International Journal of Advanced Science and Technology
Vol. 29, No. 8s, (2020), pp. 304-313

# Implementation Of Quantum Steganography Based Encryption Using Grover Search

Uday Kiran K, Navya P, Dinakar R, Santhi H
[1,2,3]*M. Tech, Computer Science Engineering, specialization in Information Security,*
[4]*Associate Professor, School of Computer Science and Engineering, VIT University, Vellore-632014, India*
[1]*udaykiran.k2019@vitstudent.ac.in,*[2]*navya.2019@vit.student.ac.in2019@vitstudent.ac.in*
[3]*ratnakaram.dinakar2019@vitstudent.ac.in,*[4]*hsanthi@vit.ac.in*

***Abstract***

*Quantum picture steganography a most significant and secure communication nowadays. It is a sizeable metadata and Quantum picture steganography which is built on quantum picture enlargement. We propose a new algorithm. Then by using that algorithm we will find the position and angle where to store the data. Later it embeds the text in quantum picture version at certain point which will be conceal. The new algorithm consists mainly of 2 procedures hiding the message, pulls out data at same angle, and for decoding the data comparison of quantum picture with copy is done. As our algorithm or protocol will perceive an result with 2 security factors to data where there is superior undetectable, dependability.*

***Keywords:*** *Quantum picture enlargement, Grover search algorithm, QUANTUM PICTURE LOG-POLARI quantum picture representation, indiscernible, reliability, AES algorithm*

## 1. Introduction

Steganography, which depicts “covered wailing" masks the confidential data in digital pictures, audios, or videos. It is one of the principal techniques used in cryptography. Steganography depicts several frameworks, with different alternatives [1]. Several steganography techniques lack the power to maintain the confidentiality and security of data. These insignificances can be abolished by the introduction of a confidential key. Method of steganography was cxi sting centuries ago. It took several decades again to bring the same concept to implementation. As conventional steganography , explains the hiding of messages in pictures audios or videos, the integrity, and confidentiality of data should be maintained[2]. If the encryption and decryption of data is known. the access to these data will be effortless. The more the data is secure, the more it can be kept confidential. Now, each day sharing of pictures over the network is increasing in large numbers. Network security is becoming a necessity because of privacy and robustness where information transmitted has to maintained. Data hiding is a technique of hiding data in pictures, audio, and video. Here, we are focusing on picture steganography. It is used since knowledge pelting of information on pictures is required. Confidential information has embedded at an picture and it is transmitted[3].

Here, we are proposing a steganography framework in which the key data is encrypted within the digital picture so that only the approved person will be able to decrypt the data and restore the initial picture.

### Steganography Types

### Text steganography

Text steganography is obtained by the alteration of text format. It adds certain white spaces, changes the case from be send Qing several algorithms. The most basic one which is used is the LSB technique. The bit patterns of the picture are changed and the message is embedded into it. Pixels of the picture are being spotted so that the location for confidential data is obtained. The message with more data requires an picture with more size. Compression techniques are used in case if the picture size has to be reduced[4].

**Audio steganography**
Audio is chosen as the medium to embed confidential information. Changes are made in the audio signals in an undetectable manner. Steganography using audio signals is quite hard to implement. Infrasound or ultrasound range is used since the detection is not so straight forward. Digital audio is also an alternative to transmit the message [5-6].

**Physical steganography**
The message is embedded within the body of the picture [7].

**Digital steganography**
Messages are sent using the lowest bits of files [8].

**Printed steganography:**
Encryption of plain text, thereby producing the ciphertext. Methods adopted includes: Digital watermarking Encryption/decryption Authentication and Picture compression [9].

**Quantum steganography**
Steganography may be a method use to hide confidential data in normal data (ex., words, sound, picture, tape recording, etc). During the wrapper, where we implemented the latest quantum steganographic procedure by the use of plaintext as normal data called as hidden information [10]. The steganographic procedure has 3 main methods. Foremost, first we will try any normal text which is independent of confidential text send between sender and receiver [11]. Once we complete with stenography information, then we don't just change the content of plaintext in any respect. Secondly, hidden texts aren't attached in open info, but they are shown in phases [12].

