DOI 10.15622/ia.22.5.6

U. PILANIA, M. KUMAR, T. ROHIT, N. NANDAL

A WALK-THROUGH TOWARDS NETWORK STEGANOGRAPHY TECHNIQUES

Pilania U., Kumar M., Rohit T., Nandal N. **A Walk-through towards Network Steganography Techniques.**

Abstract. 2D and 3D digital multimedia files offer numerous benefits like excellent quality, compression, editing, reliable copying, etc. These qualities of the multimedia files, on the other hand, are the cause of fear including the fear of getting access to data during communication. Steganography plays an important role in providing security to the data in communication. Changing the type of cover file from digital multimedia files to protocols improve the security of the communication system. Protocols are an integral part of the communication system and these protocols can also be used to hide secret data resulting in low chances of detection. This paper is intended to help improve existing network steganography techniques by enhancing bandwidth and decreasing detection rates through reviewing previous related work. Recent papers of the last 21 years on network steganography techniques have been studied, analyzed, and summarized. This review can help researchers to understand the existing trends in network steganography techniques to pursue further work in this area for algorithms' improvement. The paper is divided according to the layers of the OSI model.

Keywords: network steganography, open system interconnection model, protocol, bandwidth, embedding capacity, physical layer, data link layer, network layer, transmission layer, application layer.

1. Introduction. With the enhancement in network technologies multimedia files are used for the transfer of secret data using different protocols. Various protocols are there which can be used to transfer required data from one place to another place [1, 2]. Network steganography is gaining the attention of researchers day by day over other multimedia steganography techniques. Because of increasing reliance on digital communication and data transfer over networks, there is a growing need to secure sensitive information from unauthorized access. Network steganography offers a covert means of hiding data within network traffic, providing an additional layer of security and privacy. Protocols from mostly five layers (Physical, Data Link, Network, Transport, Application) of the OSI (Open System Interconnection) model can be used to hide secret data [3]. The presentation and session layers of the OSI model are responsible for aspects such as data formatting, encryption, establishing and maintaining communication sessions between network entities these two layer does not deal with data hiding. The steganography technique which uses a single protocol to hide secret data is known as intra-protocol steganography. These types of techniques are based on modification in PDU (Protocol Data Unit). Whereas, Inter-protocol steganography uses more than one protocol to hide secret data [4, 5]. It includes padding steganography

which uses more than one protocol to hide the existence of secret data resulting in large embedding capacity, more security, and is highly robust. It has many advantages over 2D and 3D multimedia steganography techniques as follows [6, 7, 8]:

– In network steganography, there are options to design hidden channels on mostly five layers of the OSI model.

– In it, hidden secret data flow in both directions which results in more security and robustness.

– Also, it has short life on the network during the transfer from source to destination.

– In it, the network itself acts as the carrier file, unlike other multimedia steganography techniques.

– The bandwidth of the communication channel is affected by the type of multimedia carrier file used. But bandwidth of network steganography depends only on the type of protocol used to transfer secret data from source to destination.

Steganography started in ancient Greece in the classical form [15, 83, 84]. During that time secret data was embedded in the objects used in daily life. These objects include hair, wax, printer ink, skin, wood table, etc. After that digital steganography came into existence. In digital steganography, multimedia files such as text, images, audio, and video were used to hide secret data. Among multimedia steganography techniques, video steganography has drawn the attention of researchers for many years. But video steganography also has some demerits associated with it. These demerits include low embedding capacity, chances of detection of secret data, and poor visual quality of the stego file.

Classification of network steganography techniques is shown in Figure 1. Intra-protocol network steganography techniques can be broadly defined as updating network packet headers, updating network packet payload, updating the structure of packets, and hybrid techniques. [10, 11]. In the packet header, specific fields of the header of the protocol are modified for the embedding of secret data. Such types of techniques have good embedding capacity but are not very robust against attackers. Steganography techniques are based on the application layer of network model update payload to embed secret data. These techniques have low embedding capacities and are robust against attacks. Steganography techniques based on the structure of the packet may embed data in both headers and payload. In hybrid techniques, the header of the packet as well as time dependencies are modified for the embedding of secret data. Retransmission steganography is one of the best examples of this type of technique.

The efficiency of the network steganography technique can be measured based on the evaluation parameters. These parameters are embedding capacity, robustness, imperceptibility, and bandwidth [12, 13, 14].

– Embedding capacity is the amount of secret information that can be hidden in the protocol header.

– Imperceptibility is the invisibility of secret data inside the cover protocol.

– Robustness is the ability of the stego file to remain unaltered against attacks and stego file is a file that contains concealed or secret data embedded within it.

– Bandwidth is the average concealing capacity of every packet.

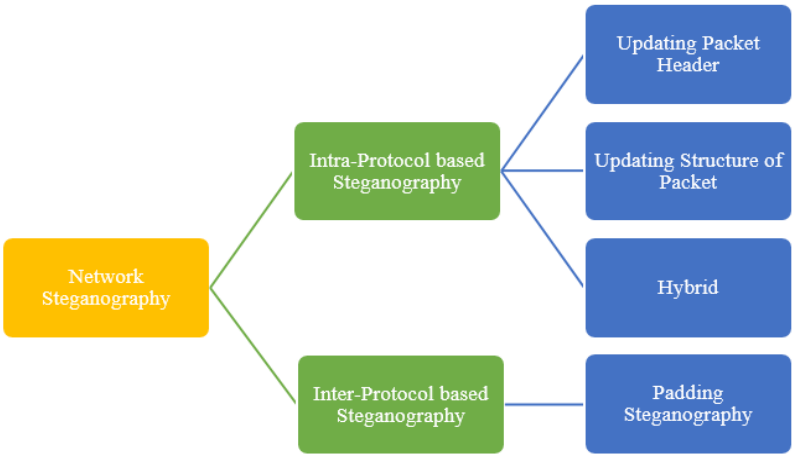

Fig. 1. Network Steganography Classifications [9]

To overcome the demerits of 2D and 3D multimedia steganography techniques, modern steganography came into existence. Network steganography is the modern steganography technique for providing safety to secret data. It provides the next level of security to secret data in a modified way. It hides the secret data into various protocols used at the different layers of the OSI model [17]. The proposed paper reviewed various network steganography techniques based on different layers of the OSI Model. A relationship was identified between the user's need and the steganography techniques to find its applications in hidden communication [6].

2. Methodology. Initially, 154 papers are selected for the review process. Then by applying certain filters, some papers are excluded as

shown in Figure 2. The network protocol-based papers are included for further processing. These network steganography papers are further segregated based on OSI model layers. An analysis of the reviewed techniques is done based on various parameters such as energy efficiency, bandwidth, visual quality of stego file, year-wise, layerwise, implementation tools, the combination of steganography and cryptography tools, etc.

The selected papers were published between the years 2002 to 2023. Papers for the review process are selected from various databases like the Web of Science, Science Direct, IEEE, Springer, Scopus, etc. Initial for the selection of articles for the proposed review paper following two quality assessment criteria have been set:

– Is the literature search likely to have covered all relevant studies?

– Are the review's inclusion and exclusion criteria described and appropriate?

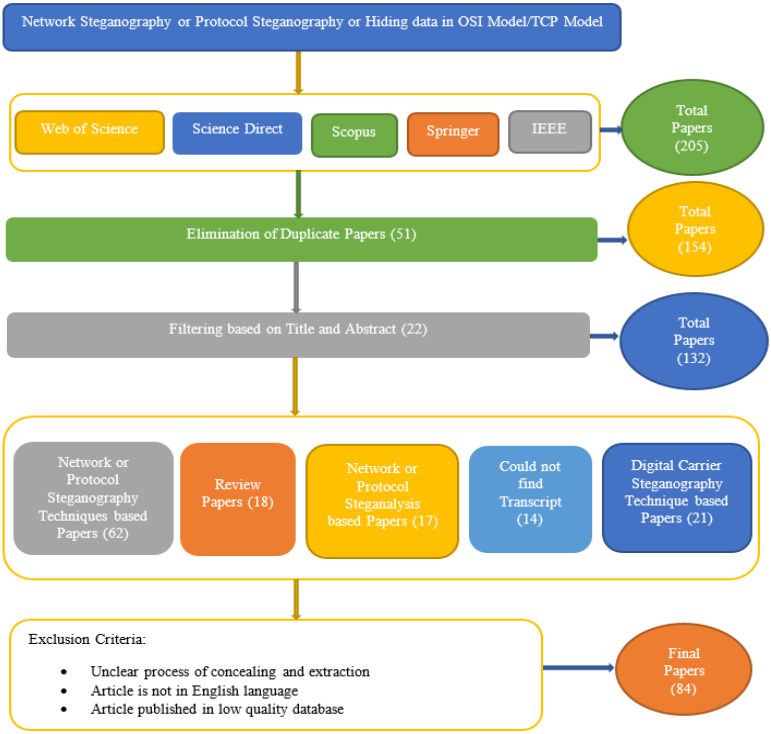

Fig. 2. Identification and selection of articles

All the included articles are published in the English language. Articles that satisfy the above-mentioned quality assessment criteria are selected for the review paper and the required information is retrieved for inclusion in our review paper.

In the research work, 84 articles have been studied and analyzed based on the statistical values. The details such as which layer of OSI model work has been done, which part of a protocol such as body or header has been used to hide secret data, what is the outcome of work in terms of bandwidth, whether work done is robust against attacks or not, steganography technique is combined with cryptography or not, on which tool implementation of work is done, etc. is being retrieved from the selected articles.

The methodology is divided into four stages, as shown in Figure 3.

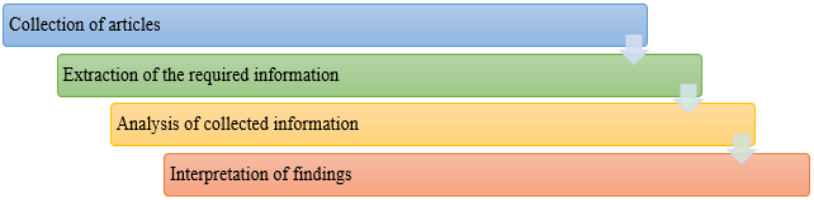

Fig. 3. Methodology Used

In the first stage, articles have been selected from different databases such as IEEE, Scopus, Springer, Web of Science, Science Direct, ACM, etc. for the review process. Duplicate papers are eliminated from the initial selection of 154 papers. The selected papers have keywords like "protocol" or "network steganography." Some papers are again eliminated based on the title and abstract of the paper. Exclusion criteria also include some critical points such as: the concealing and extraction processes are unclear, the published article is not in English, the type of carrier file used to hide secret data, the type of journal or conference, and so on. In the second stage, after exploring the article, the required information is collected and retrieved. The information is collected in the form of tables and diagrams with explanations. The explanation includes where secret data can be concealed and what the impact of hiding secret data has on the carrier file. In the third stage, an analysis of the retrieved information is done based on various evaluation parameters for the network steganography techniques. Various charts have been plotted for the analysis of the work done in the reviewed papers. Last, the statistical analysis was done for the survey of the protocol steganography techniques.

2.1. Hiding Secret Data in OSI Model. OSI model is the reference model for communication over the web. It has seven layers and each layer has its predefined functions. Each layer has a specific set of protocols. These protocols can be used to hide secret data in a different layer of the OSI model [15, 18]. Many papers have been reviewed in this section based on the reference model to analyze how protocol steganography is different from digital steganography.

2.1.1. Hiding Secret Data in Physical Layer. It is responsible for providing all the necessary connections. Data may be transmitted either through a wired connection or through a wireless connection. It decides the mode of transmission of secret data. It converts data into binary form. It has various protocols which can be used to hide secret data [19]. The protocol has various fields in its header format, and these fields can be used to hide secret data. Depending upon the size of the field used to hide secret data, the amount of secret data varies [20]. Some of the papers based on the physical layer protocol steganography are given in the section.

OFDM (Orthogonal Frequency Division Multiplexing) is used in various telecommunication applications. OFDM was the procedure of multicarrier modulation like sound, video, and images. In it, information was sent serially. In OFDM, secret data was hidden in the cyclic prefixes because cyclic prefixes are not read by any of the radio receivers. OFDM converts cyclic prefixes into codes and then converts them into fragments. Generally, prefixes were added earlier to the symbol communication but afterward its modulation. So, the fragments of the secret data should be modulated [21].

Because of modulation, the proposed method was not as effective and secure. So, to improve the security, a pseudo-random number generator (PRNG) was used by both the sender and receiver. With the PRNG, both parties were well synchronised in terms of time. Both the sender and receiver also used the private secret key to protect the data. In the proposed research work, the cost of the steganography technique was increased compared to the normal network. Implementation was done in MATLAB with many configurations of the networks. For the work, SNR (Signal Noise Ratio) was calculated as 4 DB. The embedding capacity was calculated at 3.25 Mbps to 19.5 Mbps, depending upon modulation [22].

In the previous paper, the concealing capacity achieved was very low. So, to achieve high concealing capacity again, the OFDM protocol was chosen by the author, and secret data was hidden in different parts of the protocol. It comes under the 802.11 standards. Its transmission limit of only 100 meters exists in the absence of amplification. As OFDM has its own specific format, fewer amounts of data can be hidden in it and transmitted to

the destination. In the proposed research work, it hides secret data in the padding field of the protocol. Padding carries three subfields, which are data unit, service, and tail. The size of the service and tail is fixed in the case of OFDM, but the size of the data unit may vary with the type of operation performed by the user. OFDM takes input from the user in the form of a signal. It then performed modulation on the given input signal. An Inverse Fast Fourier Transform was applied to hide the secret signals. Again, modulation was done to generate the OFDM signals. Now the transformed data is travelling through the web for its delivery to its destination. A reverse process was performed at the destination to get the original output data.

In the research work, it was considered that there were frames that were ready to transmit. The error rate was fixed by the authors to maximise the bandwidth. The rate of data transmission was also fixed for all the stations in the network. All the frames were carried at a constant length. Data frames and acknowledgment frames were exchanged between nodes for communication purposes. For the work, the maximum bandwidth obtained was calculated as 1.54 Mbps. For the data frame, it was calculated at 1.1 Mbps and for the acknowledgment field, it was calculated at 0.44 Mbps. The bit error rate was calculated as 10-5 for the research work, which was not noticeable by naked human eyes [23].

Worldwide Interoperability for WiMAX (Microwave Access) is a broadband IEEE 802.16 standard model. It can deliver advanced data rates with improved coverage. It works on the MAN (Metropolitan Area Network). It efficiently encodes and decodes the signal without information loss and then transmits it to the destination. It is commonly used in video conferencing and streaming, VoIP (Voice over Internet Protocol), e-learning, etc. WiMAX uses TDD (Time Division Duplex) and FDD (Frequency Division Duplex) for bidirectional communication. In the proposed work, WiMAX frame padding and the RS (Reed-Solomon) were both used to hide the secret data. The efficiency of the proposed work depends on the resources used and the network conditions. Implementation of the work was done in MATLAB and its performance was evaluated based on parameters such as duplex type, bandwidth, frame duration, guard intervals, etc. In the padding field of 802.16, sequences of zeros were stored. Sequences of zeros were replaced by the secret data and then transmitted to the destination. The stego file was transmitted through downlink frames. Each downlink frame has a header, a broadcast message, and data. The data field was almost 2035 bytes long, and the header has a length of 6 bytes.

The size of the secret data embedded depends on the network conditions. On embedding a large amount of secret data, noise increases,

resulting in the detection of secret data. WiMAX can operate on two networks: ATM (Asynchronous Transmission Machine) and packet network. cell has a size of 53 bytes, and the size of an IP (Internet Protocol) packet varies from 40 to 1500 bytes. As IP packets have a very large size compared to the ATM packet, they could hide a large amount of secret data without its detection. Apart from that, RS codes were also used to hide and send the secret data. This secret data was hidden in binary form in the sequences of RS code. The RS encoder helped to hide the secret data, and on the receiver side, the RS reader read the secret data. After reading secret bits of data, the receiver side retrieved them. On hiding secret data in IP packets at the rate of 60.4 Kbps, SNR was calculated as 25 DB. But hiding secret data in RS code at the rate of 0.8 Kbps SNR was calculated as 25 DB again [25].

