National Journal of Antennas and Propagation, ISSN: 2582-2659 Vol. 6, No.3, 2024 (pp. 53-59)
RESEARCH ARTICLE
HTTP://ANTENNAJOURNAL.COM

# Secure Communication in Cognitive Radio Networks: A Study on Encryption Techniques and Key Management Schemes

**Rajeev Kumar Bhaskar[1], Susovan Kumar Pan[2]**
[1]*Assistant Professor, Department of CS & IT, Kalinga University, Raipur, India.*
[2]*Assistant Professor,Department of CS & IT, Kalinga University, Raipur, India.*

*KEYWORDS:*
Cognitive Radio,
Communication,
Security,
Encryption.

*ARTICLE HISTORY:*
Received 21.09.2024
Revised 09.10.2024
Accepted 09.11.2024

*DOI:*
https://doi.org/10.31838/NJAP/06.03.07

## Abstract

In the current era of electronic networks, security is becoming more and more important globally. Data communication and security are significantly impacted by the network connection made possible by devices like computers and smartphones. There are numerous books that describe how to use encryption and data concealing to communicate securely. Both encryption and decryption have employed a variety of algorithms. By employing safe communication methods like watermarking, steganography, and cryptography, researchers have attained a respectable level of legitimacy in data transfer via networks. In order to obtain robustness against a variety of threats, it is evident that a higher degree of accomplishment is achievable in the fundamental aspects of secured communication, such as confidentiality, integrity, and availability. There are many tools to fill the research gap and improve the ability to hide data using different methods. Since there is still opportunity to get better as far as safeguarding computerized information, similar to pictures, numerous strategies have been created to implant a lot of data without causing perceptual mutilation and to accomplish heartiness against pressure, added substance commotion, and picture altering assaults, which limits clamor and further develops data concealing in pictures and recordings.

**Author's e-mail:** ku.rajeevkbhaskar@kalingauniversity.ac.in, ku.SusovanKumarPan@kalingauniversity.ac.in

**How to cite this article:** Bhaskar RK, Pan SK. Secure Communication in Cognitive Radio Networks: A Study on Encryption Techniques and Key Management Schemes. National Journal of Antennas and Propagation, Vol. 6, No. 3, 2024 (pp. 53-59).

## Introduction

The Cognitive Radio Network (CRN) archetypes viz. Cognitive Radio Ad hoc Networks (CRAHNs) and Cognitive Radio Industrial Internet of Things (CR-IIoTs), facilitate an efficacious and optimum utilization of the sporadically used licensed radio frequency (RF) spectrum in a distributed network system. In order to reach a consensus on spectrum decisions regarding the presence or absence of licensed primary users (PUs), one of the main requirements of Cognitive Radio (CR) network archetypes is their proficient competency in spectrum sensing, i.e., scanning the entire sparsely utilised radio frequency spectral band.[1] The CR network archetypes enable opportunistic and dynamic licensed radio spectrum access to unlicensed cognitive secondary users (SUs) with minimal interference to licensed primary users (PUs) by integrating software-defined radio (SDR) technology, autonomic and secure communication protocols, and artificial intelligence techniques for distributed consensus. Additionally, statistical analysis is performed to determine the appropriateness of the accessible, underutilised spectrum bands for cognitive communications. In order to anticipate and identify the most suitable radio spectrum band, statistical characteristics such as signal-to-noise ratio, link error rate, delays, interference, and holding time are frequently used.[2, 11] Only after the spectrum choice forecasts the absence of PUs and the corresponding sporadic radio spectrum bands have been identified does the transmission of SUs take place. The cognitive SUs in a dispersed SU-Network must promptly leave the associated spectrum band if they notice the PU's transmission activity.[16] They must then search for another available spectrum band. The Spectrum