The documentation is arranged in succeeding order. Section 2 discusses about introductory understanding of the new quantum picture steganography algorithm, which also includes about QUALPI picture shows an picture enlargement with decrypting method which uses the Grover search algorithm. Section 3 tells about system implementation of designed protocol. Section 4 is about the implementation of the algorithms. Section 5 is about outcomes obtained after the execution of the algorithm. The conclusion is shown in Section 6.

## 2. Literature Survey

Steganography may be a method stowing away confidential data inside innocent-looking data. amid the wrapper, were we have proposed an quantum steganographic convention utilizing normal content guilt-free data known as coat information. The steganography convention have 3 highlights. To begin with, ready to utilize any plaintext [13-14], that's autonomous with different confidential data send by 2 parties. once when we built steganographic information, were need not alter an substance with plaintext within the scarcest degree. Moment, inserted messages do not appear to be included in opened data, where they divided by stages with a snared condition. At long last, quantum conditions divided by 2 members parties ahead, a quantum key's utilized where clients recoup confidential data in stenographic information, not one or the other guilt-free info or data where confidential text contained. The wrapper which is being proposed in the quantum steganography convention implanting confidential messages to plain content. In common, steganography inserting confidential messages to plain content is harder than that of other cover information like picture information or sound information since we feel the plain content unusual whether or not the alteration is slight [15-16]. On the inverse hand[16], ready to utilize common plain content since the cover information utilized in our steganography convention. Subsequently, any busybody cannot choose whether the message is stego information or not. In addition, in spite of the fact that our convention must share snared states between parties ahead as quantum's key utilized where a clients recuperate confidential data which is in stenographic information, not one or the other guilt-free info or data in confidential text contains inside the states. By utilizing the property which will utilize any common plain content, a true blue party to boot able to have cover information made by a 3rd party, a 3rd party makes a normal content[17].

Quantum picture steganography is used in all the secure communications this paper aims on curiously large metadata quantum picture steganography convention upheld quantum picture development, and so the Grover look calculation is proposed. The modern calculation embraces quantum log-polar picture (QUANTUM PICTURE LOG-POLARI) representation [18-19], to orchestrate the quantum picture some time recently introduction of quantum extension method which makes an placing numerous picture duplicates in an indistinguishable measure point distinction since of the carrier. At that point confidential data in 1 quantum picture duplicate in an certain turn point encryption. To precisely extricate the key message inserted, the Grover look [20], an calculation is utilized to find the right quantum picture duplicate. bolstered the quantum vulnerability and quantum non-cloning hypotheses, the modern calculation cannot as it were accomplish great imperceptible, reliable too huge data because of great codes adaptability. Then unused convention primarily comprises of two prepare implanting and extricating confidential data. the strategy of inserting confidential info need a grow with an quantum picture in quantum extension procedure earlier, what can be spoken to by logpolars facilitates. After, that they chooses 1 picture duplicate with an implant a key data, where it needed to encoded a subjective point. With a method in extricating confidential info primarily employments the picture recovery backed Grover look calculation. Then copied the quantum's picture which contains confidential data is progressing to be recovered, so confidential information can be extricated through quantum picture comparison[21].

Quantum picture steganography is one of the secure communications. The complete architecture reliable component ought to cautious needed. The wrapper shows fresh system need confidential data, the haze Internet of Things. inside a system, where a client on 1 area implants the expensive information through the proposed quantum steganography convention and transfers the secured info that is haze internet technology. With expecting recipient on other area gets to a information in a mist remote locations also extricates in aiming substance through a propose extracted method. The wrapper moreover represents an interesting quantum steganographic convention bolstered hashes work, quantum entrapped conditions. there's no earlier quantum steganography convention that verifies an inserted confidential message. inside the recommended convention, the hash work is utilized to verify inserted confidential messages. The displayed convention an confidential on known assaults like text, MITM, No-text assaults[22]. The proposed approach is assigned to be utilized in haze and portable edge computing. The proposed convention doesn't utilize any additional quantum networks, quantum conditions other than it proposes convention with a transmission of keys text and confirm them. Then hashes work are utilized for confirming a reliable proposing convention[23].