ZigBee is the IEEE 802.15.4 standard PAN (Personal Area Network) protocol. It has applications in home automation, radios, medical devices, heating controls, smoking sensors, science, etc. ZigBee has four types of data frames that could be used to hide secret data. The ZigBee protocol stores secret data in the reserve bits of the protocol for security purposes in the proposed research work. The process of secret data transfer must be hidden from a third party; otherwise, hackers may detect it. Secret data was first encrypted by using the public key, and at the receiver side, it was decrypted using the private key. Secret data was taken in the form of text. ZigBee uses AES 128-bit encryption for security purposes. It has a low embedding capacity of 64 bits but has fewer chances of detection of secret data [26].

Figure 4 shows the summary of the work done on the physical layer of the OSI model. For the analysis of the research, the authors have taken different parameters like BER, Bandwidth, Embedded capacity, SNR, etc. BER is the error rate per pixel. SNR is the signal-to-noise ratio in the carrier file. Bandwidth is the amount of secret information that can be embedded per unit of time. Embedding capacity is the total amount of secret information that can be hidden in a carrier file.

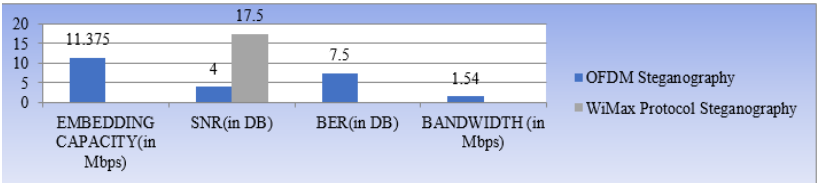

Fig. 4. Overview of Network Steganography in Physical Layer

2.1.2. Hiding Data in Link Layer. The data link layer is the second layer of the OSI model. It carries data in the form of frames. It is responsible for flow control, error control, and access control. It has many

protocols such as stop and wait, selective repeat ARQ, aloha, slotted aloha, CDMA, and many more to perform various tasks. Flow control, speed of the source, and destination need to be synchronized to minimize the traffic and to get the maximum throughput [27].

In the proposed work [28], DCT (Discrete Cosine Transform) and CDMA techniques were combined to hide the secret data. DCT was used to convert the given signal from the spatial to the frequency domain. DCT was performed up to two levels for finding the most refined coefficients and the noisy coefficients. Noisy coefficients were used to hide the secret data. Each DCT transformed coefficient was able to hide 1 byte of secret data. On increasing embedding capacity stego file might result in more distortion. The proposed codebook steganography technique divided the secret data into binary forms. A unique pseudo-random number sequence was used to divide the secret data. CDMA generated the pseudo-random number by utilising the concept of direct spread spectrum. With the help of pseudo-random numbers generated, multiple accesses on the channel could be performed without any interference. Pseudo-random numbers were transformed to status bits-1 and 1 [29]. These status bits were then multiplied by bits of secret data to produce sequences of data. These produced sequences were then added to get the complete data. The concept of CDMA improved the embedding capacity of the proposed work. The highest embedding capacity of the work was calculated at 9728 bytes, and the highest PSNR (Peak Signal to Noise Ratio) was calculated at 53.80 DB.

With the advancement in computer technology, the day-to-day security of online data is becoming a major concern among users. So, in this paper, cryptography, compression, and steganography were combined by the authors to provide security to the online data during communication. The authors used the blowfish-448 encryption algorithm for the compression of the file. Passphrase encryption was also applied to convert the secret messages into the scrambled form. Then the stop-and-wait protocol was used to hide the secret data inside the image. The amount of secret data embedded was 255 Kb without compression. The proposed work was also analysed for the security measure. The stop-and-wait protocol is the simplest protocol at the data link layer of the OSI model. It synchronises the speeds of the sender and receiver, resulting in low traffic and high throughput. In the proposed work, secret data was embedded in the retransmitted frame [30].

JPEG (Joint Photograph Expert Group) image was taken as the frame for the transmission of secret data. Secret data was taken as text in the proposed work. A passphrase was generated by the sender to avoid the detection of secret data. A key agreement was required between the sender and receiver of secret data. The same key was used at both ends for

encryption purposes. DH (Diffie–Hellman) key exchange protocol was for the key. The keys were exchanged in the numerical form resulting in no doubt to the third person. The encrypted secret data was then compressed using the blowfish-448 algorithm. The blowfish algorithm could use the variable key length varying from 32 bits to 448 bits resulting in the improved security. Because of the compression the embedding capacity was also improved. At last secret data was embedded into the image and it was transferred to the destination in the retransmission frames. The blowfish algorithm avoids the detection of secret data by applying different attacks. The proposed work embedded the secret data of approximately 255 Kb. Histogram was plotted for the original and the stego image. The histogram showed the frequency distribution of both images. The quality of original and stego images seemed to be almost equal resulting in less chance of detection of secret data [31].

The utilization of steganography and cryptography together elevates the complexity of the technique. However, when employed in combination, this approach can enhance the security of the technique to a certain degree. 802.15.4 also works on the data link layer of the OSI model. It is a part of the MAC (Media Access Control) layer under the data link layer. It is also known as the low-rate wireless personal area network. It was defined in 2003, and it acts as the base for Zigbee. It has essential support for the secure transmission of secret data. It is also able to manage the energy of wireless networks [32].

The frames in it contain many fields like frame control, the sequence number of data, source address, destination address, payload, reserved bits, command type, acknowledgment, etc. Any of these fields could be used to hide the secret data. Depending upon the size of the field secret data size varies. For the implementation of the research work, the AvroraZ simulator was used. The payload part of the frame has a large concealing capacity. In the proposed work data was hidden in the data frame. All 5 fields of the data frame were used to hide secret data one by one. The proposed work was robust against attacks and carried good embedding capacity [33].

Figure 5 shows the summary of the papers reviewed at the data link layer of the OSI model. For the evaluation of the work, different parameters were used by the authors. Some of the parameters are also given in the table such as concealing capacity, PSNR, energy consumption, histogram analysis, etc. The histogram analysis showed the frequency distribution of the stego and the original image. PSNR finds the error present between the original and the stego file. Concealing capacity is the amount of secret information that can be embedded inside the carrier. Energy consumption is the amount of energy used to conceal and extract secret information.

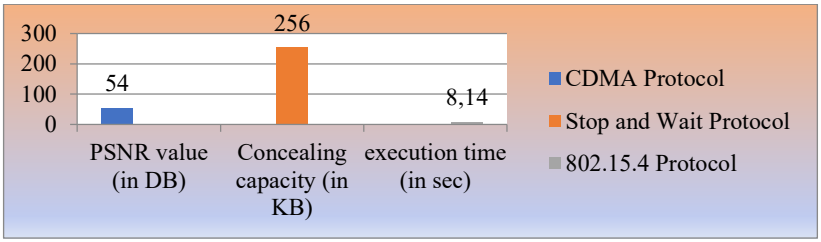

Fig. 5. Overview of Network Steganography in Data Link Layer

2.1.3. Network Layer Steganography Techniques. It is the third layer of the OSI model. It is responsible for providing routing. Routing helps to find the shortest path having low traffic. At the network layer concept of IP address is introduced. The IP address is 32-bits long and can be represented in either binary format or decimal format. Protocols such as IPv4 (Internet Protocol Version 4), IPv6 (Internet Protocol Version 6), ARP (Address Resolution Protocol), RARP (Reverse Address Resolution Protocol), etc., at the network layer, can be used to hide the secret data [34, 35]. Every protocol has its header format and various fields. More than one field can be used to hide the secret data. Hiding secret data in more than one field of protocol results in high security and large embedding capacity.

IPv4 works on the 3rd layer of the OSI model. It helps to find out the shortest possible path with almost no traffic. IPv4 has routing protocols such as border gateway protocol, routing information protocol, open shortest path first algorithm, etc. IPv4 creates a routing table for all the nodes in that particular network. Then smartly calculate the distance between a set of nodes along with measuring traffic. In the proposed research work, option field of the IPv4 protocol was used to hide the secret data. LAN (Local Area Network) was chosen to hide the secret data. LAN consists of a sender, receiver, router, and other intermediate nodes. The nodes in the LAN are connected either by wireless connection or through a wired connection. The sender has chosen 20 bits of input from the customer and then decomposes these 20 bits into 5 parts of each 4 bits. These decomposed bits are converted into a timestamp for sending data to the destination host. The overflow field was used to find the number of routers that are ideal in the network. Ideal routers did not create any timestamps. So, these timestamps were used to deliver secret data to a destination.

IPv4 used UDP (User Datagram Protocol) to transmit the packet from the sender to the receiver. To send secret data port number 11234 was used. At the receiver end, a Python script was used to retrieve secret data from the timestamps. In Python, the Scapy library is suitable to examine the packets and retrieve the secret data. All the five-time stamps were examined

to retrieve complete secret data. 10-time stamps were also created with the help of the same protocols to check the variation in the result. In the research work overall, bandwidth was calculated at almost 20 bits/packet. In the research work, packet loss was found to be almost zero [12].

In the above research work, the bandwidth was used to measure the performance of the work. The bandwidth was found to be very low for the mentioned work. So, to overcome the issue of low bandwidth some other protocols from the same layer were used. At the network layer, both ARP and RARP work. ARP has the IP address of the destination node and calculates the physical address of the same node. As the name suggests RARP is the reverse of the ARP protocol. Both ARP and RARP send the multicast request. Multicast means the request is sent to all the nodes connected to the network. The reply is unicast in the case of both protocols [36].

ARP network steganography was proposed in the local area network. LAN has sender and receiver nodes with lots of intermediate nodes. Secret message length was calculated and then the encoding of the secret message was done in hexadecimal notation. An unallocated IP address was searched for steganography. For finding an unallocated IP address a request was broadcasted to all the nodes in the local area network. Based on the reply an unallocated list of IP addresses was created. This process is repeated to make sure about the unused IP addresses. Then a seed value was entered to produce a set of random numbers. Seed value again helps to find the unallocated IP address. Now the receiver sends the ARP broadcast reply to the nodes in the network. The source host sends the unicast reply with the embedded bits of secret data on the physical address of the sender. At a time, the source node sends only 11 bits of secret data. On the receiver side, the same procedure was repeated to find the list of unallocated IP addresses. Then the value of the seed was inputted to confirm the unallocated IP address. Both source and receiver nodes put the same seed values. Now the receiver node retrieves the secret message. By using the ARP protocol 44-bit message was embedded in the ARP reply [37].

Hidden communication that does not depend on direct traffic between a sender and receiver is known as a "dead drop." In this proposed paper, ARP and SNMP (Simple Network Management Protocol) were used to hide the secret data. SNMP is the most commonly used protocol for reading information about the configuration and status of network devices. It can also modify the information of the network devices to change the behaviour of the network. Network devices commonly include cables, routers, switches, hubs, bridges, computers, servers, printers, and many more.

ARP cache was used to hide the secret data for the research work. The Sender's IP address and the physical address were utilized to hide the secret data. The complete process was done in a LAN environment. The IP address was controlled in the LAN environment due to the explicit subnet and isolated IP range. Along with that sender also monitor the traffic so that the existing address does not collide. The physical address has 48 bits so out of these bits last three bytes could be used to encode the secret data. As physical address was less controlled in the LAN resulting in a low chance of detection of secret data. Secret data was also decomposed into multiple parts to fit into the available space in the physical address of the ARP packet. Now at the receiver end, SNMP read the secret data that were hidden by ARP. Retrieved secret data by the SNMP was combined back to obtain the complete secret data. The hidden secret data was not detectable by any steganalysis technique [38].

A very less amount of secret data that is 11 bits per packet were hidden in the above research work. Steganography is not a simple task. It takes a lot of time and computer resources to hide the secret data. So to justify the research work a reasonable amount of secret data needs to be sent to the third party. IPv4 is the older version of internet protocol and its position is overtaken by IPv6. Several covert channel options were available in internet protocol to hide the secret data [39]. IPv6 could be used to hide secret data. The size of secret data hidden varies with the size of the field chosen. Bandwidth is also affected by the selection of fields for hiding secret data. As IPv6 has many fields and any field can be used to hide data. In the proposed research workflow label field was chosen to hide secret data. The flow label is 20 bits so the maximum of 20 bits can be hidden at a time. RSA (Rivest-Shamir-Adleman) encryption was applied to scramble the secret data. Chaos theory was also used to encode the secret data. Chaos theory is subtle to the initial settings, it is non-repeating and constrained. It introduces randomness in the input secret data. By using encryption and chaos theory along with network steganography security of the system was improved.

At the side of the sender, secret data was inputted as shown in Figure 6. On the input data, the fifth-order chaotic map was applied to encode the data. On the generated encoded data RSA was applied for scrambling. Generated ciphertext was converted to ASCII value first and then into hexadecimal. Again, the hexadecimal was converted to the binary value. The binary value was converted into sets of 20 bits each. Then one by one these sets were embedded into 20 bits' flow label field of IPv6. The packet number of IPv6 was sent to the destination and at the destination, the receiver retrieves secret data by applying a decoding algorithm. During decoding reverse process takes place. The proposed work was robust against attacks [40].

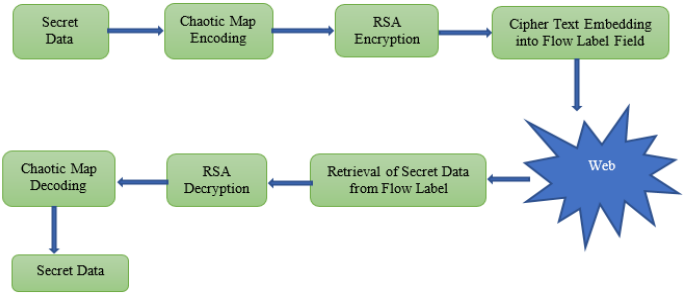

Fig. 6. Secret Data Hiding in IPv6 Flow Label [40]

Figure 7 shows the performance of the network layer protocol steganography techniques. For the evaluation of the work concealing capacity, concealing and retrieval time were used by the authors. Concealing time is the amount of time used to hide the secret data inside the carrier file. Retrieval time is the amount of time required to extract the secret data hidden in the stego file. Concealing capacity is the amount of secret data that can be embedded inside the carrier. Network steganography is most commonly used by many researchers to hide secret data.

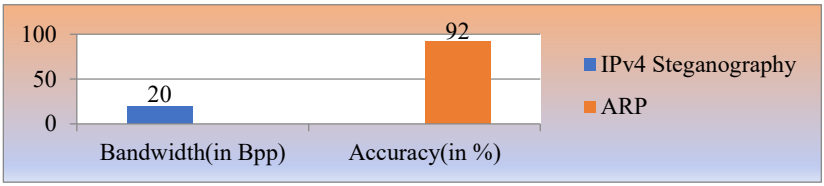

Fig. 7. Summary of Network-Layer Protocol Steganography Techniques

2.1.4. Transport Layer Protocol Steganography Techniques. It is the heart of the OSI model. On this layering concept of a port, address is introduced. It has protocols like TCP, UDP, SCTP (Stream Control Transmission Protocol), and many more. This layer provides both types of services such as connection-oriented and connectionless. TCP is a reliable protocol as its receiver after receiving a message sends an acknowledgment to the sender [41]. On the other hand, UDP is a connectionless and unreliable protocol. Again, the protocol header, as well as the data part, can be used to hide the secret data at this layer also.

The limitation of low embedding capacity can be enhanced by taking video as a carrier file. Popular social networking sites like Facebook, Skype, YouTube, and Wireless network are the focus of attackers for the detection of secret data. Along with carrier file protocols are also used to provide

security to personal data. In the proposed research work network steganography was performed by the authors to hide data. PRNG was used to minimize the chances of detecting secret data. For decoding secret data secret key was used which was generated using PRNG. This processed data was hidden in the header field of the TCP/IP protocol. Proposed techniques include sender, receiver as well attacker for the detection of secret data.

