth algorithms are used for evaluation purposes. The final accuracy of CNN, RNN and LSTM results are compared.

eISSN 1303-5150

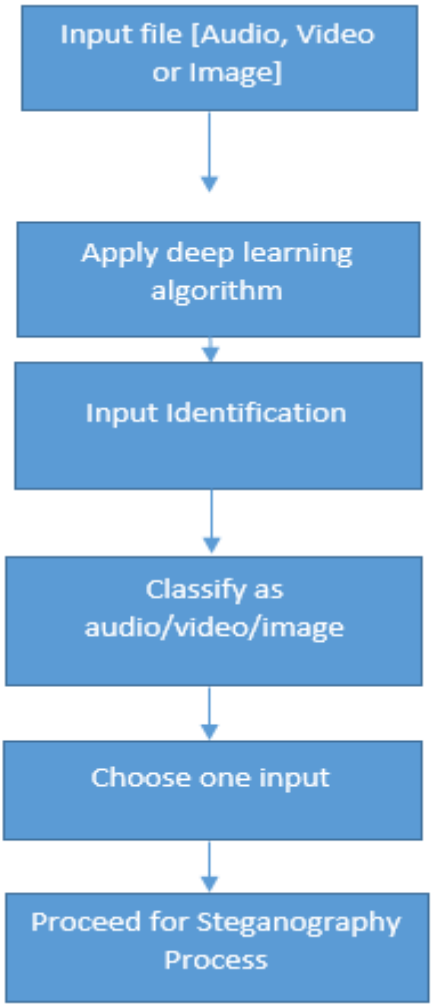


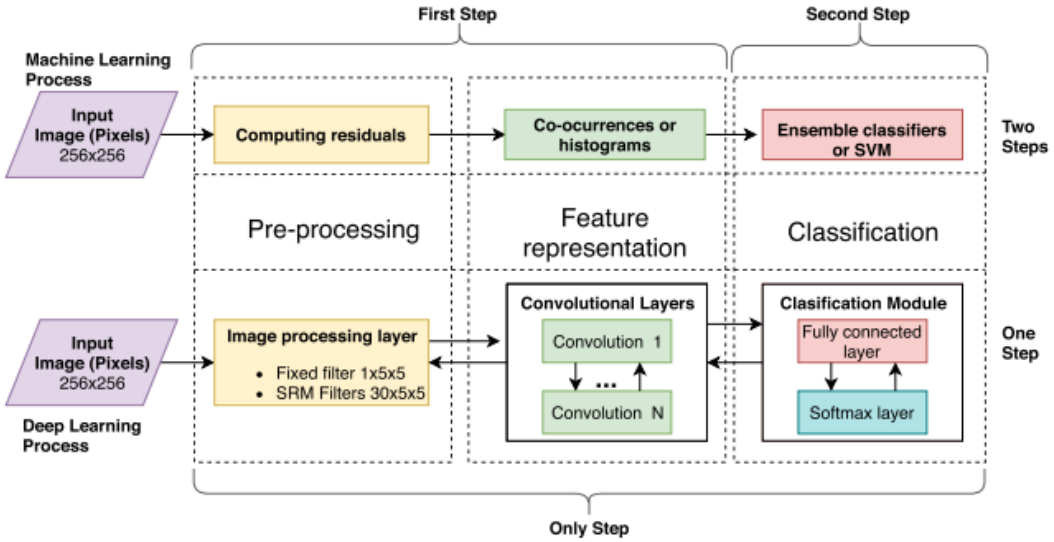
Figure 3: Steps involved in the proposed model of steganography

With the discovery of 6G generation, big records are communicated over public channels. This results in big safety demanding situations at the facts shared at the network. Hence good sized to soundly transmit the facts which may be with inside the shape of images, audio, or video need to be provided. There exist many safety techniques which includes encryption, watermarking, steganography, and plenty of extra. In the encryption approach, the total facts are encoded via way of means of the usage of the name of the game keys, and the hidden facts is decoded on the receiver quit the usage of the name of the game keys. Encrypting the facts can be insecure due to the fact attackers can without problems hint the facts this is hidden facts. To conquer this disadvantage, the facts is hidden with a few images, video, or audio the usage of the idea known as steganography. In steganography, the facts are transmitted via way of means of hiding within side the images, audio, or video, without converting any patterns. The mystery facts are hidden within side the cowl photograph and transmitted thru the network. The hidden facts on the quilt web page isn't great to the attackers. The hidden facts within side the cowl photograph is known as the stego photograph. However, the principle apprehension is in integrating the facts within side the cowl web page if you want to guard it from intruders. To cope with the safety of facts, the Blockchain framework may be carried out for reworking facts in an extra green way. But Blockchain generation additionally faces majority assaults which includes double-spending. In a decentralized machine like Blockchain, the majority of assaults are performed via way of means of a set of humans or companies that paintings collectively to capture manage of the ledger and benefit from it. To conquer those assaults device studying set of rules may be used and keep away from the bulk of assaults that can take location via way of means of the usage of Blockchain technologies.