Handoff mechanism is the process by which unlicensed cognitive SUs transfer the licensed spectrum band to the licensed PU. An unfavourable event that involves a class of collusive adversaries purposefully disrupting or corrupting lawful session communications is known as an active network security assault in the context of the CRN system. assaults on network security are usually divided into two groups: active assaults and passive attacks. A malevolent SU or opponent often initiates an active assault by first logging and preserving the communication session settings.[3] Additionally, an adversary sends phoney session information in an attempt to compromise the real system. In order to take complete control of the cognitive network sessions, the adversary nodes might also try to get real and valid session answers from the participating SUs. Rather of engaging with the session participants, the passive attacker attempts to intercept and obtain secure session parameters from established and authenticated communication sessions. The majority of the time, network security and cryptography threats that take advantage of Cognitive Radio's capabilities are active.[14]

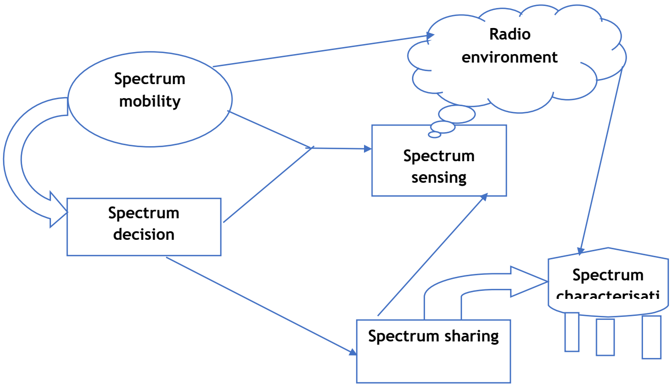

**Fig. 1: Radio Spectrum Management Lifecycle**

## Related work

In order to protect data from unauthorised access, information and data concealment has become crucial for both government and commercial sectors in recent years. Ensuring privacy and information integrity during advanced digital communication is the primary concern of architects, engineers, and assessors.[4, 12] As a result, the application of digital steganography in secure communication has captivated academics and developers. Video steganography has become more useful for blind extraction, allowing for the uninterrupted delivery of enormous amounts of data. Video steganography's application has been driven by its compressibility, simplicity, and speed. The crucial factors to be taken into account when using steganography for secret communication were covered in advance. In the subject of systems administration, secure data transmission is essential. The goal of algorithm development has been to provide confirmed covert data transmission through the system. Numerous secret specialised systems exist, such as steganography, cryptography, reversible data concealment, and others. The data bits that the non-proposed beneficiary cannot study are jumbled by cryptographic computations.[42] The process of inserting private information into the host medium is known as hidden correspondence. There are two steps in this process. The problem with this approach is that unique data in the spread medium cannot be recovered. First, the data is hidden in the spread medium, and then the data is recovered.[5] This is because the insertion operation causes the host medium substance to become permanently twisted while the payload substance is being removed. Yet, in some basic applications like restorative imaging, military imaging, satellite imaging, law criminological and so on, even host media carries some crucial data. Therefore, bending with respect to the host medium substance is not allowed. The primary task is to suggest novel secure communication techniques that might be used for sharing various multimedia files. These techniques should be capable of delivering high security, resilience and good embedding capacity to store the payload data into cover media.

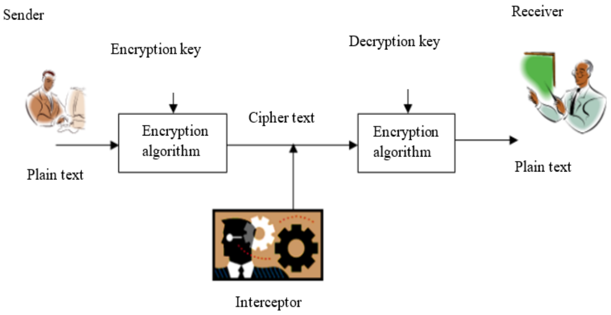

**Fig. 2: Conventional secure communication**

In order to truly quantify security taking into account unique cryptographic and steganographic attacks, the investigation aims to conduct flawlessly undetectable correspondence over open correspondence channels. A variety of multimedia files, such as audio, video, and image groups, are regarded as the concealed data to create information concealing systems using just an image or a group of images as the host medium. [6][13].

1. To put effective data hiding technology into use, since there is still much room for advancement in protecting digital data from hackers through the use of watermarking, steganography, and cryptography.
2. To further develop the inserting limit and PSNR and accomplish vigor against pressure and added

substance commotion assaults overwhelmingly of data into an image without bringing on any perceptual twisting.