Inserting confidential information into quantum carrier picture for clandestine communication is one in all significant inquire about fields of quantum secure communication. Utilizing great imperceptibility and tall implanting efficiency of lattice coding, this paper proposes a interesting network [24], coding-based quantum steganography calculation for quantum color pictures. To raised apply framework coding in genuine request, two distinctive implanting strategies are proposed. One inserting strategy is single pixel-embedded coding called as SPE coding. This strategy implants two quantum bits of confidential information into three slightest significant qubits of one pixel of quantum carrier picture, and at the foremost fair one LSQb would be changed. the inverse implanting strategy is different pixels-embedded coding called as MPSE coding, amid which three LSQbs of different carrier pixels are utilized to insert two confidential qubits. this paper plans a widespread quantum circuit for network coding and a committed quantum circuit for coding to raised get it the forms of implanting and extricating confidential data. By watching the picture quality comparison between carrier pictures conjointly the comparing stego pictures, calculating their PSNR values [25], comparing their histograms, and analyzing the results of quantum channel commotions and Eve attacks.

Data hiding points to insert secret data into the interactive media, like picture, sound, video, and content. amid this paper, 2 unused quantum data hiding approaches ar suggests. A quantum steganography approach is planned to hide quantum secret picture into a quantum cover picture.

The quantum secret picture is disorganized to start with using a controlled-NOT door maybe the safety of the planted data. The disorganized secret picture is planted into the quantum cowl picture utilizing the two most and slightest essential qubits. moreover, a quantum picture watermarking approach is exhibited to cowl a quantum watermark grey picture into a quantum carrier picture. The quantum watermark picture, that is mixed by utilizing Arnold's cat define, is at that time planted into the quantum carrier picture utilizing the two slightest and most important qubits. solely the watermarked picture in addition the key ar adequate free the inserted quantum watermark image. The planned oddity has been printed using a state of affairs of sharing therapeutic symbolism between 2 inaccessible healing centers. The reenactment and investigation illustrate that the two recently planned approaches have fabulous visual quality and tall embedding capability and security. to produce security, additional keys or any data round the cowl picture, or the key picture is needed[26-27].

In [28] the authors proposed the quantum steganography by combining quantum error-correcting codes with earlier ensnarement. In various steganographic ways, inserting secret messages in error-correcting codes could cause damage to them on the off probability that the inserted portion is debased. In any case, our projected steganography will severally build secret messages together the substance of canopy messages. The natural kind of the duvet message does not got to be altered for implanting secret messages. we tend to projected quantum steganography utilizing earlier entice. Our projected steganography combines quantum error-correcting codes with earlier ensnarement, that empowers creating secret messages and canopy messages severally. In common, steganographic ways for implanting secret messages in error-correcting codes influence their substance since they are inserted as a element of error-correcting codes. Our steganography utilizes earlier ensnarement. As of late, quantum codes utilizing earlier ensnarement known as entanglement-assisted quantum error-correcting codes square measure projected. These codes square measure a range of stabilizer quantum error-correcting codes.

Quantum steganography that utilizes the quantum mechanical impact to achieve the reason of information covering up may be a prevalent theme of quantum data. El Allati et al proposed a unused quantum steganography utilizing the GHZ4 state. Since all of the 8 bunches of unitary changes utilized within the key message encoding run the show alter the GHZ4 state into 6 instead of 8 distinctive quantum states when the around the world stage isn't considered, we point out that a 2-bit instead of a 3-bit confidential message may be encoded by one bunch of the given unitary changes [29]. To encode a 3-bit confidential message by performing a bunch of unitary changes on the GHZ4 state, we allow another 8 bunches of unitary changes which is able alter the GHZ4 state into 8 distinctive quantum states. since of the symmetry of the GHZ4 state, all the conceivable 16 groupsofunitarytransformationschangetheGHZ4 state into 8 distinctive quantum states, so the moved forward convention [30-32], accomplishes a tall efficiency.TheGHZ4 state could be a extraordinary state within the chart state family which has numerous curiously highlights, just like the thought-provoking hypothetical structure, non-locality, and de-coherence. Particularly, numerous of their ensnarement properties are closely related with their fundamental charts.