After embedding of data compression of stego file was done to reduce its size back to normal. Secret data embedding was done in the various fields of TCP/IP protocol. Embedding data in more than one part of the carrier file results in good embedding capacity as well as improved security.

The introduction of random number generation increased the security of the system. Along with that, the concept of the fake key was also introduced to mislead the attacker in case they got access to concealed information. Secret data and keys, along with fake keys, were sent to the receiver. The generated key and location of bits of secret data were shared by the sender with the receiver. At the receiver end, the same key was used to encode data that was previously generated by the sender. The Stego file was decrypted and decompressed to retrieve the secret data. The quality of the recovered secret data is high [4].

The mechanism of using keys in steganography increases the security of the techniques, but along with that, complexity also increases. The security of secret data also varies with the size of the packet used to hide it. Secret data can be distributed randomly over the UDP protocol, resulting in more security. The secret message was decomposed into N 4-bit numbers. A matrix with 16 rows was created to store the decomposed numbers. The 4-bit number was converted to binary form before being sent to the destination. This binary secret data was sent successively through the chatting system. The length of the original cover file as well as the stego file was calculated by the receiver. For the retrieval of secret data, modular arithmetic was calculated by the receiver [9].

Research work was simulated for the 50 different chat models. The length of the original and stego files was calculated for all 50 chat files. Time series were performed for both original and the stego files. Time series has shown the difference in packet length pattern of both files. So, secret data could be detected with the help of time series performed on the chat group. By using the UDP protocol difference in the packet length pattern could be reduced. Because UDP introduces randomness in the packet length resulting in more security [9].

Detection of secret data has become easy on concealing a large amount of secret data. The proposed research work used TCP and UDP for concealing secret information as shown in Figure 8. Hiding data into two

protocols avoid network traffic and increases randomness. Randomness results in high robustness for the proposed work.

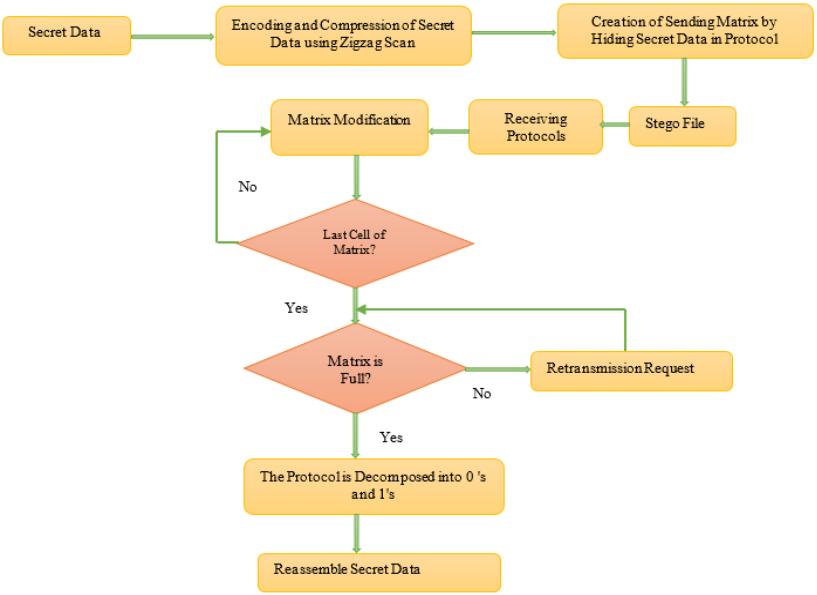

Fig. 8. Embedding and Retrieval of Secret Data [42]

The feasibility test as well as the bandwidth of the proposed work was calculated to analyze imperceptibility. For checking feasibility secret image was converted into binary form. These binary values were stored in the matrix. Each cell of the matrix has a decimal number that was equal to a pixel in the secret image. The dimensions of the matrix were reduced by using the zigzag method. This reduced matrix was sent to the receiver under TCP or UDP protocol. The receiver first converts the reduced matrix to the original matrix then-secret data was retrieved. The retrieved data was compared to the original secret data to compare the quality of the research work. The process was repeated 100 times for the set of images. The average bit error rate was calculated as 0%. The relationship between bandwidth and undetectability was also found by the authors in the proposed work. To provide no packet loss and almost no traffic bits of secret data need to be embedded is 1 bit per packet. In case of loss of secret bit, retransmission of a particular packet takes place resulting in low bandwidth. The bandwidth for the proposed research work was calculated as 0.998 Bpp [42].

In the world of the computer, everyone tries to transfer data in digital form. Transfer of online data also results in concerns about security issues. Using steganography, secret data can be transferred to the destination without the third party's knowledge. RSTEG (Retransmission Steganography) is applied when retransmission of packets is required. If TTL (Total Time to Leave) expires and no acknowledgment is received from the destination, then retransmission of the packet takes place. The RSTEG was applied to the TCP as it is the most reliable protocol. RSTEG comes under the hybrid class of network steganography techniques. Its main objective is to check the number of retransmissions, not to recognise the received packets.

In the process of sending secret data through RSTEG, both the sender and the receiver should be aware. When retransmission of the packet was required, then-secret data was encapsulated inside the packet itself. On the other hand, the receiver extracts secret data from the packet. Depending upon the amount of secret data embedded and the retransmission rate, the performance of the technique can be measured. RSTEG was implemented in the Linux environment. Its performance was measured through bandwidth, retransmission differences in packets, and the throughput of TCP. The proposed method has high bandwidth and embedding capacity compared to other existing network steganography techniques [44].

SCTP (Stream Control Transmission Protocol) was developed in 2000 and is the replacement for the TCP protocol. It is also a reliable protocol like TCP and sends data in sequence. It is also able to provide congestion control at the transport layer of the OSI model. SCTP overcomes the demerits of the TCP protocol. It sends a packet in the same order in which it receives the packets. It informs the receiver in advance about the non-transmission of a particular packet. In TCP, complete data is sent in one stream, but in SCTP, data can be sent into multiple streams. These multiple streams are independent of each other and can be transmitted independently.

The author proposed 13 chunks in the paper to hide the secret data, which were: init, ack, data, authorized, pad, etc. In the second method, SCTP packets were updated to hide the secret data. Multihoming was the main feature that could be updated. In this method, first, a path was tried to send the hidden secret data; when communication failed through this path, another path was chosen to transmit the data. Multi-streaming is another way to transmit secret data. SCTP used multiple streams to transmit the data. The value of the data was different for different streams. The last method was a hybrid of both the above-mentioned methods. Steganalysis techniques were also tried in the proposed work to identify the hidden secret data. But the hidden data was not exposed by any of the steganalysis techniques. Bandwidth was calculated to measure the quality of research work. The maximum bandwidth of 320 Bps was calculated

for the variable parameters under the category of the content modification method of SCTP. The minimum bandwidth calculated was 4 bits per chunk for authenticating parameters [45].

Improvements in the concealing capacity or the bandwidth of the technique may result in the loss of secret data because of compression. LACK (Lost Audio Steganography) was created in 2008, as shown in Figure 9 [46]. has its application in telephony steganography? To hide the secret data, it updates the RTP (Real-time Transport Protocol) packet in terms of audio and time dependencies. The sender chooses RTP from the audio stream and then its payload is replaced by the bits of secret data. RTP was an extremely overdue packet, and such types of packets were not used in the reform of secret data. These chosen RTP packets were intentionally overdue before transmission took place [47].

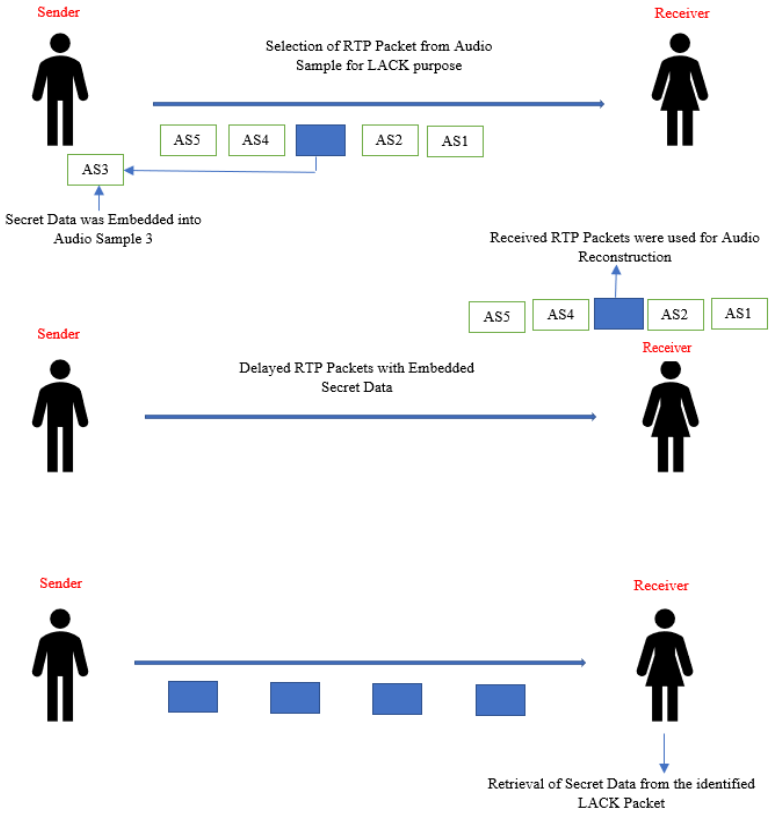

Fig. 9. LACK Steganography Process [46]

When these packets reach the receiver then he/she ignores these packets unaware of the hidden data. In case when the receiver is aware of the hidden data then he/she must retrieve it. LACK followed the hybrid method as it was the combination of time and storage. Time helped in the selection of RTP packets and storage would be responsible for hiding secret data. LACK could also be combined with the VoIP technique [48, 49]. In LACK with VoIP worked with a sequence number and the timestamp field. This technique was further extended by many authors. LACK was also combined with TCP protocol.

StegBlocks-based network steganography technique was proposed by the authors. Using it secret data was hidden in the network traffic. The performance of the research work was checked against malware. Static and dynamic analysis was done for the exposure of secret data. The behaviour of the network traffic was also studied for the detection of secret data. StegBlock used transport layer protocol to hide the secret data. It used two guards or the uniquely created packets which act as the separation between the characters. In the given Figure 10 block 1 and block 5 acted as the guards. Sending no packet between the guards means the value field has 0. Next time 4 packets were sent between blocks 1 and 5 which means value field=5.

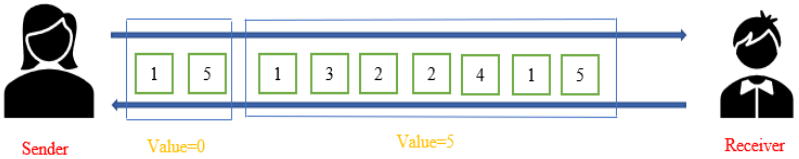

Fig. 10. StegBlock Process [50]

In the process of StegBlock, originally the SCTP protocol was used, and then many researchers used the TCP protocol as well. It usually transmits secret data in the form of text. It converts text data into binary form and then transmits it in the form of 0 and 1. In the SCTP protocol, guards act as the streams of blocks. One guard acts as the encoder and the second acts as the decoder. The proposed work has a low bit rate as compared to the existing research work. The bitrate depends on the traffic of the network. It was also carried out through lossy compression, in which case part of the secret data might be lost. As the bitrate increased, the chances of detection of secret data also increased. One more thing that needed to be taken care of was the involvement of the client [50].

In network steganography, secret data is hidden in protocols. It is a trend since 2003 and is growing among researchers. In this research article, the concept of the dead drop was applied to hide the secret data. When

secret data is not passed directly between sender and receiver but comes through a third person, that process is known as a "dead drop". But in Dead Drop, the third person is not aware of the hidden secret data. A dead drop is also known as the broadcast of secret data. NTP (Network Time Protocol) is the most commonly used protocol for providing time synchronisation for all the devices connected to the network. The data transmission of the NTP protocol is based on the routing protocols. NTP can also handle the monitoring and configuration mode using UDP protocol.

The NTP client and server carry data about the communication partner in the variables. These variables are of two types: system variables and peer variables. System variables carry data about themselves, but the peer variable has info about its surrounding system also. In this paper, the peer variables were used. Peer variables carry the IP address, physical address, port number, subnet mask, etc. The proposed work represents two methods that were discussed for reading and writing secret data to and from the NTP protocol based on a dead drop [51].

Data Hiding in Refid: In NTP refid field was used for hiding the secret data. The refid field carried the complete information of synchronizing the time of the server and the associated devices. Primary servers are connected to the secondary servers and so on. Through the mentioned connectivity complete information of time synchronization was provided for all the devices connected in the network. The IP address of the devices helps to synchronize the time of the whole network. Secret data was hidden in the IP address and no one was aware of it except the sender and receiver. As the IP address is 32 bits so a total of 32 bits of secret data can be hidden. Now NTP utilized broadcast mode which was: the client might have the broadcast IP address in that case all the packets sent to the broadcast address were accepted by the client.

Data Hiding in MRU (Most Recently Used) List: This method used a list of the most recent client and servers for hiding the secret data. For editing and writing data to the MRU list a request needed to be sent to the dead drop. MRU list has all the information about the request made by the client. So, no association was required between the drop and the sender of the data. NTP clients were requested to share the data about local time with everyone on the list. The address field of the MRU list was used to hide the secret data. 4 bytes of secret data could be hidden in the address field. Port addresses could also store 2 bytes of secret data. For retrieval of secret data at the receiver end, the receiver needs to answer some queries. After getting a satisfactory answer from the receiver within 20 seconds secret data can be retrieved.

Both the proposed covert channel was implemented into the Python language using the Scapy library. The reliability of the proposed work was also checked by the authors. The throughput of the proposed work was measured in the number of bits transferred per unit of time. Throughput was calculated as 240 bytes per minute. It is the secret data communicated with the number of entries on dead drops. A detectability test was also performed by the authors to check the robustness of the proposed work [52].

Figure 11 shows the summary of the transport layer protocol steganography. Different evaluation parameters were used to evaluate the research work. The evaluation parameters used were BER, bandwidth, variance, skew, mean, median, and payload capacity. All the parameters measure the quality of research work in different aspects. The original cover protocols were studied and then secret data was hidden in the suitable fields which are less exposed to the third person. Transport layer protocols are very useful in hiding secret data in various fields.

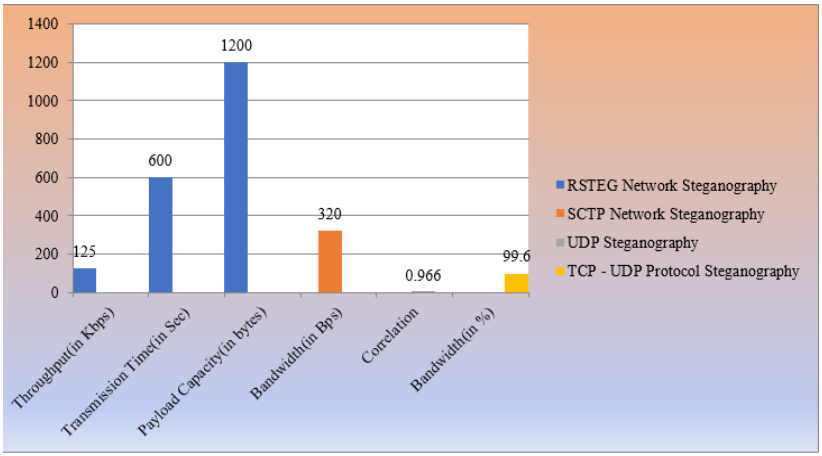

Fig. 11. Summary of Transport Layer Steganography Techniques

2.1.5. Hiding Data at Application Layer. The application layer is the uppermost layer of the OSI model. It is responsible for the user interface. With the help of the application, layer users interact with the system for performing various applications. It has many protocols like HTTP (Hyper Text Transfer Protocol), SMTP (Simple Mail Transfer Protocol), DNS (Domain Name Server), FTP (File Transfer Protocol), POP (Post Office Protocol), SNMP, Telnet, and many more [54]. Header as well as data part of these protocols can be used to hide the secret data.