3. To create steganographic methods that might protect the stego-signal from statistical steganalysis.
4. To reduce noise to improve information concealment in pictures and videos

"Data Shuffling," often called "Data Masking," is the process of rearranging the original data or information in columns. The knight visit is a numerical method that decides a knight's move design on a chessboard when the knight shows up on each square just once. The S-Box technique is used to shuffle the secret image, and pixels chosen by applying the "Least Significant Bit (LSB)" replacement scheme are used to conceal it in the cover image.

## Overview ofproposed Framework

Data security, which can be achieved by appropriate education, awareness, and technology use, is the protection of privacy, accuracy, and accessibility of information resources while utilising, storing, or transferring data. The process of concealing the original data with modified information is known as data masking.[7] Protecting sensitive data from malevolent hackers is the main objective of data concealing. The data must also have a genuine appearance, be consistent, and be usable for future use. In corporate systems where data is utilised for application development involving programming and coding, data masking is most prevalent. In order to transfer information from manufacturing systems to nonproduction systems and vice versa, businesses also use data concealing. Certain places, especially when it comes to billing, conceal information such card numbers based on user security permissions so that operators cannot see them on the screen. The most significant issue for a business is that employee data is not always protected, allowing unauthorised persons to steal it—a situation known as a security breach [8]. Thus, "Test Management Practice" should be closely linked to organisational information concealment.

## Data Shuffling

The process of shuffling involves arranging a level of data in a random manner, with the assurance that the shuffler has not deployed the result. This technique is very useful in many applications; for instance, it is possible to shuffle the original value of accounts in the database of a calendar of financial information by concealing the names of the suppliers, making it extremely difficult to reshuffle the original information back even with the knowledge of the original data values. The two most important algorithms used in data shuffling are Knight tour and Fisher Yates, which are mathematical methods for determining a knight's move sequence on a chessboard where the knight is positioned only once on each square.[9, 15] Suppose the knight stops on a square, it travels from the initial square immediately ensuing the same path. Varieties of the knight's visit issue include chessboards of unexpected sizes in comparison to the standard 8 × 8. The knight's move is similar to that of neural network and any problem in movement can be solved by employing the method of neural network. The path is built in a fashion that, every move of knight is symbolised by a neuron, and every neuron is set off with no obvious end goal in mind to be either dynamic or idle. The 'Fisher-Yates mix' is called after 'Ronald Fisher' and 'Forthright Yates' who at first portrayed it, and after 'Donald Knuth' is otherwise called the 'Knuth mix.' 'Sattolo's Calculation' is a variety of the Fisher-Yates mix that can be utilized to create irregular cyclic changes of length 'n' instead of irregular stages.[10, 17] A method for creating a finitely sequenced random permutation is the Fisher-Yates shuffle. Until there are no more elements, the procedure keeps selecting the next element at random.. It produces a balanced permutation in such a way that every permutation is equally possible.