Data security becomes the most important role in computer science. Because keeping data secure from attackers is the most important task of insecure applications[34]. With the later huge assault base on cryptography plans and innovation trending into more capable computing of quantum computing, cryptography-based plans are enormously powerless and steganography the science of covered up communication utilizing cover media has gotten to be an critical investigate region in data security[35].

## 3. Proposed Work

We propose a Quantum Picture Steganography to Secure Data using Grover search algorithm Method. Quantum bit is represented in a vector form. It can represent as a Dirac notation are column vector. This algorithm gives a sensible speed advantage for unstructured search.

### *3.1. THE QUANTUM PICTURE LOG-POLARI REPLICA AND COMPOSITION QUANTUM PICTURE*

In 2013, Zhang's Yt. suggested the latest version on the Quatum log-polar picture model. The log picture polar with dimension 2m×2n and a grey level of 2^q can be shown as below[35].

$$|I\rangle = \frac{1}{\sqrt{2^{m+n}}} \sum_{\rho=0}^{2^m-1} \sum_{\theta=0}^{2^n-1} |g(\rho,\theta)\rangle \otimes |\rho\rangle \otimes |\theta\rangle \quad (1)$$

$$g(\rho,\theta) = C_0 C_1 \cdots C_{q-2} C_{q-1}, \; g(\rho,\theta) \in [0, 2^q - 1) \quad (2)$$

The revolving of Quantum log-polar picture model quantum pictures is used in the quantum picture required in this project. We primarily focus on the revolving and outward n-th hour. Where it can be performed 2k units rotations in quantum log-polar picture quantum picture as R2k.

### *3.2. Picture Expansion*

Quantum picture enlargement is lhe process expanding a picture to get and every picture can be moved with an theta point. This procedure with quantum picture enlargement can be repeated up to ith iteration in the process. For a coordinate of logs-polar picture quantum within the dimension 2m*2n along with grey height 2q, with ith rounds.

The main aim is to change picture 2^n-1-I pixels in revolving where the ith bits quantum with a serial number registered as |1>.

### *3.3. Proposed Algorithm*

We apply the cipher algorithm like caser encryption and decryption methods to convert plain text into ciphertext which is used to embed information into quantum enlarged picture. Later we use the same algorithm to decrypt the ciphertext to plain text.

Algorithm for generating Cipher Text:

1. Take a color picture.
2. Consider primary color components R, G, and B.
3. Consider the confidential message to be embedded.
4. Encrypt the confidential message using the Caser algorithm.
5. Consider the ciphertext and the confidential key.
6. Find the pixel location to embed the message by adding n" key with (n-1)" hey.
7. For further key generation perform n " key XOR (n-1)" key.

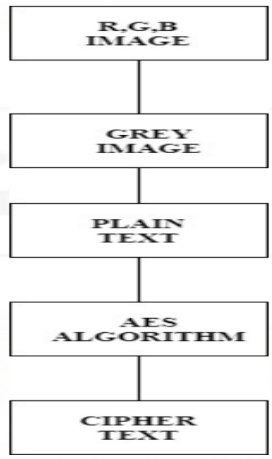
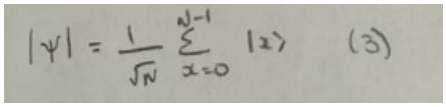



**Figure1. Workflow of Encryption Process**

### *3.4. Grover Search Algorithm*

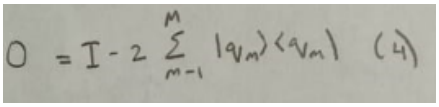
This search method is normally used in an unsorted data to find for N outputs which satisfy the certain conditions like f (n) = b where we can find the spacing with n(n =2n) info. This procedure for this method is as follows:

1. An amalgam of parallel bits of quantum. The Hadamard change should executed till nth round in starting condition within a serial registered numbers |X| for obtaining required result [27].