HTTP is the best option to hide secret data. The web is growing dynamically these days so the use of HTTP protocol is also increased. HTTP is the binary protocol having many features such as [55, 56]:

– At a time, several HTTP requests can be transferred through TCP connections as distinct streams. HTTP reply might be received in some other order. HTTP can use the same connection to transfer more than one request at a time.

– It can perform server push. In server push, if the server knows that some resources are needed by a particular website then it can fulfill the request.

– It can compress the header size of the file drastically.

– It can set priority among the multiple requests sent by the client.

– It is bidirectional or it can transfer data in both directions.

– The padding field of HTTP protocol can also be used to hide the secret data.

DNS-based network steganography was performed in the paper. DNS is the protocol that converts the domain name of any website into an IP address. Any field from the header format of DNS can be used to hide the secret data like name, type, class, TTL, message length, IP address, etc. In the proposed work secret data was hidden in more than one above-mentioned field. Secret data was converted to the binary form and then the complete message was divided into the block of 4 bits each. The DNS application was written in Java language. Java helps to manage the network tasks and supports multithreading. It is a real-time algorithm with no delay. Testing was done on a virtual machine having window7. LAN having a router was used to experiment. Users browse the web according to his/her interest. He/she searches the content on the web and then moves to another website. In this way, many web pages were visited by the user. During web browsing, the malware was launched. The malware sent a number of packets carrying secret data to cooperating server every second. The process of browsing was monitored by malware continuously. In 600 seconds, 17.3 Kb of secret data was sent by the proposed technique. The proposed research has high security [57].

In the proposed paper, DNS transmits secret data by establishing a connection. As it worked along with TCP so it guarantees the delivery of packets. After the connection was established, the selection of secret data was done. A personal ID was generated for the user. The seed was generated that helped in producing a random number. The secret message was checked for its type. HMAC (Hash-based Message Authentication Code) was applied to encrypt secret data. The encrypted message was encoded by a random number. The complete process on the client-side is explained with the help of Figure 12.

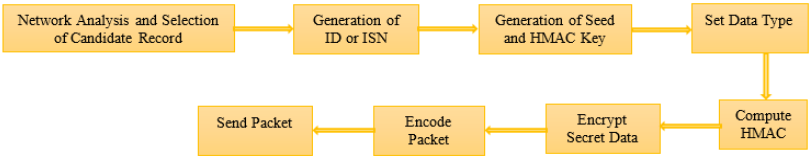

Fig. 12. Data Transmission from Client-Side [58]

At the receiving end, decoding of the secret data was done as shown in Figure 13. Then it was decrypted using the HMAC algorithm. The retrieved secret data was matched with the original secret data. HMAC helped in checking the integrity and authenticity of secret data.

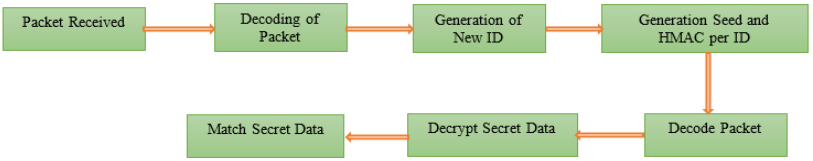

Fig. 13. Data Transmission at Server-Side [58]

Simulation of work was done in Python programming. User records used were of character and integer type. Two datasets were taken to check the traffic and other characteristics of the channel. One dataset was chosen from the home network and the other from the xDSL network. Different sizes and format files of secret data were tried to check the performance of the work. The average embedding capacity of 2.65 bytes of secret data was hidden in a packet. About 72 packets were transferred in 30 seconds [58].

Energy efficiency is also the most important parameter in network steganography. It is a new concept that uses the protocol to hide secret data. CoAP (Constrained Application Protocol) is a unique protocol that can constrain the devices in the network. CoAP works on the client-server model. The client sends the request to the server and then the server search for the result in its database. After collecting a response, it sends back the reply to the client. It describes 4 categories of communications: Confirmable (CON), Non-Confirmable (NON), Acknowledgment (ACK), and Reset (RST). Reliable service provided by this protocol is known as CON and unreliable services are known as NON [59].

The version field represents the current version of the protocol and requires two bits. The 2-bit Type field represents the 4 categories of communication i.e., CON, NON, RST, and ACK. 4-bit token length field and represent the error in the message format. The 8-bit code field is divided into two parts: the most significant and the least significant bit. It

determines the type of message: client request, client error response, server response, server error response. 16-bit message perceives matching communication and acknowledgment. 64-bit token field used to associate request and response. The 64-bit option field represents a set of options for the request and response query. Payload is another field in the protocol which represents the request and responses from users. Any of the fields of the CoAP protocol can be used to hide the secret data. If a particular field is represented in more than one way that means secret data can also be hidden. The embedding capacity and robustness of the technique change as the covert channel changes. The quality of the research work was measured in terms of PRBR and concealing capacity. A maximum of 2040 PRBR was obtained for the case-insensitive part of URI in 10 seconds. A low of 1 PRBR was calculated for many options such as delete, conditional request, piggybacking, re-transmission and accept in 10 seconds [60].

Complexity is also one of the major concerns in steganography. Because of the increased complexity, concealing time, retrieval time, key management, cost, etc. need to be adjusted. SCONeP (Steganography and Cryptography over Network Protocols) is the process of hiding secret data inside network protocols. It utilises the protocols ICMP (Internet Control Message Protocol) and UDP for its work. The proposed research work provides additional security through the encryption process. Before embedding the secret data, it was encrypted using Huffman coding. Then secret data was hidden inside either ICMP or UDP. After hiding secret data, compression was done, which resulted in improved embedding capacity. At last, an active warden was used to avoid the attacks [61]. The proposed work of the SCONeP model is shown in Figure 14.

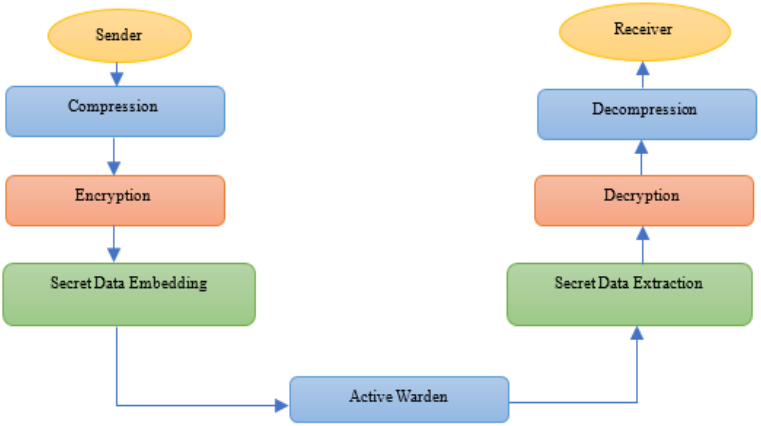

Fig. 14. SCONeP Working Model [61]

Compression was done using the Huffman coding algorithm. This algorithm converts the given file into binary form. A list of binaries was created and then transmitted for the next process. The next process was the compression module first; two bytes of the file contain information about whether compression is needed or not. If the value carried out by the first byte was the negative value that means no compression was done. The value between 1 to 7 represents the number of bits changed in the original file. Now in the second module encryption took place using both the private and the shared keys. Private key encryption was done using RSA and shared key encryption was done using triple-DES (Data Encryption Standard) or Vigenère algorithm. For both, the algorithm OpenSSL library was used. A random value generated at run time was used to decide which one shared key algorithm is needed to apply. If the random value was found to be odd that means the Vigenère algorithm will be required. Even the value generated means the RSA algorithm was used. To make the encryption module more general 24 bits' keys were used.

SCONeP was used to embed the secret data into the header of any of the protocols TCP, IP, UDP, and ICMP. In TCP, ISH (Initial Sequence Header) was used to hide the secret data. In ISH 32 bits of secret data were embedded. On the receiver side, the same processes take place in the reverse direction. The receiver first extracts the secret data from the protocol. The extracted secret data was then decrypted using the Huffman coding algorithm. At last decompression of secret data was done to get the complete secret data. Warden was used to checking the delectability of the proposed work. Both active and passive wardens were used to test the delectability. SCONeP was able to hide a maximum of 6 bytes of secret data [62].

MKIPS (Master Key Identifier-based Protocol Steganography), was proposed by authors in this research work. Initially, VoIP was developed to transfer audio over the web but these days its applications are increasing. It is used in traffic management, security, online gaming, video conferencing, and many more. SRTP (Secure Real-time Transfer Protocol) could also be used for providing all the mentioned applications along with confidentiality, replay protection of messages, and authentication. SRTP working was based on the random keys generated by MKI (Master Key Identifier). With the help of MKI, it did encryption and decryption of secret data and revived key values after a time interval. It worked efficiently when used in video conferencing with multiple users. It decreased the chance of detection of secret data because of refreshing the master key periodically. A refreshment table of the MKI was provided to the list of users. MKI was added to every packet before its transmission. At the destination, the receiver has chosen

the key from the MKI for the decryption of secret data. Depending upon the value of the master key size of secret data varies.

In the proposed work SRTP packets were used to hide the secret data. Secret data was concealed in the MKI field of the SRTP protocol. SRTP maintained the replay protection, confidentiality, and authorization of secret data. The receiver needs to first select the correct key from the set of keys and then retrieve the secret data. After retrieval of secret data, it was decrypted. The research work was implemented in Python using a Wireshark analyzer. The flow chart in Figures 15 and 16 represent the embedding and extraction of secret data. In the work maximum of 128 bytes were provided for the MKI and 80 bits were provided for the authentication purpose.

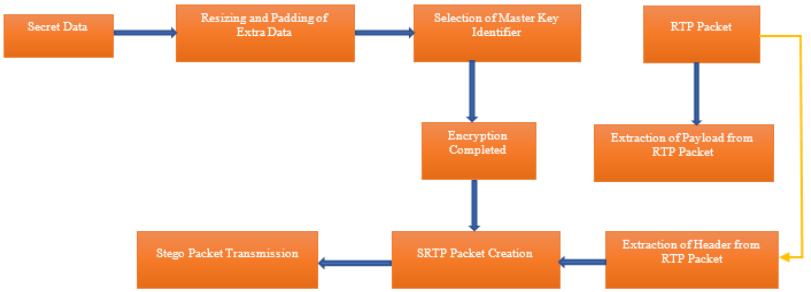

Fig. 15. Embedding of Secret Data using MKI [63]

Fig. 16. Extraction of Secret Data using MKI [63]

Experimental results were compared with the existing work as well. The research work has a high embedding capacity with almost no disturbance in the cover protocol. The data communication speed of the work is dependent upon the chosen MKI field. The size of the MKI field varies from 1 byte to 128 bytes but it was fixed for a specific session. An embedding capacity of 128 bytes was provided by the proposed work along with authentication, confidentiality, and replay protection. It provided a double level of security because of the combination of encryption and steganography techniques [63].

In today's world communication of digital information through email, the system is most common. So steganography in email does not result in the detection of secret data. SMTP and POP work on the application layer of the OSI model. Both protocols are used by email systems to send and transmit the data. Initially, SMTP was handling only the text files but now it handles MIME (Multipurpose Internet Mail Extension) files as well. Secret data transmission can be done through an email system. In the proposed work secret data was hidden in the body of the email. As email has some hidden field where secret data could be embedded. Part of email like headers and some other fields are not visible to the user as well to the intermediate agents. So, these fields were neither used by the agents nor updated by anyone. These fields just look like the ASCII strings and their usages were also restricted to end-users. These fields could be used to hide the secret data following certain rules for the integrity, confidentiality, and authentication of secret data. It does not matter where the sender and receiver are sitting and sending mail messages to each other. For retrieval of secret data embedded receiver must have prior information.

SMTP has two parts body and the header. The body may have normal text or a MIME file as the attachment. The complete mailing system is divided into four parts. Both sender and receiver were required to run MAU (Mail User Agent) on their machine. The sender prepared the message body and then established a connection with MAU. MAU checked the header part of the mail for finding the recipient's mailing address. MAU then requested DNS for resolving the IP of the destination. The receiver side MAU then sends mail to the particular user. With the help of the POP protocol receiver later on, after login can download the mail. Secret data could also be sent through spam mail. MAU directly sends them through their anti-spam scanners. Spam was considered unwanted stuff and it was stored in the spam folder directly by the MAU.

Figure 17 represents the complete flow of the process of embedding and retrieval of secret data. Secret data was compressed using Deflate compression algorithm. The compressed data was divided into parts and converted to binary form. Using the PBKDF2 encryption algorithm two keys were generated. The hash function was selected using the MD5 hashing algorithm. After applying hashing and encryption on the secret data, segregated secret data were combined back to get the complete message. HMAC was used to provide integrity, authentication, and confidentiality to the secret data. Timestamp was also used to verify the time of each operation performed and to avoid the attacks. Secret data was embedded in the header of the email. The index field contains the sequence

number of the segregated secret data and it was required during the process of obtaining the complete secret data through concatenation. At the time of retrieval of secret data reverse process of encryption takes place.

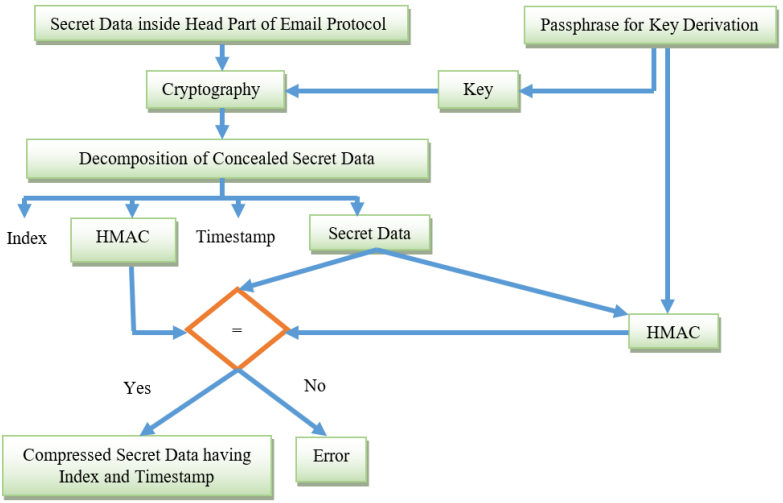

Fig. 17. Retrieval of Secret Data from Email Header [64]

HMAC, timestamp, and secret data retrieved were compared for finding whether any error was present or not. Bandwidth, embedding capacity, and detection of secret data all are directly related to each other. Bandwidth can be defined as the number of bits of secret data embedded per unit of time. So, on increasing bandwidth embedding capacity automatically increases. The improved embedding capacity increases the chances of detection of secret data. For the proposed research work embedding capacity was calculated as 50 bytes per second [64].

In almost all the steganography techniques author compromise with the concealing capacity because on increasing concealing capacity chances of detection of secret data increase. SSH (Secure Shell) is the protocol for providing secure remote login. It has built-in encryption techniques for security purposes. It works on the client-server architecture. SSH client sends the request to its server. They establish a connection and then communicate through that connection. SSH uses public-key cryptography and hashing for the security of data transmission. It provides the following functionality to the users [65]:

– It first establishes the connection and then transmits data through that connection.

– It can provide remote login using some set of commands.

– It is the authentication protocol. With the help of a password or some other option, it provides an authentication mechanism.

The packet size field is 32-bits long and represents the size of the packet. Padding size is the length of the packet to represent the padding in the packet. The payload is the real information inside the packet. Random padding is the additional data required to provide security. MAC provides the required authentication code for security. As shown in the figure first four fields are already encrypted. Packet payload and random padding fields are already encrypted.

In the research work, secret data was hidden in the traffic generated by the network. For traffic analysis, PT (Packet Transmogrifies) was used which was written in C language. It has been calculated that SSH in a session has 48 to 80 bytes to hide the secret data. PT selected a random packet for hiding secret data and at the receiver side, it was retrieved. PT used many protocols precise packet converters as the connector modules for selecting specific packets to hide secret data. 12 octets of secret data were hidden in the payload field of the packet. Before hiding secret data, it was divided into smaller chunks and converted into binary form. The CRC (Cyclic Redundancy Checksum) was used to check the integrity of secret data. The bandwidth for the proposed research work was found to be good as compared to other existing work [65].