eISSN 1303-5150

V. EXPERIMENTAL RESULTS

1. Figure 4 represents steganographic process of images using deep learning.



2. Figure 5 depicts the flow Diagram of Image Steganography Using CNN

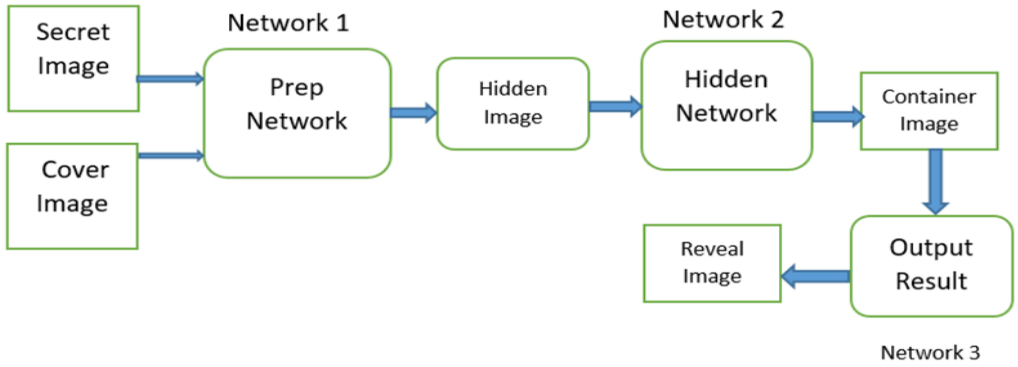


Image steganography is the main content of encryption. The sender hides the secret message in the mask image. and get a pocket photo called a stego or Hidden Photo. Then, the transfer of the secret information to the public channel is done by transferring the stego image. Then, the receiving side of the transmission can reveal the secret information.

3. Training Phase and Testing Phase using CNN

Steganalysis follows a common pattern:

It starts by extracting some features from the input, then analysing and classifying those features to detect steganography. There are two types of features: technical features and deep features. In this technique, known characters such as statistical characters are manually extracted. The deep feature is not well defined whether it is automatically generated by a neural network or an automatic depth masker. After feature extraction, classification is performed to distinguish between half cover and stego. Planning can be done in three different ways: first, using rigorous statistical methods to determine the existence of confidential information. In the second stage, it goes through some models and machine learning to train and learn the insurance support model; therefore, it can distinguish between the cover and the stego-media during the test. The last method is the use of neural networks.