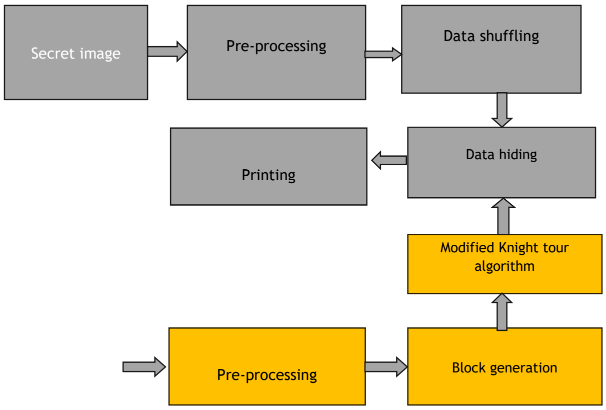

Fig. 3: Proposed Framework 1

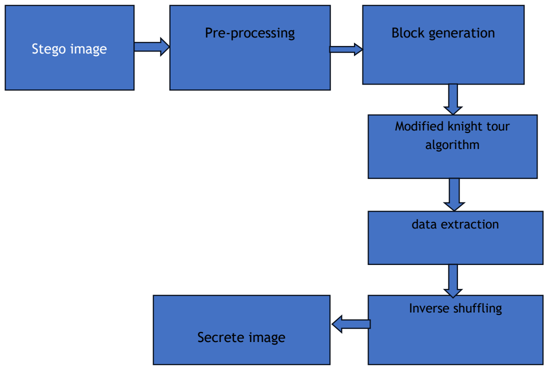

Fig. 4: Proposed System 2

The recommended model is applied to both Framework 1: "Information transmission endlessly segment 2: "Information extraction segment." The cover picture is pre-handled utilizing a middle channel to lessen commotion before it is sent over the organization, and it is then separated into blocks utilizing block age, with each block's pixels chose in view of the knight visit development design, a self-laid out calculation used to characterize the knight's way. The mystery picture is shuffled using the SBox algorithm, which shuffle. Through the use of previously chosen pixels and the "Least Significant Bit (LSB)" substitution technique, this scrambled secret image is concealed within the cover image. The use of RGB planes for the cover image, which are further subdivided into four-pixel blocks for knight's travel, ensures higher security embedding. The knight's route allows the original image's pixel coordinates to be permuted, creating the scrambled image. As seen in Figure 3, system 1 finally sends the secured stego image across the network.

Data shuffling is a method of concealing information that is guaranteed to be confidential by rearranging the original data in a column-by-column fashion [65]. The proposed S-box information rearranging calculation takes into consideration repeating and unassuming encoding, where n × m Sbox can be utilized as a query table with 2n expressions of m-bits each. The system starts with j = 1 on each column from left to right and finishes with the last byte of the last line with j = n × m. The information picture's size is thought to be n × m bytes. This method incorporates two working advances.

- Step-1: Encoding of information grid known as S-box or query table by expansion of nonlinear bytes to particular info information.
- Step-2: Straight rearranging of items in the network table.
- Step-3: The over two stages are rehashed for p times where p ≥ 1.

To recuperate the first information, the pixel values are modified utilizing a converse rearranging system. For 'p' times (where p ≥ 1), the whole cycle is rehashed. By thinking about a Key [i] for conBit, the vector "A" is made, and the relating single digit (i.e., conBit) is put something aside for the jth byte of the image as A [j]. Also, make two unequivocal vectors called "B0" and "B1" and put the ongoing picture's byte [j] numbers in vector B0. The quantity of bytes [j] in the ongoing picture that have both the put away vector pixel data mixed is remembered for "B1." Bytes from the first picture are traded out so byte A [data shuffle[j]] takes up another area.

To extract the secret image from the stego image, reverse LSB is used. Here, the stego image's R plane is divided and altered. The initial point for the knight's tour is determined by the dictionary, and the knight's journey is then calculated on its own. To extract the secret image, the pixel values of the framed Stego image are converted into decimal numbers and then redesigned.

## Experimental results

The proposed work's presentation is assessed utilizing MSE and PSNR." To evaluate the level of contortion in the got Stego picture, MSE is utilized. The PSNR worth of the subsequent stego picture in the wake of implanting demonstrates how well it is. The framework's vigor and productivity are surveyed in light of the PSNR upsides of the stego and cover pictures. The secret picture and the extricated secret picture PSNR are additionally analyzed.

The 1-digit LSB procedure for information disguising is displayed in Figure 5. The secret pictures 1 and 2, which are implanted in a solitary cover picture as found in Figure 5 (c), are alluded to in Figure 5 (a) and Figure 5 (b), separately. Figure 6 represents the utilization of a reversible 1-bit information extraction method to recuperate the inserted secret pictures. A stego picture with embedded emit pictures is displayed in Figure 6(a). Figure 6 (b) and Figure 6 (c) show the recovered mystery picture 1 and mystery picture 2, separately.