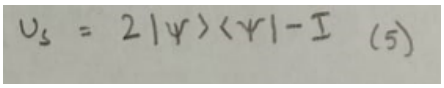
$$|\psi| = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle \quad (3)$$

2. We later apply Oracle Black box which is expressed below.



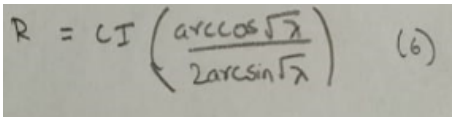
$$O = I - 2 \sum_{m-1}^{M} |q_m\rangle\langle q_m| \quad (4)$$

3. The Condition phase shift is performed as shown.



$$U_s = 2|\psi\rangle\langle\psi| - I \quad (5)$$

4. The process is repeated from 2 to 3 for n times till we get the required output.



$$R = CI\left(\frac{\arccos\sqrt{\lambda}}{2\arcsin\sqrt{\lambda}}\right) \quad (6)$$

5. We then perform measure registers & measure of quantum to find the output to the statement.

## 4. IMPLEMENTATION

The latest quantum picture steganography protocol with huge data or payload uses quantum enlargement and Grover search methods, it also includes two processes of encrypting and decrypting of secure data. The figure 2 shows the work flow of the proposed architecture.

### 4.1. The procedure for Encrypting the confidential data:

The procedure for encrypting the confidential data in the quantum carrier picture. We can obtain various quantum steganography pictures by shifting them from various points. Quantum picture expansion method is implemented to enlarge the picture and superimpose the carrier picture.
Later after enlarging the barrier picture as pic set superimposed, the confidential information can be hide in a specific picture in a chosen picture at an angle of θ1. But to programming rule, the confidential data can be presented by a certain angle of θ2. So, the procedure of encrypting the confidential data will convert the barrier picture copy's with an angle of θ1+θ1.

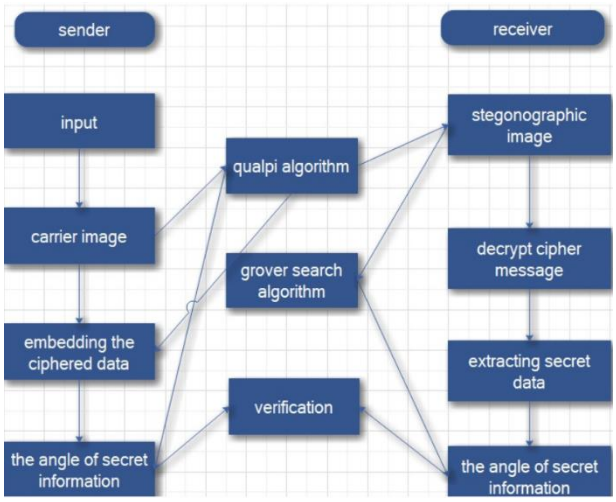



**Figure 2. Work Flow of Proposed architecture**

The following are the steps for encrypting the data:

1. First we consider a plain text as an input then by using shift the cipher we will encrypt the data and get the cipher text.
2. Later we store the ciphertext in the temp variable.
3. Then we consider an picture as a barrier and convert the picture into a grayscale picture using the OpenCV package.
4. We perform quantum picture enlargement process on the converted grayscale picture and later the picture is enlarged into a set of pictures that are moved in anticlockwise in a radial direction.

If the quantum picture has a resolution with 2m×2n, rounds then the procedure is repeated n times.

5. If the picture rotation angle is l in the enlargement procedure will be chosen as a barrier picture. Consider the angle is θ1 and the confidential data is embedded, then the rotational angle of the barrier picture after embedding the confidential data is θ+θ1+s.

This is the last stage for embedding the confidential data or data and we finally get the encrypted picture.

### 4.2. The procedure for Decrypting the confidential data:

The process response to extract secure data within the stenographic picture carrier. It retrieve the quantum extension map book by utilizing look instrument like Grover till the same picture is recovered. The strategy for recovering picture is as takes after:

1. By implementing the Grover search method we first process for retrieval of quantum picture to get the same picture which is used first for barrier picture.
2. After retrieval of the picture we will try to find the embedded confidential data from the barrier where picture is stored in the rotational angle.
3. By using the Grover algorithm we search for every pixel in the grayscale to get the ciphertext and we perform this step till we get all the encrypted data stored in the picture.
4. After getting ciphertext we will try to decrypt the ciphertext using the AES algorithm.
5. After decrypting the ciphertext we get the final confidential data that we have to give as an input.