eISSN 1303-5150

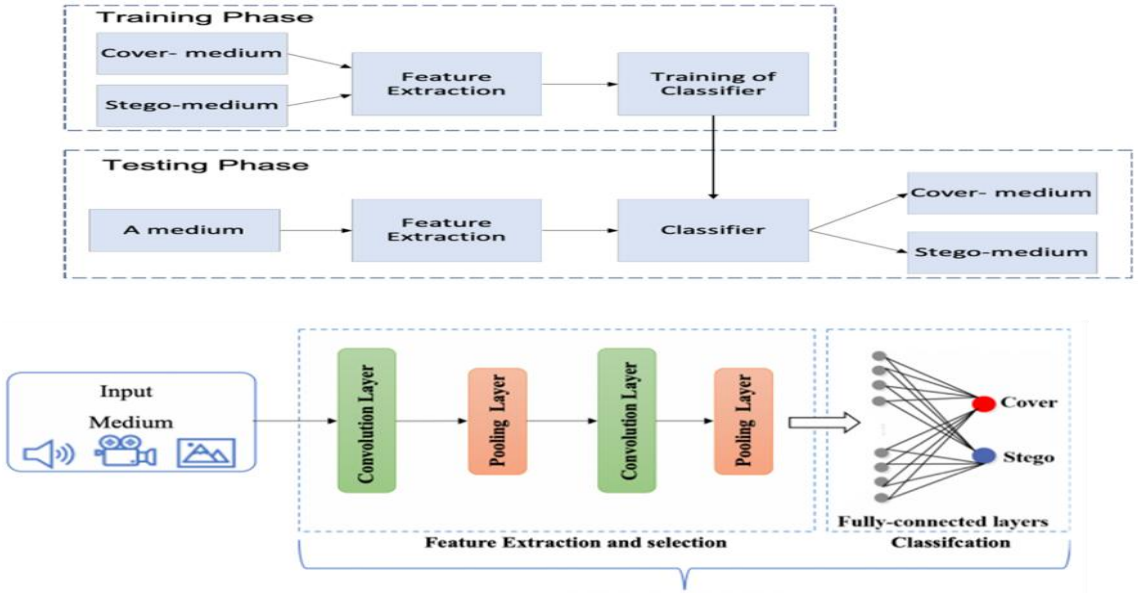


Figure 6: Training Phase and Testing Phase using CNN

4. Evaluation Matrices

Confusion matrix is used as one of the evaluation matrices

- True-Positive (TP) are actual cases correctly identified by the algorithms.
- True-Negative (TN) are undesirable cases correctly identified by algorithms
- False-Positive (FP) are undesirable cases where the algorithms classify erroneously as positive.
- False Negative (FN) are positive cases where different algorithms incorrectly classify them as negative

Actual class \ Predicted class	P	N
P	True Positives (TP)	False Negatives (FN)
N	False Positives (FP)	True Negatives (TN)

The matrix based performance measures are analysed for different machine learning algorithms in this proposed model are given by:

a. Accuracy: The accuracy measure is applied to recognize correctly predicted values among all the other values in a data set $Accuracy=(TP+TN)/(TP+TN+FP+FN)$
b. F1 Score: Is taken as the harmonic mean of precision and sensitivity. In F1 score True Negative values are not considered: $F1\ score= (2 \text{ X } TP)/ (2\ X\ TP+FN+FP)$
c. Precision: This predicts the true diseased patient from the total number of data set taken for analysis: Precision=TP/(TP+FP)
d. Sensitivity: is used for categorizing the input images from the given sample datasets: Sensitivity = Recall = $True\ positive\ rate$=TP/(TP+FN)
e. Specificity: Is used for predicting the patients who are not having the disease from the patient dataset. $Specificity$=TN/(TN+FP)

eISSN 1303-5150

VI. CONCLUSION

Steganography can be used to hide almost any form of virtual content material, which includes textual content, photographs, video or audio content; the records to be hidden may be hidden in almost another form of virtual content material. Content material to be hidden using steganography, referred to as hidden textual content, is often encrypted before it is integrated into the seemingly innocuous textual content of a document or record stream. If hidden textual content isn't always encrypted, it's miles generally processed in several ways to make it extremely difficult to figure out the name of the game's content material. The most important objective of the steganography technique is to cover the lifestyle of the name of the game. Massive surveillance operations have shown that even if the content is unknown, the way in which records are routinely communicated can also lead to leakages from privatizations. Therefore, steganography is essential for personal communication. Steganographic strategies can be used in many areas such as watermarking, copyright protection, and secret transmission. The sender typically uses a set of steganographic rules to mask the name of the game message on the cover side, with the outer detectors unchanged. The most important attempt in steganography is to reduce the interference inside the cover side photo while the secret is inserted, and at the same time to allow recovery of the name of the game message, then the steganography photo, which is known as stego, has changed to transmitted in public channels. In turn, the receiver obtains the stego and uses the decryption rule set and shared key to extract the name of the game message. In state-of-the-art virtual steganography, records are first encrypted or obfuscated in several different ways before they are embedded in records, this is part of a particular document format, which includes a photo, audio or video JPEG document, using a unique set of rules. In many ways, the name of the game message can be inserted into regular log files. One technique is to hide records in bits that make up identical color pixels in a row of a photographic document. By subtly applying encrypted records to redundant records, the end result can be a photographic document that looks just like an authentic photograph, but contains the "noise" styles of regular, unencrypted records. With the rapid improvement of deep learning, photo editing in steganography will become much easier and automatic. The addition of blockchain technology provides an additional layer of security in addition to encryption. In the proposed work, encryption is considered as the first level of security for hiding data, and this hidden data will be processed through the blockchain network to make the data immutable to changes and theft.