In the subsequent technique, 2-bit LSB information stowing away is finished to embed a few pictures into a solitary cover picture. Figure 8 shows the strategy for information stowing away with 2 - bit LSB method. Figure 8 (a), 8 (b) 8 (c) and 8 (d) separately alludes to the mystery picture - 1, secret picture - 2, secret picture - 3 and mystery picture - 4 which are implanted in to a solitary cover picture as portrayed in Figure 8 (d). Reversible 2 - bit information extraction procedure is carried out to recover the implanted mystery pictures and is displayed in Figure 9. Figure 9 (a) portrays a stego picture in which four discharge pictures are implanted. The separated mystery pictures are separately shown in the Figure 9 (b), 9 (c), 9 (d) and 9 (e). The size of the stego picture PSNR is utilized to evaluate the recommended framework's effectiveness. Figure 10 and Figure 11 show the reaction of the variety picture "Lena." For LSB substitution strategies for 1 cycle and 2 digit, separately, the greatness of PSNR and MSE of a couple of normal variety pictures with a size of 512 × 512.

Some normal variety photos have a typical PSNR greatness of 58.9131 for LSB 1-digit, which is fundamentally higher than the 51.4240 for LSB 2-bit. Moreover, obviously the normal MSE size of a couple of standard variety photos.

The calculated value of 0.08352 for the LSB 1-bit is significantly lower than the 0.4685 value for the LSB 2-bit. Two mystery pictures are implanted in LSB 1-cycle, though four mystery pictures are installed in LSB 2-bit, which brings down the picture nature of the subsequent stego picture. This results in an increase in PSNR and a decrease in MSE. All things considered, the research's findings have sparked interest in investigating novel ways to find steganographic techniques as an extension of existing research, and it has been demonstrated that steganography is better than other data hiding techniques because it can embed large amounts of data without permanently distorting it and achieve robustness against compression, additive noise, and tampering attacks with perceptual transparency, imperceptibility, and high embedding capacity and embedding complexity.

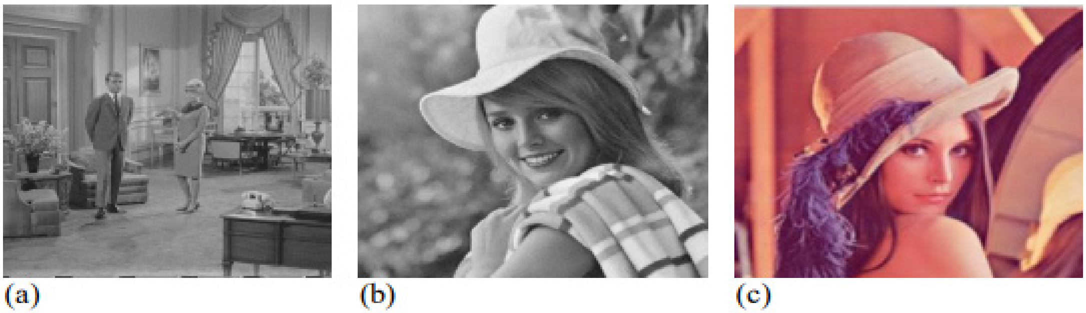

Fig. 5: Single bit data hiding (i.e. LSB 1 - bit) (a) and (b) : Input Secret Images (c) : Cover Image

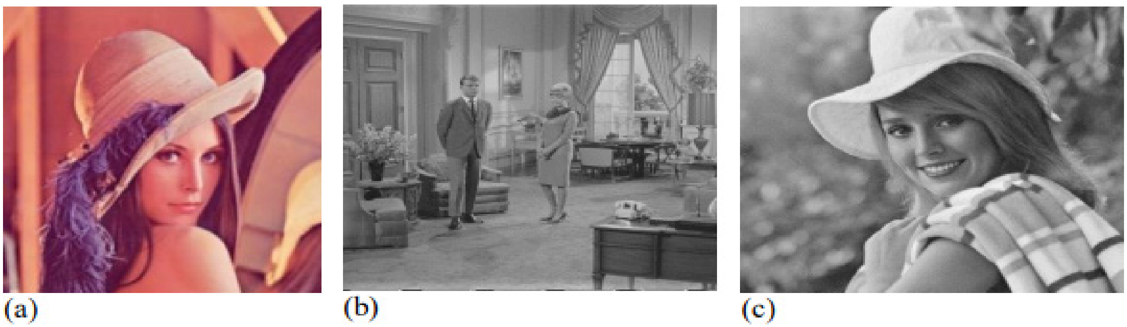

Fig. 6: Single bit data extraction (a) Stego Image; (b) and (c) Extracted Secret Image