## 5. Result and Discussion

This method consists of execution assessment indicators: security, undetectable, and size. Intangible implies the private data is scrambled at a theta point and afterward it is covered up in

any one of the barrier picture duplicate. This strategy guarantees the security of the confidential data amid the method of private data exchange, and the relaibility of information within the medium. Measure implies, the strategy of embedding private data which is covered up at a specific point.

(a) Actual Image Before Converting to greyscale

(b) Grey Scale image after conversion using opencv

(c) The actual image after expanding the image into 40 degree angle

(d) Final stego image of the original input

Figure 3. (a) Original picture of Mountains. (b)GrayScale picture of Mountains after conversion. (c) The original picture expanded at 40 degrees. (d) Stego picture after embedding the data.

## 6. Conclusion

The unused convention primarily comprises of two prepare: implanting and extricating confidential data strategy of inserting confidential data can be extended in quantm picture in quantum development method earliest, with spoken to by log-polars facilitates. With, that where that can choose 1 picture duplicate which can insert key data, which is encoded as an subjective point. the strategy of extricating confidential data basically employments the picture recovery backed Grover look calculation. The duplicate of quantum picture containing confidential data are attending to be recovered, at that point confidential data may be extricated between quantum picture comparing. With convention one can transfer the quantum picture nor as it were hides presence the confidential data, where too key data about inconceivable to be listened stealthily amid the transmission prepare. We concluded that private browsing modes in advanced browsers and inspected their victory at accomplishing the specified objectives of security. The hand worked and computerized testing tool pointed out a few vulnerability within the current plans. The foremost basic powerlessness is em-power the neighborhood programmer to totally overcome the benefits of private mode. At long last we found diverse issues of keeping browser expansions and plug-ins from destruction of private browsing objectives.

**References**

1. "Adaptive Batch Size Picture Merging Steganography and Quantized Gaussian Picture Steganography," in *IEEE Transactions on DataForensics and Security*, vol. 15, pp. 867-879, 2020.
2. K. Martin, ‘‘Steganographic communication with quantum information,’’ in Proc. Int. Workshop Inf. Hiding, Jun. 2007, pp. 32–49.
3. G. Mogos, ‘‘Stego quantum algorithm,’’ in Proc. Int. Symp. Comput. Sci. Appl., vol. 24, pp. 187–190, Oct. 2008.
4. Peng Meng, Liusheng Hang, Wei Yang and Zhili Chen, "Attacks on Translation Based Steganography," *2009 IEEE Youth Conference on Information, Computing and Telecommunication*, Beijing, 2009, pp. 227-230.
5. A. A. Z., A. W. Naji, S. A. Hameed, F. Othman, and B. B. Zaidan, "Approved Undetectable-Antivirus Steganography for Multimedia Datain PE-File," *2009 International Association of Computer Science and DataTechnology - Spring Conference*, Singapore, 2009, pp. 437-441.
6. P. Meng, L. Hang, W. Yang, Z. Chen and H. Zheng, "Linguistic Steganography Detection Algorithm Using Statistical Language Model," *2009 International Conference on DataTechnology and Computer Science*, Kiev, 2009, pp. 540-543.
7. H. Sun, C. Weng, C. Lee and C. Yang, "Anti-Forensics with Steganographic Data Embedding in Digital Pictures," in *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 7, pp. 1392-1403, August 2011.
8. Zhi-Hui Wang, The Duc Kieu, Chin-Chen Chang, and Ming-Chu Li, "Emoticon-based text steganography in chat," *2009 Asia-Pacific Conference on Computational Intelligence and Industrial Applications (PACIIA)*, Wuhan, 2009, pp. 457-460.
9. L. Kothari, R. Thakkar and S. Khara, "Data hiding on web using combination of Steganography and Cryptography," *2017 International Conference on Computer, Communications and Electronics (Comptelix)*, Jaipur, 2017, pp. 448-452.
10. Ran-Zan Wang and Yeh-Shun Chen, "High-payload picture steganography using two-way block matching," in *IEEE Signal Processing Letters*, vol. 13, no. 3, pp. 161-164, March 2006.
11. X. Zhang, S. Wang, and Z. Zhou, "Multibit Assignment Steganography in Palette Pictures," in *IEEE Signal Processing Letters*, vol. 15, pp. 553-556, 2008, doi: 10.1109/LSP.2008.2001117.
12. Tao Zhang, Wenxiang Li, Yan Zhang,, and Xijian Ping, "Detection of LSB matching steganography based on distribution of pixel differences in natural pictures," *2010 International Conference on Picture Analysis and Signal Processing*, Zhejiang, 2010, pp. 548-552, doi: 10.1109/IASP.2010.5476056.
13. L. Li and C. Cai, "Multiple description picture coding using dual-tree discrete wavelet transform," *2009 International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS)*, Kanazawa, 2009, pp. 655-658, doi: 10.1109/ISPACS.2009.5383887.
14. X. Zhang, F. Peng, and M. Long, "Robust Coverless Picture Steganography Based on DCT and LDA Topic Classification," in *IEEE Transactions on Multimedia*, vol. 20, no. 12, pp. 3223-3238.
15. L. Guo, J. Ni, and Y. Q. Shi, "Uniform Embedding for Efficient JPEG Steganography," in *IEEE Transactions on DataForensics and Security*, vol. 9, no. 5, pp. 814-825, May 2014.
16. S. Velliangiri, P. Karthikeyan & V. Vinoth Kumar (2020) Detection of distributed denial of service attack in cloud computing using the optimization-based deep networks, *Journal of Experimental & Theoretical Artificial Intelligence*, DOI: 10.1080/0952813X.2020.1744196
17. Praveen Sundar, P.V., Ranjith, D., Vinoth Kumar, V. et al. Low power area efficient adaptive FIR filter for hearing aids using distributed arithmetic architecture. *Int J Speech Technol* (2020). https://doi.org/10.1007/s10772-020-09686-y
18. Vinoth Kumar V, Karthikeyan T, Praveen Sundar P V, Magesh G, Balajee J.M. (2020). A Quantum Approach in LiFi Security using Quantum Key Distribution. *International Journal of Advanced Science and Technology*, 29(6s), 2345-2354.