A trade-off exists between bandwidth, security, and robustness in network steganography. VoIP is the most commonly used network steganography technique these days. VoIP uses the LSB (Least Significant Bit) technique to hide secret data. Embedding capacity can be improved by hiding secret data in voice packets during transmission. Random numbers in the selection of LSB bits improve the security of the research work. Embedding capacity varies from sample to sample of voice packet [66, 67]. Analysis of a few VoIP steganography techniques is shown as follows:

– Another way to hide secret data in the voice packet was using G.711 codec. The process includes compression of secret data and then it results in less embedding time. By doing so embedding capacity that is bandwidth can also be improved. By selecting 4-bits modification in the carrier can be reduced [68, 69, 70].

– In the proposed work Partial Similarity Value (PSV) between LSB of G.729a speech and secret data. This proposed combination resulted in high security and robustness. Concealing capacity was calculated by the number of similar bits and threshold. Embedding capacity was calculated at 1444 bits in 126 frames [71].

– A covert transmission scheme on G.711 stream over VoIP was proposed by the authors. It used sharp blocks to hide secret data for avoiding exposure. It carried an embedding capacity of 7.34 Kbps. It also avoided attacks from exposure to secret data [72].

The author proposed a real-time system for hidden transmission in VoIP using the LSB technique. First encryption of secret data was done and then embedding of encrypted secret data was done. The research work embedded 0.8 Kbps [73].

Figure 18 shows the summary of the work done at the application layer of the OSI model. Many papers have been published using the application layer protocols. Evaluation of the work published was done based on various parameters like bandwidth, concealing capacity, entropy, etc. Entropy is the measure of randomness in the carrier and the stego file. The higher is the randomness high are the chances of detection of secret data.

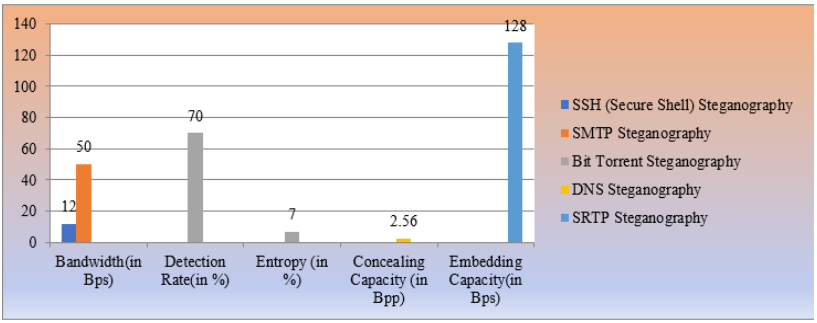

Fig. 18. Summary of Application Layer Steganography Techniques

3. Analysis of Research Trend in Network Steganography. Analysis of research trends is done on network steganography technique based on many parameters. The parameters include layer-wise analysis of the paper reviewed, year-wise analysis of the paper reviewed, bandwidth measure of the paper reviewed based on the layer of the OSI model, analysis based on steganalysis technique, the tool used to implement the research work, and, the combination of steganography with cryptography, etc. Analysis trend is explained in detail based on the mentioned parameters shown as follows:

3.1.1. Layer-Wise Analysis of Paper Reviewed. In the research work as shown in Figure 19, 73 papers related to network steganography techniques have been studied. Mainly three (Network, Transport, Application) layers of the OSI model are used by researchers to hide the secret data.

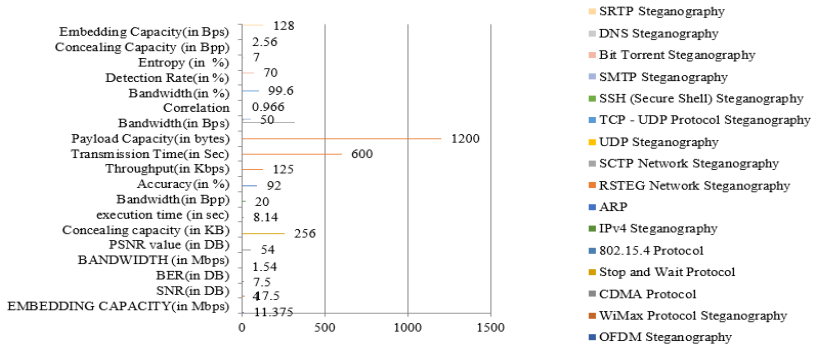

Fig. 19. Layer-wise summary of Steganography Techniques

These three layers are commonly used by steganography techniques to hide data but steganography can also be applied to other layers depending on the specific requirements and limitations of the application or system. The choice of layers depends on factors such as ease of implementation, the likelihood of detection, and the desired level of security or covert communication. The amount of secret data embedded depends on the type of protocol and the field used to hide it. Figure 20 is presenting the summary of all Layers based on the Steganography Techniques.

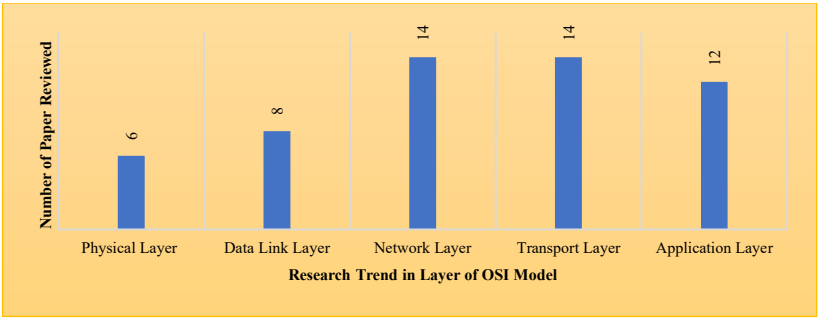

Fig. 20. Layer-Wise Count of Paper Published

TCP, UDP from the transport layer, and IP from the network layer are the mainly used protocols to hide secret data. Mainly during the retransmission of particular frames secret data is hidden in TCP protocol. Padding and option fields are mainly used by researchers to hide the secret data in IP and UDP protocols. It has been observed that physical and data link layer protocols are less used to hide the secret data.

3.1.2. Year-Wise Paper Reviewed. To prepare this research article, a total of 73 papers are reviewed. Network steganography has been investigated in 2003. Figure 21 shows the year-wise analysis of some of the papers from network steganography. These days' researchers are moving from digital steganography to modern steganography techniques. Modern steganography uses protocols of the OSI model to hide secret data.

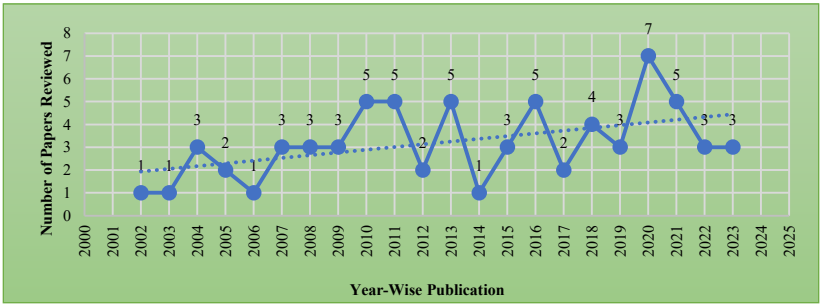

Fig. 21. Total Paper Reviewed

Papers are selected using network or protocol steganography keywords from several academic databases. As per a proposed paper lot of papers are published in the year 2020 and 2023. It has been observed that still; some issues exist with the network steganography techniques. Bandwidth and visual quality of the stego file are the issues of concern in the network steganography. On increasing the bandwidth of a particular technique visual quality of the stego file got compromised.

3.1.3. Layer-wise Bandwidth Measure of Reviewed Network Steganography Techniques. The performance of the network steganography techniques was measured by the authors in terms of bandwidth. In some papers, the correlation coefficient was also calculated to evaluate the research work. In this section, layer-wise evaluation of the research work is done based on the bandwidth. In some papers, steganography and cryptography techniques were combined to get better security.

Figure 22 showed the bandwidth achieved at the physical layer of the OSI model. Bandwidth is measured in the number of megabits per second for the physical layer steganography techniques. The value of bandwidth varies from protocol to protocol on the same layer. The maximum bandwidth is achieved by the OFDM technique and lowest by the ZigBee protocol steganography technique.

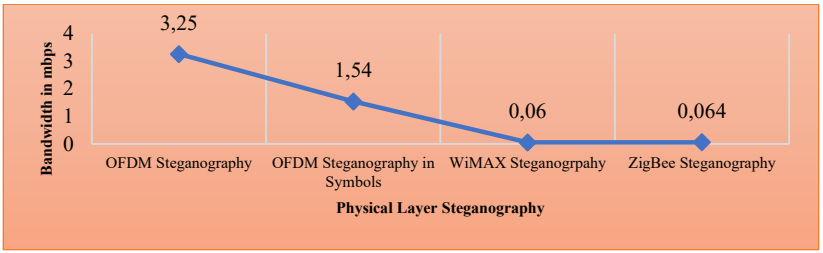

Fig. 22. Performance Measure at Physical Layer

Again, the performance of the data link layer protocols is calculated in terms of bandwidth as shown in Figure 23. This layer is responsible for flow control, access control, and error control. It has many protocols to provide the above-mentioned responsibilities. Bandwidth is measured in kilobits per second for the data link layer. Stop and wait protocol has a maximum bandwidth of 255 Kbps and CDMA has a minimum bandwidth of 77.8 Kbps.

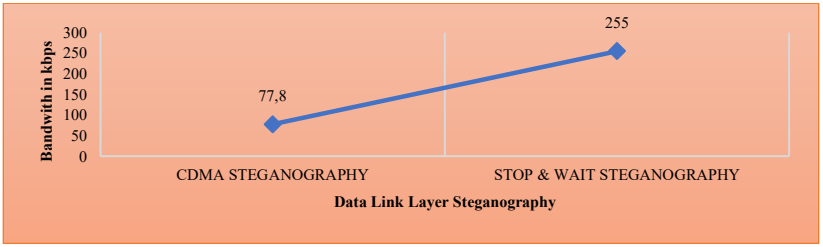

Fig. 23. Performance Measure at Data Link Layer

It mainly has IPv4, ARP, RARP, and IPv6 protocols. This layer works on the concept of IP address. Among the reviewed papers ARPNet has the highest bandwidth. As shown in Figure 24 bandwidth is measured in bits per second for the network layer. Bandwidth varies from protocol to protocol and the field was chosen to hide the secret data as well.

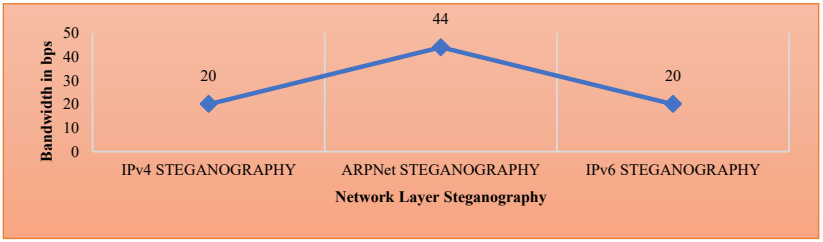

Fig. 24. Performance Measure at Network Layer

This layer provides reliable service as well as non-reliable service. Bandwidth is measured in kilobits per second for the transport layer. Maximum bandwidth is achieved by the combination of TCP and UDP protocols. Depending upon the application, the protocol is used to transfer data from source to destination. Figure 25 shows the bandwidth of the protocols used at the transport layer.

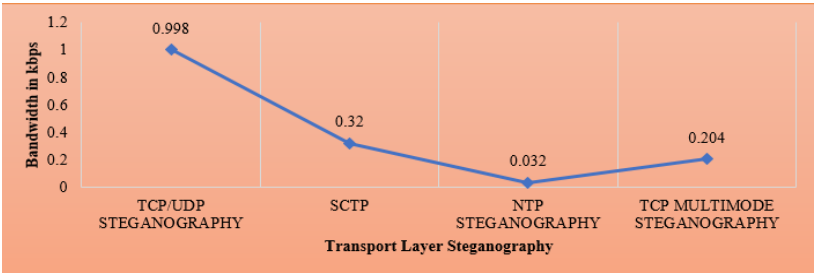

Fig. 25. Performance Measure at Transport Layer

Analysis of application-layer steganography techniques is shown with the help of Figure 26. The performance of these techniques is measured in terms of bandwidth. Bandwidth is the amount of secret data embedded per unit of time. The bandwidth of the technique depends on the size of the field of the protocol in which the secret was embedded.

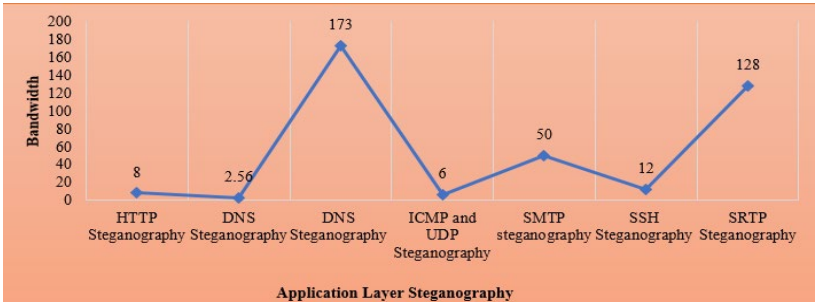

Fig. 26 Performance Measure at Application Layer

3.1.4. Analysis based on Steganalysis Technique. As we thoroughly reviewed different network steganography techniques. Some steganalysis techniques also exist to detect the hidden secret data. In some of the papers along with steganography, steganalysis techniques were also covered by the authors. In Table 1, 7 steganalysis techniques are analysed.

Table 1. Analysis of Steganalysis Techniques

Paper Title	Year	Method	Applied to
A Lightweight Adaptable DNS Channel for Covert Data Transmission [58]	2020	Opnsense 17.1 Firewall and Suricata 3.2.1 IDS	Open Sense and Suricata were run on the client-server machine. The firewall was installed on the same machine. When stego file was transferred, the firewall was not able to detect the hidden message.
A Multimode Network Steganography for Covert Wireless Communication Based on BitTorrent [53]	2020	Entropy Test	The regularity of data traffic is measured. The irregularity of traffic represents a high chance of detection of secret data.
An Approach of Covert Communication Based on the Adaptive Steganography Scheme on Voice over IP [72]	2011	RS Steganalysis	RS steganalysis is used to detect the hidden secret data. It is not able to detect the hidden data specifically in audio files.
Multilayer Detection of Network Steganography [2]	2020	Multilayer detection of RSTEG	Each layer used a different approach to detect the hidden secret data. It has been concluded that on the upper layers' detection is easy compared to the lower layers. For steganalysis, machine learning algorithms are applied.
Network Steganography and Steganalysis [74]	2013	GMM Model	Gaussian Mixture and Mel Frequency Cepstral Coefficients Model was used to detect the hidden secret data. The average detection possibility was found to be approximately equal to 89% in different formats of audio. Statistical properties were used to detect secret information.
Covert channel detection: A survey-based analysis [75]	2012	Irregularity in Time Intervals	In this paper, storage-based and timing-based covert channels were analysed to detect the secret message. It is very difficult or almost impossible to detect the hidden message. The irregularities in time intervals were used to detect the data.
Steganography and steganalysis in voice over ip: A review [76].	2021	VoIP Steganalysis	Steganalysis was done based on codebook destruction. Correlation between the pulse position of audio was calculated to detect secret messages. CNN and RNN models were also used to detect the hidden data but the presence of secret data was not detected.

For analysis paper title, year of publication, the method used, and work is included. For analysis statistical properties, traffic irregularities,

correlation, and many other parameters were used by the authors. It has been concluded from the analysis that it is not possible to detect the secret data.