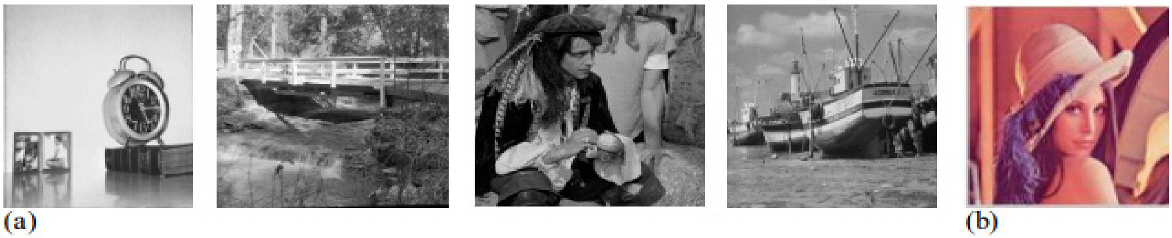

Fig. 7: Input Images (a) Secret Images (e) Cover Image

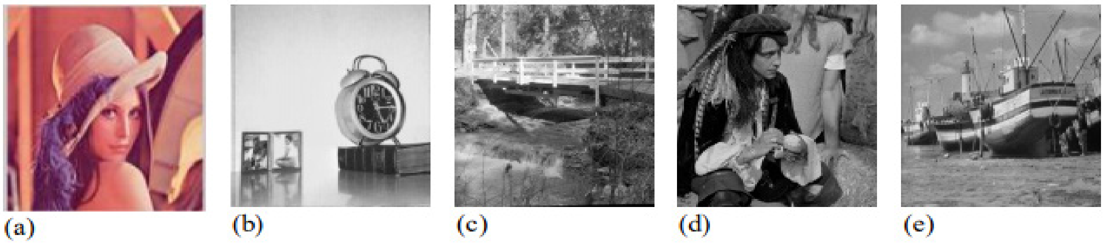

Fig. 8: Output Images (a) Stego Image; (b), (c) , (d) and (e) Extracted Secret Images

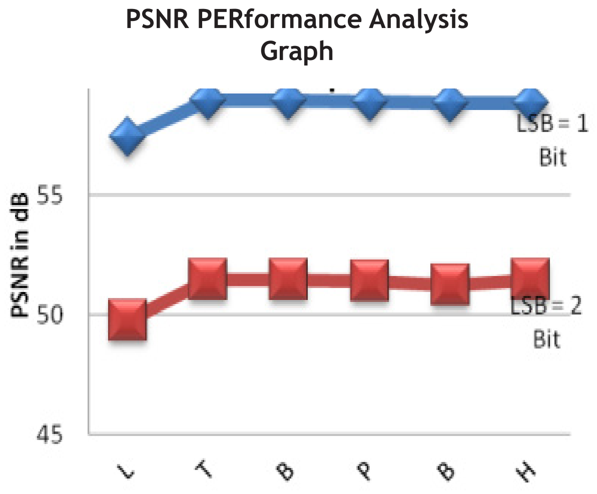

Fig. 9: PSNR Graph.