VII. REFERENCES

[1] K. Thangadurai and G. Sudha Devi, "An analysis of LSB based image steganography techniques," 2014 International Conference on Computer Communication and Informatics, 2014, pp. 1-4, doi: 10.1109/ICCCI.2014.6921751.

[2] çataltaş, Özcan & Tutuncu, Kemal. (2017). Improvement of LSB Based Image Steganography. 5. 1-5.

[3] K Thangadurai PG, Sudha Devi, "Evaluation of LSB Based Image Steganography Technique for various File Formats", International Journal of Computational Intelligence and Informatics, Vol. 3: No. 3, October - December 2013.

[4] MUSTAFA CEM KASAPBAS¸ WISAM ELMASRY, "New LSB-based colour image steganography method to enhance the efficiency in payload capacity, security and integrity check", Sådhanå (2018) 43:68, Indian Academy of Sciences, https://doi.org/10.1007/s12046-018-0848-4.

[5] Dr. Amarendra K, Venkata Naresh Mandhala, B.Chetan gupta, G.Geetha Sudheshna, V.Venkata Anusha, "Image Steganography Using LSB", INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VOLUME 8, ISSUE 12, DECEMBER 2019 ISSN 2277-8616.

[6] Arun Kumar Singh, Juhi Singh, Dr. Harsh Vikram Singh, "Steganography in Images Using LSB Technique", International Journal of Latest Trends in Engineering and Technology (IJLTET).

[7] Manjinder Kaur, Varinder Kaur Attri, "Implementation of Steganographic Method based on Interpolation and LSB Substitution of Digital Images with Watermarking and Visual Cryptography", International Journal of Computer Applications (0975 – 8887) Volume 121 – No.21, July 2015.

[8] Amit Kumar Agrahari, Mayank Sheth, N. Praveen, "Comprehensive Survey on Image Stegnography Using LSB with AES", International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 8 (2018) pp. 5841-5844 © Research India Publications. http://www.ripublication.com.

eISSN 1303-5150

[9] TANMAY SINHA ROY, "IMAGE STEGANOGRAPHY USING LSB BIT-PLANE SUBSTITUTION", International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056 Volume: 03 Issue: 12 | Dec -2016, p-ISSN: 2395-0072.

[10] Mustafa Sabah Taha et al, 2nd International Conference on Sustainable Engineering Techniques (ICSET 2019), IOP Conf. Series: Materials Science and Engineering 518 (2019) 052003, IOP Publishing, doi:10.1088/1757-899X/518/5/052003.

[11] Ambika, Rajkumar L. Biradar & Vishwanath Burkpalli (2019) Encryption-based steganography of images by multiobjective whale optimal pixel selection, International Journal of Computers and Applications, DOI: 10.1080/1206212X.2019.1692442.

[12] 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.

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

[14] Elisa, Noe, Longzhi Yang, Fei Chao, and Yi Cao. "A framework of blockchain-based secure and privacy-preserving E-government system." Wireless networks (2018): 1-11.

[15] Liu, Si, Yunxia Liu, Cong Feng, Hongguo Zhao, and Yu Huang. "Blockchain privacy data protection method based on HEVC video steganography." In 2020 3rd International Conference on Smart BlockChain (SmartBlock), pp. 1-6. IEEE, 2020.

[16] 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).

[17] 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.

[18] 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.

[19] 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.

[20] 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.

[21] Serrano, J. Steganalysis: A Study on the Effectiveness of Steganalysis Tools. Ph.D. Thesis, Utica College, Utica, NY, USA, 2019. [Google Scholar]

[22] Tabares-Soto, R.; Ramos-Pollán, R.; Isaza, G.; Orozco-Arias, S.; Ortíz, M.A.B.; Arteaga, H.B.A.; Rubio, A.M.; Grisales, J.A.A. Digital media steganalysis. In Digital Media Steganography; Elsevier: Amsterdam, The Netherlands, 2020; pp. 259–293. [Google Scholar]

[23] Jin, C.; Wang, R.; Yan, D. Steganalysis of MP3Stego with low embedding-rate using Markov feature. Multimed. Tools Appl. 2017, 76, 6143–6158. [Google Scholar] [CrossRef]