3.1.5. Analysis based on Implementation Tool. Figure 27 shows the analysis of the tool used for the implementation of the reviewed techniques. Work is implemented using MATLAB, Python, and a network simulator as well. In most of the papers, the UNIX environment is used for implementation. Different simulators are used for the implementation of the work. Simulators have a component library and these are object-oriented. Simulators are wireless and discrete. By predicting the behaviour of a particular network on which the researcher is working secret data is concealed in protocols. Simulators are fast in calculating results. But simulators are difficult to build and also costly.

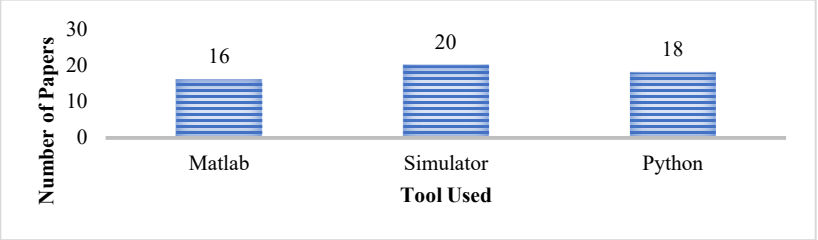

Fig. 27. Tool-wise Analysis

Python has very strong libraries as compared to MATLAB libraries [77]. Python can run on any type of platform. It has a good interface to all the databases. It is user-friendly and easy to maintain. MATLAB also has many built-in functions for plotting, visualization, numerical computation, and application development. MATLAB functions are written in C, C++, and Java. One major difference between mentioned two tools is that MATLAB treats every input as an array but Python takes input as objects [78, 79].

3.1.6. Analysis based on Combination of Cryptography and Steganography. A lot of work has already been done in the field of cryptography as well as steganography for security separately. Figure 28 shows how much work is done separately on steganography and how much on the combination of both steganography as well cryptography for the proposed paper based on the papers reviewed. Out of 73 papers reviewed for the proposed work, 43 are based on only steganography techniques and 21 are based on the combination of both techniques.

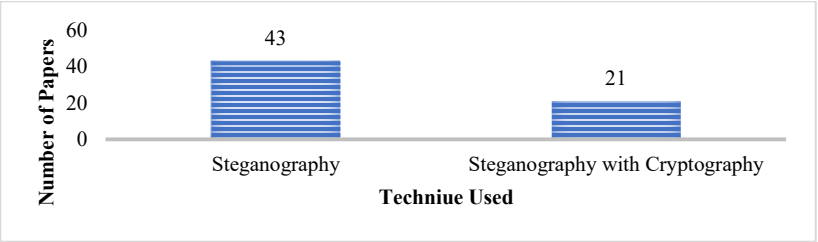

Fig. 28. Analysis based on Technique used

RSA, MD5, Digital Signature, DES, AES, HMAC, Blowfish, etc. are the most widely used cryptography techniques along with steganography [80, 81]. By combining these two techniques security is improved to some extent but complexity in terms of time and cost also increased [82]. So, to overcome the increased time and cost further research is required and that can be suggested as future research work.

4. Observations and Findings. A study of the last 21 years of network steganography techniques has been done in research work. A lot of pros and cons are associated with these techniques. These observations and findings are listed and will help researchers in future research. A few of the observations and finding are given as follows:

– **Overview of Network Steganography Techniques:** The paper would likely provide an introduction and overview of different network steganography techniques used to hide information within network communications.

– **Analysis of Steganography Methods:** The study examined different steganography methods employed in network environments, such as covert channels, protocol-based steganography, or payload-based techniques.

– **Evaluation of Security and Detection:** The researchers examined the security aspects of network steganography techniques, including the vulnerability of different methods to detection and countermeasures.

– **Challenges and Limitations:** The challenges or limitations associated with network steganography, including the potential for increased network traffic, limited payload capacity, or the risk of detection are highlighted in this paper.

– **Bandwidth and Detection of Secret Data:** Bandwidth and detection of secret data played an important role in all layers of the OSI model. Bandwidth is observed to be very low in the case of network steganography. Improvement in the bandwidth of a particular technique results in increased chances of detection of secret data.

– **Hybrid Technique:** To balance bandwidth and secret data detection, a hybrid of cryptography and steganography has also been implemented by the researchers. A hybrid of these two techniques improved the security, but the bandwidth was not improved.

5. Conclusion. In conclusion, various aspects of network steganography have been explored and examined its importance in securing data during communication. The paper has presented an in-depth analysis of existing network steganography techniques of the last 21 years. Exploration and examination of network steganography techniques have been done based on many parameters. The parameters include year-wise analysis of the reviewed paper, layer-wise analysis of the reviewed paper, bandwidth measure of the reviewed paper based on the layer of the OSI model, analysis based on steganalysis technique, analysis of the tool used to implement the research work, and the combination of steganography with cryptography. By examining and summarizing these techniques, researchers and practitioners can gain valuable insights into the current trends and advancements in the area of network steganography. This review serves as a foundation for future work, encouraging further research and development in network steganography algorithms and methodologies.

References

1. Mortazavian P., Jahangiri M., Fatemizadeh E. A Low-Degradation Steganography Model for Data Hiding in Medical Images. Proceedings of the Fourth Lasted International Conference Visualization, Imaging and Image Processing. 2004. pp. 914–920.
2. Smolarczyk M., Szczypiorski K., Pawluk J. Multilayer detection of network steganography. Electronics. 2020. vol. 9. no. 12. pp. 1–14. DOI: 10.3390/electronics9122128.
3. Szczypiorski K. HICCUPS: Hidden communication system for corrupted networks. Internation Multi-Conference Advance Computing System. 2003. pp. 31–40.
4. Sekhar A., Kumar G.M., M A.R. A Novel Approach for Hiding Data in Videos Using Network Steganography Methods. Procedia Computer Science. 2015. vol. 7. no. 4. pp. 49–61. DOI: 10.5121/ijwmn.2015.7404.
5. Almohammedi A.A., Shepelev V. Saturation Throughput Analysis of Steganography in the IEEE 802.11p Protocol in the Presence of Non-Ideal Transmission Channel. IEEE Access. 2021. vol. 9. pp. 14459–14469. DOI: 10.1109/ACCESS.2021.3052464.
6. Seo J.O., Manoharan S., Mahanti A. A Discussion and Review of Network Steganography. IEEE 14th International Confernce Pervasive Intelligent Computer. 2016. pp. 384–391. DOI: 10.1109/DASC-PICom-DataCom-CyberSciTec.2016.80.
7. Ouda A.H., El-Sakka M.R. A step towards practical steganography systems. Lecture Notes Computer Science. LNCS. 2005. vol. 3656. pp. 1158–1166. DOI: 10.1007/11559573_140.
8. Tanwar R., Pilania U., Zamani M., Manaf A.A. An Analysis of 3D Steganography Techniques. Electronics. 2021. vol. 10. no. 19. p. 2357. DOI: 10.3390/electronics10192357.

9. Nair A.S., Kumar A., Sur A., Nandi S.иLength based network steganography using UDP protocol. IEEE 3rd International Conference Communication Software Networks, ICCSN 2011. 2011. pp. 726–730. DOI: 10.1109/ICCSN.2011.6014994.
10. Zander S., Armitage G., Branch P. A survey of covert channels and countermeasures in computer network protocols. IEEE Communications Surveys and Tutorials 2007. vol. 9. no. 3. pp. 44–57.
11. Huang Z., Sun X., Luo J., Wang J. Security Against Hardware Trojan Attacks Through a Novel Chaos FSM and Delay Chains Array PUF Based Design Obfuscation Scheme. Lecture Notes Computer Science. 2015. vol. 9483. pp. 14–24. DOI: 10.1007/978-3-319-27051-7.
12. Bedi P., Dua A. Network Steganography using the Overflow Field of Timestamp Option in an IPv4 Packet. Procedia Computer Science. 2020. vol. 171. pp. 1810–1818. DOI: 10.1016/j.procs.2020.04.194.
13. Pilania U., Tanwar R., Gupta P. Stable High Capacity Video Steganography in Wavelet Domain. Turkish Journal of Computer and Mathematics Education Research Article. 2021. vol. 12. no. 7. pp. 2142–2158.
14. Pilania U. A Proposed Optimized Steganography Technique using ROI, IWT and SVD. International Journal of Information Systems and Management Science. 2018. pp. 313–318.
15. Zielińska E., Mazurczyk W., Szczypiorski K. Trends in steganography. Communication ACM. 2014. vol. 57. no. 3. pp. 86–95. DOI: 10.1145/2566590.2566610.
16. Zielińska E., Mazurczyk W., Szczypiorski K. Developement Trends in steganography. Communication ACM. 2014. vol. 57. no. 3. pp. 86–95. DOI: 10.1145/2566590.2566610.
17. Amirtharajan R., Rayappan J.B.B. Steganography-time to time: A review. Journal Information Technology. 2013. vol. 5. no. 2. pp. 53–66. DOI: 10.3923/rjit.2013.53.66.
18. Theodore G., Maxwell T., Sandford I.I. Hiding data in the OSI network model. Lecture Notes Computer Science. 1996. vol. 1174. pp. 24–38. DOI: 10.1007/3-540-61996-8_29.
19. Frikha L., Trabelsi Z. A new Covert channel in WIFI networks. Proceeding 2008 3rd International Conference on Risks and Security of Internet and Systems. 2008. pp. 255–260. DOI: 10.1109/CRISIS.2008.4757487.
20. Martins D., Guyennet H. Attacks with Steganography in PHY and MAC Layers of 802.15.4 Protocol. Fifth International Conference on Systems and Networks Communications. 2010. DOI: 10.1109/ICSNC.2010.11.
21. Shah D.C., Rindhe B.U., Narayankhedkar S.K. Effects of cyclic prefix on OFDM system. Proceeding of International Conference and Workshop on Emerging Trends in Technology (ICWET). 2010. pp. 420–424. DOI: 10.1145/1741906.1741996.
22. Grabski S., Szczypiorski K. Steganography in OFDM symbols of fast IEEE 802.11n networks. IEEE Security and Privacy Workshops. 2013. pp. 158–164. DOI: 10.1109/SPW.2013.20.
23. Szczypiorski K., Mazurczyk W. Steganography in IEEE 802.11 OFDM symbols. Security and Communication Networks. 2016. vol. 9. no. 2. pp. 118–129. DOI: 10.1002/sec.306.
24. Khan M.N., Ghauri S. The WiMAX 802.16e Physical Layer Model. IET Conference on Wireless, Mobile and Multimedia Networks. 2008. pp. 117–120. DOI: 10.1049/cp:20080159.
25. Grabska I., Szczypiorski K. Steganography in WiMAX networks. 5th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT). 2013. pp. 20–27. DOI: 10.1109/ICUMT.2013.6798399.

26. Hussain I., Negi M.C., Pandey N. Security in ZigBee Using Steganography for IoT Communications. System Performance and Management Analytics. 2019. pp. 217–227.
27. Jankowski B., Mazurczyk W., Szczypiorski K. Information hiding using improper frame padding. Proceedings of 14th Internationl Telecommunication Network Strategy Planning Symposium (Networks). 2010. DOI: 10.1109/NETWKS.2010.5624901.
28. Banoci V., Bugar G., Levicky D. Steganography systems by using CDMA techniques. Proceedings of 19th International Conference Radioelektronika. 2009. pp. 183–186. DOI: 10.1109/RADIOELEK.2009.5158731.
29. Khalife J., Kassas Z.M. Navigation with Cellular CDMA Signals-Part II: Performance Analysis and Experimental Results. IEEE Transaction Signal Processing. 2018. vol. 66. no. 8. pp. 2204–2218. DOI: 10.1109/TSP.2018.2799166.
30. Hasan O., Tahar S. Performance analysis and functional verification of the stop-and-wait protocol in HOL. Journal Automation Reason. 2009. vol. 42. no. 1. pp. 1–33. DOI: 10.1007/s10817-008-9105-6.
31. Shukla V., Chaturvedi A., Srivastava N. A Secure Stop and Wait Communication Protocol for Disturbed Networks. Wireless Communication. 2020. vol. 110. no. 2. pp. 861–872. DOI: 10.1007/s11277-019-06760-w.
32. Kim B., Lee B., Cho J. ASRQ: Automatic segment repeat request for IEEE 802.15.4-based WBAN. IEEE Sensor Journal. 2017. vol. 17. no. 9. pp. 2925–2935. DOI: 10.1109/JSEN.2017.2676163.
33. Martins D., Guyennet H. Steganography in MAC Layers of 802.15.4 Protocol for Securing Wireless Sensor Networks. International Conference on Multimedia Information Networking and Security. 2010. pp. 824–828. DOI: 10.1109/MINES.2010.175.
34. Xue P.F., Hu J.S., Liu H.L., Hu R.G. A new network steganographic method based on the transverse multi-protocol collaboration. Journal Information Hiding Multimedia Signal Processing. 2017. vol. 8. no. 2. pp. 445–459.
35. Maya A. Steganology and information hiding: Stegop2py: embedding data in TCP and IP headers. Centria University of Applied Science. 2021. 59 p.
36. Maulana B., Rahim R. Go-Back-N Arq Approach for Identification and Repairing Frame in Transmission Data. International Journal Resource Science Engineering. 2016. vol. 2. no. 6. pp. 208–212.
37. Bedi P., Dua A. ARPNetSteg: Network steganography using address resolution protocol. International Journal Electronic Telecommunication. 2020. vol. 66. no. 4. pp. 671–677. DOI: 10.24425-ijet.2020.134026/769.
38. Schmidbauer T., Wendzel S., Mileva A., Mazurczyk W. Introducing Dead Drops to Network Steganography using ARP-Caches and SNMP-Walks. Proceedings of the 14th International Conference on Availability, Reliability and Security. 2019. pp. 1–10. DOI: 10.1145/3339252.3341488.
39. Llamas D., Miller A., Allison C. Covert channels in internet protocols: A survey. Proceedings of the 6th Annual Postgraduate Symposium about the Convergence of Telecommunications, Networking and Broadcasting, PGNET. 2005. vol. 2005.
40. Bobade S., Goudar R. Secure data communication using protocol steganography in IPv6. Proceedings of the 1st International Conference on Computing Communication Control and Automation (ICCUBEA). 2015. pp. 275–279. DOI: 10.1109/ICCUBEA.2015.59.
41. Miller P. Applying Steganography to Standard Network Traffic. Proceedings of the 4th Winona Computer Science Undergraduate Research Symposium. 2004. pp. 3–6.