19. Umamaheswaran, S., Lakshmanan, R., Vinothkumar, V. et al. New and robust composite micro structure descriptor (CMSD) for CBIR. *International Journal of Speech Technology* (2019), doi:10.1007/s10772-019-09663-0
20. Karthikeyan, T., Sekaran, K., Ranjith, D., Vinoth kumar, V., Balajee, J.M. (2019) "Personalized Content Extraction and Text Classification Using Effective Web Scraping Techniques", *International Journal of Web Portals (IJWP)*, 11(2), pp.41-52
21. Vinoth Kumar, V., Arvind, K.S., Umamaheswaran, S., Suganya, K.S (2019), "Hierarchal Trust Certificate Distribution using Distributed CA in MANET", *International Journal of Innovative Technology and Exploring Engineering*, 8(10), pp. 2521-2524
22. Maithili, K , Vinothkumar, V, Latha, P (2018). "Analyzing the security mechanisms to prevent unauthorized access in cloud and network security" *Journal of Computational and Theoretical Nanoscience*, Vol.15, pp.2059-2063.
23. V.Vinoth Kumar, Ramamoorthy S (2017), "A Novel method of gateway selection to improve throughput performance in MANET", *Journal of Advanced Research in Dynamical and Control Systems*,9(Special Issue 16), pp. 420-432
24. Dhilip Kumar V, Vinoth Kumar V, Kandar D (2018), "Data Transmission Between Dedicated Short-Range Communication and WiMAX for Efficient Vehicular Communication*" Journal of Computational and Theoretical Nanoscience*, Vol.15, No.8, pp.2649-2654
25. Kouser, R.R., Manikandan, T., Kumar, V.V (2018), "Heart disease prediction system using artificial neural network, radial basis function and case based reasoning" *Journal of Computational and Theoretical Nanoscience*, 15, pp. 2810-2817
26. Shalini A, Jayasuruthi L, Vinoth Kumar V, "Voice Recognition Robot Control using Android Device" *Journal of Computational and Theoretical Nanoscience*, 15(6-7), pp. 2197-2201