[24] Wang, Y.; Yi, X.; Zhao, X. MP3 steganalysis based on joint point-wise and block-wise correlations. Inf. Sci. 2020, 512, 1118–1133. [Google Scholar] [CrossRef]

[25] Kodovsky, J.; Fridrich, J.; Holub, V. Ensemble classifiers for steganalysis of digital media. IEEE Trans. Inf. Forensics Secur. 2011, 7, 432–444. [Google Scholar] [CrossRef][Green Version]

[26] Ghasemzadeh, H.; Arjmandi, M.K. Universal audio steganalysis based on calibration and reversed frequency resolution of human auditory system. IET Signal Process. 2017, 11, 916–922. [Google Scholar] [CrossRef][Green Version]

[27] Ghasemzadeh, H.; Arjmandi, M.K. Universal audio steganalysis based on calibration and reversed frequency resolution of human auditory system. IET Signal Process. 2017, 11, 916–922. [Google Scholar] [CrossRef][Green Version]

[28] Han, C.; Xue, R.; Zhang, R.; Wang, X. A new audio steganalysis method based on linear prediction. Multimed. Tools Appl. 2018, 77, 15431–15455. [Google Scholar] [CrossRef]

[29] Lin, Y.; Wang, R.; Yan, D.; Dong, L.; Zhang, X. Audio steganalysis with improved convolutional neural network. In Proceedings of the ACM Workshop on Information Hiding and Multimedia Security, Paris, France, 3–5 July 2019; pp. 210–215. [Google Scholar]

[30] Madhura, K. and Mahalakshmi, R. (2022), "Designing an optimized confidential-data management system using preeminent access-control and block-chain", International Journal of Intelligent Computing and Cybernetics, Vol. ahead-of-print No. ahead-of-print. https://doi.org/10.1108/IJICC-12-2021-0295.

[31] Madhura, K. and Mahalakshmi, R. (2022), "APPLYING CRYPTOGRAPHY AND BLOCK CHAIN TECHNOLOGY TO SECURE AN ORGANIZATION'S CONFIDENTIAL DOCUMENTS", KOREA REVIEW OF INTERNATIONAL STUDIES, Vol. 15, Spl. Issue 02, pp. 96-110.

[32] Madhura, K. and Mahalakshmi, R. (2021), " Securing the organization documents in content management system with two levels of security using encryption and block chain technology", Design Engineering, ISSN: 0011-9342, Issue: 7, pp. 14025- 14039.

[33] Madhura, K. and Mahalakshmi, R. (2018), " An Approach for Securing Organizational Data using Block-chain and Cryptography", Solid State Technology, Volume: 63 Issue: 2s, pp. 2429-2441.

[34] Madhura, K., Mahalakshmi, R, "Usage of block chain in real estate business for transparency and improved security", Proceedings - IEEE International Conference on Advances in Computing, Communication and Applied Informatics, ACCAI 2022, 2022.

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

[36] Madhura, K., Mahalakshmi, R, "END2END UNSTRUCTURED DATA PROCESSING, CONFIDENTIAL DATA STRUCTURING & STORAGE USING IMAGE PROCESSING, NLP, MACHINE LEARNING, AND BLOCKCHAIN", Journal of Theoretical and Applied Information Technology, 2022, 100(13), pp. 4702–4715.

[37] HM Manjula, SP AnandaRaj, "Ayurvedic Diagnosis using Machine Learning Techniques to examine the diseases by extracting the data stored in AyurDataMart", 3rd International Conference on Advances in Computing, Communication Control and Networking (ICAC3N), 2021.

[38] Chaudhary, Ayushi, and Ashish Sharma. "Designing LSB based Steganographic Approach Using Randomization Process." Design Engineering (2021): 11644-11655.

[39] Madhura, K., Mahalakshmi, R. (2021). Securing the organization documents in content management system with two levels of security using encryption and block chain technology. Design Engineering, 14025-14039.

[40] Dr. Madhura K. (2022). Applying Block Chain Technology to Improve the Storage Security of Static Contents in Content Management System. Mathematical Statistician and Engineering Applications, 71(4), 2487–2498. Retrieved from https://www.philstat.org.ph/index.php/MSEA/article/view/809.

eISSN 1303-5150