42. Xue P.F., Hu J.S., Hu R.-G., Liu H.-L., Gu Y. A new DHT: Network steganography based on distributed coding. Journal of Information Hiding and Multimedia Signal Processing. 2018. vol. 9. no. 2. pp. 355–369.
43. Mazurczyk W., Smolarczyk M., Szczypiorski K. On information hiding in retransmissions. Telecommunication System. 2013. vol. 52. no. 2. pp. 1113–1121. DOI: 10.1007/s11235-011-9617-y.
44. Mazurczyk W., Smolarczyk M., Szczypiorski K. Retransmission steganography applied. Proceedings of 2nd International Conference on Multimedia Information Networking and Security. 2010. pp. 846–850. DOI: 10.1109/MINES.2010.179.
45. Siddiqui F., Zeadally S. Stream control transmission protocol (SCTP). Encyclopedia Internet Technology Application. 2007. pp. 575–582. DOI: 10.4018/978-1-59140-993-9.ch081.
46. Mazurczyk W., Szczypiorski K. Steganography of VoIP streams, Lecture Notes Computer Science. 2008. vol. 5332. LNCS, no. PART 2, pp. 1001–1018. DOI: 10.1007/978-3-540-88873-4_6.
47. Lubacz J., Mazurczyk W., Szczypiorski K. Principles and overview of network steganography. IEEE Communications Magazine. 2014. vol. 52(5). pp. 225–229.
48. Hamdaqa M., Tahvildari L. ReLACK: A reliable VoIP steganography approach. Proceedings of 5th International Conference Security Software Integration Reliability Improvement. 2011. pp. 189–197. DOI: 10.1109/SSIRI.2011.24.
49. Na S., Yoo S. Allowable Propagation Delay for VoIP Calls. International Workshop on Advanced Internet Services and Applications. 2002. pp. 47–55.
50. Bak P., Bieniasz J., Krzeminski M., Szczypiorski K. Application of perfectly undetectable network steganography method for malware hidden communication. 4th International Conference Frontier Signal Processing (ICFSP). 2018. pp. 34–38. DOI: 10.1109/ICFSP.2018.8552057.
51. Mills D.L. A brief history of NTP time: Memoirs of an Internet timekeeper. Computer Communication Reverse. 2003. vol. 33. no. 2. pp. 9–21. DOI: 10.1145/956981.956983.
52. Schmidbauer T., Wendzel S. Covert storage caches using the NTP protocol. Proceedings of the 15th International Conference on Availability, Reliability and Security. 2020. DOI: 10.1145/3407023.3409207.
53. Wang M., Gu W., Ma C. A Multimode Network Steganography for Covert Wireless Communication Based on BitTorrent. Security Communication Networks. 2020. vol. 2020. DOI: 10.1155/2020/8848315.
54. K Shah M., Virparia A.M., Sharma K. An Overview of Advanced Network Steganography. International Journal Computer Application. 2015. vol. 118. no. 21. pp. 23–26. DOI: 10.5120/20871-3364.
55. Dimitrova B., Mileva A. Steganography of Hypertext Transfer Protocol Version 2 (HTTP/2). Journal of Computer Communication. 2017. vol. 05. no. 05. pp. 98–111. DOI: 10.4236/jcc.2017.55008.
56. Collins J., Agaian S. Trends Toward Real-Time Network Data Steganography. International Journal Network Security and Its Applications. 2016. vol. 8. no. 2. pp. 01–21. DOI: 10.5121/ijnsa.2016.8201.
57. Drzymała M., Szczypiorski K., Urbański M.Ł. Network Steganography in the DNS Protocol. International Journal of Electronic and Telecommunications. 2016. vol. 62. no. 4. pp. 343–346. DOI: 10.1515/eletel-2016-0047.
58. Nazari M., Tarahomi S., Aliabady S. A Lightweight Adaptable DNS Channel for Covert Data Transmission. arXiv preprint arXiv:2003.14094. 2020.
59. Bormann C., Castellani A.P., Shelby Z. CoAP: An application protocol for billions of tiny internet nodes. IEEE Internet Computing. 2012. vol. 16. no. 2. pp. 62–67. DOI: 10.1109/MIC.2012.29.

60. Mileva A., Velinov A., Stojanov D. New Covert Channels in Internet of Things. 12th International Conference on Emerging Security Information, Systems and Technologies. 2018. pp. 30–36.
61. Patuck R., Hernandez-Castro J. Steganography using the Extensible Messaging and Presence Protocol (XMPP). arXiv:1310.0524. 2013. DOI: 10.48550/arXiv.1310.0524.
62. Ciobanu R.I., Tirsa M.O., Lupu R., Stan S., Andreica M.I. SCONeP: Steganography and Cryptography approach for UDP and ICMP. Proceedings of RoEduNet IEEE International Conference. 2011. pp. 1–6. DOI: 10.1109/RoEduNet.2011.5993700.
63. Alishavandi A.M., Fakhredanesh M. MKIPS: MKI-based protocol steganography method in SRTP. ETRI Journal. 2021. vol. 43. no. 3. pp. 561–570. DOI: 10.4218/etrij.2018-0410.
64. Castiglione A., De Santis A., Fiore U., Palmieri F. E-mail-based covert channels for asynchronous message steganography. Proceedings of 5th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computer. 2011. pp. 503–508. DOI: 10.1109/IMIS.2011.133.
65. Lucena N.B., Pease J., Yadollahpour P., Chapin S.J. Syntax and Semantics-Preserving Application-Layer Protocol Steganography. Information Hiding: 6th International Workshop. 2004. pp. 164–179. DOI: 10.1007/978-3-540-30114-1_12.
66. Ali A.H., Mokhtar M.R., George L.E. Recent approaches for VoIP steganography. Indian Journal Science Technology. 2016. vol. 9. no. 38. DOI: 10.17485/ijst/2016/v9i38/101283.
67. Mazurczyk W. VoIP steganography and its detection – a survey. ACM Computer Surve s. 2013. vol. 46. no. 2. DOI: 10.1145/2543581.2543587.
68. Wang C., Wu Q. Information hiding in real-time VoIP streams. Proceedings of the 9th IEEE International Symposium Multimedia (2007). 2007. pp. 255–262. DOI: 10.1109/ISM.2007.33.
69. Xu T., Yang Z. Simple and effective speech steganography in G.723.1 low-rate codes. 2009 International Conference on Wireless Communication and Signal Processing. 2009. pp. 1–5. DOI: 10.1109/WCSP.2009.5371745.
70. Ito A., Suzuki Y. Information hiding for G.711 speech based on substitution of least significant bits and estimation of tolerable distortion. IEICE Transaction Fundamentals of Electronics, Communications and Computer Science. 2010. vol. 93. no. 7. pp. 1279–1286. DOI: 10.1587/transfun.E93.A.1279.
71. Tian H., Zhou K., Jiang H., Huang Y., Liu J., Feng D. An adaptive steganography scheme for voice over IP. Proceedings of the IEEE International Symposium on Circuits Systems. 2009. pp. 2922–2925. DOI: 10.1109/ISCAS.2009.5118414.
72. Miao R., Huang Y. An approach of covert communication based on the adaptive steganography scheme on voice over IP. IEEE International Conference on Communications (ICC). 2011. DOI: 10.1109/icc.2011.5962657.
73. Tian H., Zhou K., Huang Y., Feng D., Liu J. A covert communication model based on least significant bits steganography in voice over IP. Proceeding of the 9th International Conference for Young Computer Scientists. 2008. pp. 647–652. DOI: 10.1109/ICYCS.2008.394.
74. Janicki A., Mazurczyk W., Szczypiorski K. Steganalysis of transcoding steganography. annals of telecommunications-annales des télécommunications. 2014. vol. 69. pp. 449–460.
75. Goher S., Javed B., Saqib N. Covert channel detection: A survey-based analysis. High-Capacity Optical Networks and Emerging/Enabling Technologies. 2012. pp. 057–065.
76. Wu Z., Guo J., Zhang C., Li C. Steganography and steganalysis in voice over ip: A review. Sensors. 2021. vol. 21. no. 4.

77. Neubert T., Caballero Morcillo A.J., Vielhauer C. Improving Performance of Machine Learning based Detection of Network Steganography in Industrial Control Systems. Proceedings of the 17th International Conference on Availability, Reliability and Security. 2022. pp. 1–8.
78. Zhang X.-G., Yang G.-H., Ren X.-X. Network steganography based security framework for cyber-physical systems. Information Sciences. 2022. vol. 609. pp. 963–983.
79. Tymchenko O., Havrysh B. Steganography in TCP/IP Networks. International Conference of Artificial Intelligence, Medical Engineering, Education. 2023. pp. 47–56.
80. Chai H., Li Z., Li F., Zhang Z. An end-to-end video steganography network based on a coding unit mask. Electronics. 2022. vol. 11. no. 7. pp. 1142.
81. Olawoyin L.A., Abdul-Rahman M., Faruk N., Oloyede A., Adeniran C., Lasisi O., Sikiru I., Baba B.A. Hybridization of OFDM and Physical Layer Techniques for Information Security in Wireless System. SLU Journal of Science and Technology. 2023. vol. 6. no. 1, 2. pp. 21–29.
82. Rajesh S., Joshi A. Estimation of Transmission Bandwidth for VoIP Signals over IP Packet Transmission Network using Capacity Computing Method. IEEE International Conference on Integrated Circuits and Communication Systems (ICICACS). 2023. pp. 01–07. DOI: 10.1109/ICICACS57338.2023.10100177.
83. Pilania U., Tanwar R., Zamani M., Manaf A.A. Framework for video steganography using integer wavelet transform and JPEG compression. Future Internet. 2022. vol. 14(9). pp. 1–16. DOI: 10.3390/fi14090254.
84. Pilania U., Kumar M., Kaur G. Region of Interest Using Viola-Jones Algorithm for Video Steganography. Applied Computational Technologies: Proceedings of ICCET 2022. 2022. pp. 405–415. DOI: 10.1007/978-981-19-2719-5_38.

Pilania Urmila — Ph.D., Associate professor, Department of computer science and technology, Manav Rachna University. Research interests: computer vision, image processing, information security. The number of publications — 25. urmilapilania@gmail.com; Aravali Hills, Faridabad, 121004, Haryana, India; office phone: +91(129)419-8000.

Kumar Manoj — Ph.D., Associate professor, Department of computer science and technology, Manav Rachna University. Research interests: computer vision, image processing, machine learning. The number of publications — 21. manojattri003@gmail.com; Aravali Hills, Faridabad, 121004, Haryana, India; office phone: +91(129)419-8000.

Rohit Tanwar — Ph.D., Associate professor, Department of computer science and technology, University of Petroleum and Energy Studies. Research interests: information security, machine learning. The number of publications — 80. rohit.tanwar.cse@gmail.com; P.O. Kandoli (Via Prem Nagar), Dehradun, 248007, Uttarakhand, India; office phone: +91(999)225-7914.

Nandal Neha — Ph.D., Associate professor of the department, Department of computer science and engineering, Geethanjali College of Engineering and Technology. Research interests: machine learning, deep learning, pattern recognition, data mining. The number of publications — 22. nehanandal012@gmail.com; Medchal, Cheeryal, 501301, Hyderabad, Telangana, India; office phone: +91(720)771-4441.

DOI 10.15622/ia.22.5.6

У. Пилания, М. Кумар, Т. Рохит, Н. Нандал

КРАТКИЙ ОБЗОР МЕТОДОВ СЕТЕВОЙ СТЕГАНОГРАФИИ

Пилания У., Кумар М., Рохит Т., Нандал Н. **Краткий обзор методов сетевой стеганографии.**

Аннотация. Цифровые мультимедийные файлы 2D и 3D обладают многочисленными преимуществами, такими как отличное качество, сжатие, редактирование, надежное копирование и т. д. С другой стороны, эти качества мультимедийных файлов являются причиной опасений, в том числе боязни получить доступ к данным во время общения. Стеганография играет важную роль в обеспечении безопасности передаваемых данных. Изменение типа файла покрытия с цифровых мультимедийных файлов на протоколы повышает безопасность системы связи. Протоколы являются неотъемлемой частью системы связи, и эти протоколы также могут использоваться для сокрытия секретных данных, что снижает вероятность их обнаружения. Этот документ призван помочь улучшить существующие методы сетевой стеганографии за счет увеличения пропускной способности и снижения скорости обнаружения путем анализа предыдущей связанной работы. Были изучены, проанализированы и обобщены последние статьи о методах сетевой стеганографии за последний 21 год. Этот обзор может помочь исследователям понять существующие тенденции в методах сетевой стеганографии, чтобы продолжить работу в этой области для улучшения алгоритмов. Статья разделена по уровням модели OSI.

Ключевые слова: сетевая стеганография, модель взаимосвязи открытых систем, протокол, пропускная способность, возможности внедрения, физический уровень, канальный уровень, сетевой уровень, уровень передачи, прикладной уровень.

Литература

1. Mortazavian P., Jahangiri M., Fatemizadeh E. A Low-Degradation Steganography Model for Data Hiding in Medical Images. Proceedings of the Fourth Lasted International Conference Visualization, Imaging and Image Processing. 2004. pp. 914–920.
2. Smolarczyk M., Szczypiorski K., Pawluk J. Multilayer detection of network steganography. Electronics. 2020. vol. 9. no. 12. pp. 1–14. DOI: 10.3390/electronics9122128.
3. Szczypiorski K. HICCUPS: Hidden communication system for corrupted networks. Internation Multi-Conference Advance Computing System. 2003. pp. 31–40.
4. Sekhar A., Kumar G.M., M A.R. A Novel Approach for Hiding Data in Videos Using Network Steganography Methods. Procedia Computer Science. 2015. vol. 7. no. 4. pp. 49–61. DOI: 10.5121/ijwmn.2015.7404.
5. Almohammedi A.A., Shepelev V. Saturation Throughput Analysis of Steganography in the IEEE 802.11p Protocol in the Presence of Non-Ideal Transmission Channel. IEEE Access. 2021. vol. 9. pp. 14459–14469. DOI: 10.1109/ACCESS.2021.3052464.
6. Seo J.O., Manoharan S., Mahanti A. A Discussion and Review of Network Steganography. IEEE 14th International Confernce Pervasive Intelligent Computer. 2016. pp. 384–391. DOI: 10.1109/DASC-PICom-DataCom-CyberSciTec.2016.80.
7. Ouda A.H., El-Sakka M.R. A step towards practical steganography systems. Lecture Notes Computer Science. LNCS. 2005. vol. 3656. pp. 1158–1166. DOI: 10.1007/11559573_140.

8. Tanwar R., Pilania U., Zamani M., Manaf A.A. An Analysis of 3D Steganography Techniques. Electronics. 2021. vol. 10. no. 19. p. 2357. DOI: 10.3390/electronics10192357.
9. Nair A.S., Kumar A., Sur A., Nandi S.иLength based network steganography using UDP protocol. IEEE 3rd International Conference Communication Software Networks, ICCSN 2011. 2011. pp. 726–730. DOI: 10.1109/ICCSN.2011.6014994.
10. Zander S., Armitage G., Branch P. A survey of covert channels and countermeasures in computer network protocols. IEEE Communications Surveys and Tutorials 2007. vol. 9. no. 3. pp. 44–57.
11. Huang Z., Sun X., Luo J., Wang J. Security Against Hardware Trojan Attacks Through a Novel Chaos FSM and Delay Chains Array PUF Based Design Obfuscation Scheme. Lecture Notes Computer Science. 2015. vol. 9483. pp. 14–24. DOI: 10.1007/978-3-319-27051-7.
12. Bedi P., Dua A. Network Steganography using the Overflow Field of Timestamp Option in an IPv4 Packet. Procedia Computer Science. 2020. vol. 171. pp. 1810–1818. DOI: 10.1016/j.procs.2020.04.194.
13. Pilania U., Tanwar R., Gupta P. Stable High Capacity Video Steganography in Wavelet Domain. Turkish Journal of Computer and Mathematics Education Research Article. 2021. vol. 12. no. 7. pp. 2142–2158.
14. Pilania U. A Proposed Optimized Steganography Technique using ROI, IWT and SVD. International Journal of Information Systems and Management Science. 2018. pp. 313–318.
15. Zielińska E., Mazurczyk W., Szczypiorski K. Trends in steganography. Communication ACM. 2014. vol. 57. no. 3. pp. 86–95. DOI: 10.1145/2566590.2566610.
16. Zielińska E., Mazurczyk W., Szczypiorski K. Developement Trends in steganography. Communication ACM. 2014. vol. 57. no. 3. pp. 86–95. DOI: 10.1145/2566590.2566610.
17. Amirtharajan R., Rayappan J.B.B. Steganography-time to time: A review. Journal Information Technology. 2013. vol. 5. no. 2. pp. 53–66. DOI: 10.3923/rjit.2013.53.66.
18. Theodore G., Maxwell T., Sandford I.I. Hiding data in the OSI network model. Lecture Notes Computer Science. 1996. vol. 1174. pp. 24–38. DOI: 10.1007/3-540-61996-8_29.
19. Frikha L., Trabelsi Z. A new Covert channel in WIFI networks. Proceeding 2008 3rd International Conference on Risks and Security of Internet and Systems. 2008. pp. 255–260. DOI: 10.1109/CRISIS.2008.4757487.
20. Martins D., Guyennet H. Attacks with Steganography in PHY and MAC Layers of 802.15.4 Protocol. Fifth International Conference on Systems and Networks Communications. 2010. DOI: 10.1109/ICSNC.2010.11.
21. Shah D.C., Rindhe B.U., Narayankhedkar S.K. Effects of cyclic prefix on OFDM system. Proceeding of International Conference and Workshop on Emerging Trends in Technology (ICWET). 2010. pp. 420–424. DOI: 10.1145/1741906.1741996.
22. Grabski S., Szczypiorski K. Steganography in OFDM symbols of fast IEEE 802.11n networks. IEEE Security and Privacy Workshops. 2013. pp. 158–164. DOI: 10.1109/SPW.2013.20.
23. Szczypiorski K., Mazurczyk W. Steganography in IEEE 802.11 OFDM symbols. Security and Communication Networks. 2016. vol. 9. no. 2. pp. 118–129. DOI: 10.1002/sec.306.
24. Khan M.N., Ghauri S. The WiMAX 802.16e Physical Layer Model. IET Conference on Wireless, Mobile and Multimedia Networks. 2008. pp. 117–120. DOI: 10.1049/cp:20080159.

25. Grabska I., Szczypiorski K. Steganography in WiMAX networks. 5th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT). 2013. pp. 20–27. DOI: 10.1109/ICUMT.2013.6798399.
26. Hussain I., Negi M.C., Pandey N. Security in ZigBee Using Steganography for IoT Communications. System Performance and Management Analytics. 2019. pp. 217–227.
27. Jankowski B., Mazurczyk W., Szczypiorski K. Information hiding using improper frame padding. Proceedings of 14th Internationl Telecommunication Network Strategy Planning Symposium (Networks). 2010. DOI: 10.1109/NETWKS.2010.5624901.
28. Banoci V., Bugar G., Levicky D. Steganography systems by using CDMA techniques. Proceedings of 19th International Conference Radioelektronika. 2009. pp. 183–186. DOI: 10.1109/RADIOELEK.2009.5158731.
29. Khalife J., Kassas Z.M. Navigation with Cellular CDMA Signals-Part II: Performance Analysis and Experimental Results. IEEE Transaction Signal Processing. 2018. vol. 66. no. 8. pp. 2204–2218. DOI: 10.1109/TSP.2018.2799166.
30. Hasan O., Tahar S. Performance analysis and functional verification of the stop-and-wait protocol in HOL. Journal Automation Reason. 2009. vol. 42. no. 1. pp. 1–33. DOI: 10.1007/s10817-008-9105-6.
31. Shukla V., Chaturvedi A., Srivastava N. A Secure Stop and Wait Communication Protocol for Disturbed Networks. Wireless Communication. 2020. vol. 110. no. 2. pp. 861–872. DOI: 10.1007/s11277-019-06760-w.
32. Kim B., Lee B., Cho J. ASRQ: Automatic segment repeat request for IEEE 802.15.4-based WBAN. IEEE Sensor Journal. 2017. vol. 17. no. 9. pp. 2925–2935. DOI: 10.1109/JSEN.2017.2676163.
33. Martins D., Guyennet H. Steganography in MAC Layers of 802.15.4 Protocol for Securing Wireless Sensor Networks. International Conference on Multimedia Information Networking and Security. 2010. pp. 824–828. DOI: 10.1109/MINES.2010.175.
34. Xue P.F., Hu J.S., Liu H.L., Hu R.G. A new network steganographic method based on the transverse multi-protocol collaboration. Journal Information Hiding Multimedia Signal Processing. 2017. vol. 8. no. 2. pp. 445–459.
35. Maya A. Steganology and information hiding: Stegop2py: embedding data in TCP and IP headers. Centria University of Applied Science. 2021. 59 p.
36. Maulana B., Rahim R. Go-Back-N Arq Approach for Identification and Repairing Frame in Transmission Data. International Journal Resource Science Engineering. 2016. vol. 2. no. 6. pp. 208–212.
37. Bedi P., Dua A. ARPNetSteg: Network steganography using address resolution protocol. International Journal Electronic Telecommunication. 2020. vol. 66. no. 4. pp. 671–677. DOI: 10.24425-ijet.2020.134026/769.
38. Schmidbauer T., Wendzel S., Mileva A., Mazurczyk W. Introducing Dead Drops to Network Steganography using ARP-Caches and SNMP-Walks. Proceedings of the 14th International Conference on Availability, Reliability and Security. 2019. pp. 1–10. DOI: 10.1145/3339252.3341488.
39. Llamas D., Miller A., Allison C. Covert channels in internet protocols: A survey. Proceedings of the 6th Annual Postgraduate Symposium about the Convergence of Telecommunications, Networking and Broadcasting, PGNET. 2005. vol. 2005.
40. Bobade S., Goudar R. Secure data communication using protocol steganography in IPv6. Proceedings of the 1st International Conference on Computing Communication Control and Automation (ICCUBEA). 2015. pp. 275–279. DOI: 10.1109/ICCUBEA.2015.59.

41. Miller P. Applying Steganography to Standard Network Traffic. Proceedings of the 4th Winona Computer Science Undergraduate Research Symposium. 2004. pp. 3–6.
42. Xue P.F., Hu J.S., Hu R.-G., Liu H.-L., Gu Y. A new DHT: Network steganography based on distributed coding. Journal of Information Hiding and Multimedia Signal Processing. 2018. vol. 9. no. 2. pp. 355–369.
43. Mazurczyk W., Smolarczyk M., Szczypiorski K. On information hiding in retransmissions. Telecommunication System. 2013. vol. 52. no. 2. pp. 1113–1121. DOI: 10.1007/s11235-011-9617-y.
44. Mazurczyk W., Smolarczyk M., Szczypiorski K. Retransmission steganography applied. Proceedings of 2nd International Conference on Multimedia Information Networking and Security. 2010. pp. 846–850. DOI: 10.1109/MINES.2010.179.
45. Siddiqui F., Zeadally S. Stream control transmission protocol (SCTP). Encyclopedia Internet Technology Application. 2007. pp. 575–582. DOI: 10.4018/978-1-59140-993-9.ch081.
46. Mazurczyk W., Szczypiorski K. Steganography of VoIP streams, Lecture Notes Computer Science. 2008. vol. 5332. LNCS, no. PART 2, pp. 1001–1018. DOI: 10.1007/978-3-540-88873-4_6.
47. Lubacz J., Mazurczyk W., Szczypiorski K. Principles and overview of network steganography. IEEE Communications Magazine. 2014. vol. 52(5). pp. 225–229.
48. Hamdaqa M., Tahvildari L. ReLACK: A reliable VoIP steganography approach. Proceedings of 5th International Conference Security Software Integration Reliability Improvement. 2011. pp. 189–197. DOI: 10.1109/SSIRI.2011.24.
49. Na S., Yoo S. Allowable Propagation Delay for VoIP Calls. International Workshop on Advanced Internet Services and Applications. 2002. pp. 47–55.
50. Bak P., Bieniasz J., Krzeminski M., Szczypiorski K. Application of perfectly undetectable network steganography method for malware hidden communication. 4th International Conference Frontier Signal Processing (ICFSP). 2018. pp. 34–38. DOI: 10.1109/ICFSP.2018.8552057.
51. Mills D.L. A brief history of NTP time: Memoirs of an Internet timekeeper. Computer Communication Reverse. 2003. vol. 33. no. 2. pp. 9–21. DOI: 10.1145/956981.956983.
52. Schmidbauer T., Wendzel S. Covert storage caches using the NTP protocol. Proceedings of the 15th International Conference on Availability, Reliability and Security. 2020. DOI: 10.1145/3407023.3409207.
53. Wang M., Gu W., Ma C. A Multimode Network Steganography for Covert Wireless Communication Based on BitTorrent. Security Communication Networks. 2020. vol. 2020. DOI: 10.1155/2020/8848315.
54. K Shah M., Virparia A.M., Sharma K. An Overview of Advanced Network Steganography. International Journal Computer Application. 2015. vol. 118. no. 21. pp. 23–26. DOI: 10.5120/20871-3364.
55. Dimitrova B., Mileva A. Steganography of Hypertext Transfer Protocol Version 2 (HTTP/2). Journal of Computer Communication. 2017. vol. 05. no. 05. pp. 98–111. DOI: 10.4236/jcc.2017.55008.
56. Collins J., Agaian S. Trends Toward Real-Time Network Data Steganography. International Journal Network Security and Its Applications. 2016. vol. 8. no. 2. pp. 01–21. DOI: 10.5121/ijnsa.2016.8201.
57. Drzymała M., Szczypiorski K., Urbański M.Ł. Network Steganography in the DNS Protocol. International Journal of Electronic and Telecommunications. 2016. vol. 62. no. 4. pp. 343–346. DOI: 10.1515/eletel-2016-0047.
58. Nazari M., Tarahomi S., Aliabady S. A Lightweight Adaptable DNS Channel for Covert Data Transmission. arXiv preprint arXiv:2003.14094. 2020.

59. Bormann C., Castellani A.P., Shelby Z. CoAP: An application protocol for billions of tiny internet nodes. IEEE Internet Computing. 2012. vol. 16. no. 2. pp. 62–67. DOI: 10.1109/MIC.2012.29.
60. Mileva A., Velinov A., Stojanov D. New Covert Channels in Internet of Things. 12th International Conference on Emerging Security Information, Systems and Technologies. 2018. pp. 30–36.
61. Patuck R., Hernandez-Castro J. Steganography using the Extensible Messaging and Presence Protocol (XMPP). arXiv:1310.0524. 2013. DOI: 10.48550/arXiv.1310.0524.
62. Ciobanu R.I., Tirsa M.O., Lupu R., Stan S., Andreica M.I. SCONeP: Steganography and Cryptography approach for UDP and ICMP. Proceedings of RoEduNet IEEE International Conference. 2011. pp. 1–6. DOI: 10.1109/RoEduNet.2011.5993700.
63. Alishavandi A.M., Fakhredanesh M. MKIPS: MKI-based protocol steganography method in SRTP. ETRI Journal. 2021. vol. 43. no. 3. pp. 561–570. DOI: 10.4218/etrij.2018-0410.
64. Castiglione A., De Santis A., Fiore U., Palmieri F. E-mail-based covert channels for asynchronous message steganography. Proceedings of 5th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computer. 2011. pp. 503–508. DOI: 10.1109/IMIS.2011.133.
65. Lucena N.B., Pease J., Yadollahpour P., Chapin S.J. Syntax and Semantics-Preserving Application-Layer Protocol Steganography. Information Hiding: 6th International Workshop. 2004. pp. 164–179. DOI: 10.1007/978-3-540-30114-1_12.
66. Ali A.H., Mokhtar M.R., George L.E. Recent approaches for VoIP steganography. Indian Journal Science Technology. 2016. vol. 9. no. 38. DOI: 10.17485/ijst/2016/v9i38/101283.
67. Mazurczyk W. VoIP steganography and its detection – a survey. ACM Computer Surve s. 2013. vol. 46. no. 2. DOI: 10.1145/2543581.2543587.
68. Wang C., Wu Q. Information hiding in real-time VoIP streams. Proceedings of the 9th IEEE International Symposium Multimedia (2007). 2007. pp. 255–262. DOI: 10.1109/ISM.2007.33.
69. Xu T., Yang Z. Simple and effective speech steganography in G.723.1 low-rate codes. 2009 International Conference on Wireless Communication and Signal Processing. 2009. pp. 1–5. DOI: 10.1109/WCSP.2009.5371745.
70. Ito A., Suzuki Y. Information hiding for G.711 speech based on substitution of least significant bits and estimation of tolerable distortion. IEICE Transaction Fundamentals of Electronics, Communications and Computer Science. 2010. vol. 93. no. 7. pp. 1279–1286. DOI: 10.1587/transfun.E93.A.1279.
71. Tian H., Zhou K., Jiang H., Huang Y., Liu J., Feng D. An adaptive steganography scheme for voice over IP. Proceedings of the IEEE International Symposium on Circuits Systems. 2009. pp. 2922–2925. DOI: 10.1109/ISCAS.2009.5118414.
72. Miao R., Huang Y. An approach of covert communication based on the adaptive steganography scheme on voice over IP. IEEE International Conference on Communications (ICC). 2011. DOI: 10.1109/icc.2011.5962657.
73. Tian H., Zhou K., Huang Y., Feng D., Liu J. A covert communication model based on least significant bits steganography in voice over IP. Proceeding of the 9th International Conference for Young Computer Scientists. 2008. pp. 647–652. DOI: 10.1109/ICYCS.2008.394.
74. Janicki A., Mazurczyk W., Szczypiorski K. Steganalysis of transcoding steganography. annals of telecommunications-annales des télécommunications. 2014. vol. 69. pp. 449–460.
75. Goher S., Javed B., Saqib N. Covert channel detection: A survey-based analysis. High-Capacity Optical Networks and Emerging/Enabling Technologies. 2012. pp. 057–065.

76. Wu Z., Guo J., Zhang C., Li C. Steganography and steganalysis in voice over ip: A review. Sensors. 2021. vol. 21. no. 4.
77. Neubert T., Caballero Morcillo A.J., Vielhauer C. Improving Performance of Machine Learning based Detection of Network Steganography in Industrial Control Systems. Proceedings of the 17th International Conference on Availability, Reliability and Security. 2022. pp. 1–8.
78. Zhang X.-G., Yang G.-H., Ren X.-X. Network steganography based security framework for cyber-physical systems. Information Sciences. 2022. vol. 609. pp. 963–983.
79. Tymchenko O., Havrysh B. Steganography in TCP/IP Networks. International Conference of Artificial Intelligence, Medical Engineering, Education. 2023. pp. 47–56.
80. Chai H., Li Z., Li F., Zhang Z. An end-to-end video steganography network based on a coding unit mask. Electronics. 2022. vol. 11. no. 7. pp. 1142.
81. Olawoyin L.A., Abdul-Rahman M., Faruk N., Oloyede A., Adeniran C., Lasisi O., Sikiru I., Baba B.A. Hybridization of OFDM and Physical Layer Techniques for Information Security in Wireless System. SLU Journal of Science and Technology. 2023. vol. 6. no. 1, 2. pp. 21–29.
82. Rajesh S., Joshi A. Estimation of Transmission Bandwidth for VoIP Signals over IP Packet Transmission Network using Capacity Computing Method. IEEE International Conference on Integrated Circuits and Communication Systems (ICICACS). 2023. pp. 01–07. DOI: 10.1109/ICICACS57338.2023.10100177.
83. Pilania U., Tanwar R., Zamani M., Manaf A.A. Framework for video steganography using integer wavelet transform and JPEG compression. Future Internet. 2022. vol. 14(9). pp. 1–16. DOI: 10.3390/fi14090254.
84. Pilania U., Kumar M., Kaur G. Region of Interest Using Viola-Jones Algorithm for Video Steganography. Applied Computational Technologies: Proceedings of ICCET 2022. 2022. pp. 405–415. DOI: 10.1007/978-981-19-2719-5_38.

Пилания Урмила — Ph.D., доцент, факультет компьютерных наук и технологий, Международный университет Манав Рахна. Область научных интересов: компьютерное зрение, обработка изображений, информационная безопасность. Число научных публикаций — 25. urmilapilania@gmail.com; Холмы Аравали, Фаридабад, 121004, Харьяна, Индия; р.т.: +91(129)419-8000.

Кумар Маной — Ph.D., доцент, факультет компьютерных наук и технологий, Международный университет Манав Рахна. Область научных интересов: компьютерное зрение, обработка изображений, машинное обучение. Число научных публикаций — 21. manojattri003@gmail.com; Холмы Аравали, Фаридабад, 121004, Харьяна, Индия; р.т.: +91(129)419-8000.

Рохит Танвар — Ph.D., доцент, департамент компьютерных наук и технологий, Университет нефтяных и энергетических исследований. Область научных интересов: информационная безопасность, машинное обучение. Число научных публикаций — 80. rohit.tanwar.cse@gmail.com; П.О. Кандоли (Прем-Нагар), Дехрадун, 248007, Уттаракханд, Индия; р.т.: +91(999)225-7914.

Нандал Неха — Ph.D., доцент кафедры, кафедра компьютерных наук и инженерии, Гитанджалиский инженерно-технологический колледж. Область научных интересов: машинное обучение, глубокое обучение, распознавание образов, интеллектуальный анализ данных. Число научных публикаций — 22. nehanandal012@gmail.com; Медчал, Чирил, 501301, Хайдарабад, Телангана, Индия; р.т.: +91(720)771-4441.