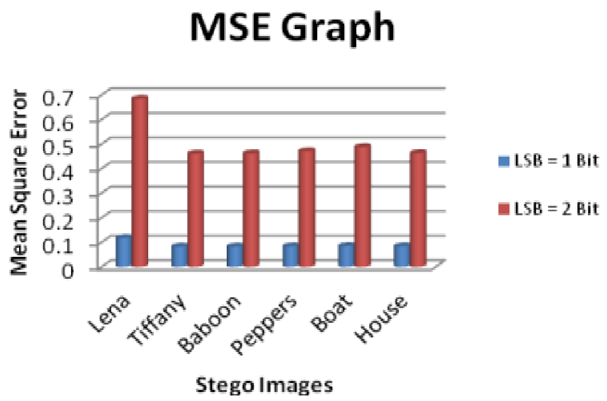

Fig. 10: MSE Graph

## Conclusion

The first strategy uses the modified Knight-Tour and LSB algorithms, which are novel and special techniques for picture steganography in view of the S-Box information rearranging calculation, to permit clandestine correspondence. The information concealing level in the cover picture has been improved with the use of the Knight Tour algorithm. The second method, which combines RSA encryption with Fisher Yates data shuffling, is likewise a novel approach to video steganography. The suggested architecture effectively embeds a larger payload with improved durability and security. To assess the efficiency, the performance metrics are contrasted with the methods currently in use. Measures like PSNR and MSE are used to assess the experimental outcomes of the image steganography. The cover video's data hiding level has been improved by the use of the data shuffling technique. The MATLAB tool is used to implement the entire system, and mean square error and peak signal to noise ratio are used to measure performance in both methods. When compared to the outcomes of current procedures, it is found that both of the suggested ways exhibit enhanced imperceptibility. Furthermore, it has been verified that the security and resilience against different types of assaults.

## References

[1] Shuaib, Khaled, Ezedin Barka, Nedaa Al Hussien, Mohammed Abdel-Hafez, and Mahmoud Alahmad. "Cognitive radio for smart grid with security considerations." Computers 5, no. 2 (2016): 7.

[2] Uchida, N., Sato, G., & Shibata, Y. (2019). Device-to-Device Communication based DTN for Disaster Information System by using Emergent User Policy and Locational Information. Journal of Internet Services and Information Security, 9(3), 41-51.

[3] Premarathne, UthpalaSubodhani, Ibrahim Khalil, and Mohammed Atiquzzaman. "Secure and reliable surveillance over cognitive radio sensor networks in smart grid." Pervasive and Mobile Computing 22 (2015): 3-15.

[4] Shiraishi, Y., Mohri, M., &Fukuta, Y. (2011). A Server-Aided Computation Protocol Revisited for Confidentiality of Cloud Service. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 2(2), 83-94.

[5] Hamood, Ameer Sameer, and Sattar B. Sadkhan. "Cognitive radio network security status and challenges." In 2017 Annual Conference on New Trends in Information & Communications Technology Applications (NTICT), pp. 1-6. IEEE, 2017.

[6] Farzad yaghoubidizaji. (2015). Modified Histogram Based Contrast Enhancement using Homomorphic Filtering for Medical Images. International Academic Journal of Science and Engineering, 2(2), 265–273

[7] Jagan, B. O. L. (2024). Low-power design techniques for VLSI in IoT applications: Challenges and solutions. Journal of Integrated VLSI, Embedded and Computing Technologies, 1(1), 1-5. https://doi.org/10.31838/JIVCT/01.01.01

[8] Shefer, R., and Plessner, B. "Secure Computing Protocols without Revealing the Inputs to Each of the Various Participants." *International Journal of Communication and Computer Technologies*, vol. 12, no. 2, 2024, pp. 31-39.

[9] Meghanathan, Natarajan. "A survey on the communication protocols and security in cognitive radio networks." International Journal of Communication Networks and Information Security 5, no. 1 (2013): 19.

[10] Prasath, C. Arun. "Cutting-Edge Developments in Artificial Intelligence for Autonomous Systems." Innovative Reviews in Engineering and Science 1.1 (2024): 11-15.

[11] El-Hajj, Wassim, Haidar Safa, and Mohsen Guizani. "Survey of security issues in cognitive radio networks." Journal of Internet Technology 12, no. 2 (2011): 181-198.

[12] Le, Trong Nghia, Wen-Long Chin, and Hsiao-Hwa Chen. "Standardization and security for smart grid communica-

tions based on cognitive radio technologies—A comprehensive survey." IEEE Communications Surveys & Tutorials 19, no. 1 (2016): 423-445.

[13] Sajid, Adnan, Bilal Khalid, Mudassar Ali, Shahid Mumtaz, Usman Masud, and Farhan Qamar. "Securing cognitive radio networks using blockchains." Future Generation Computer Systems 108 (2020): 816-826.

[14] Surendar, A. "Internet of Medical Things (IoMT): Challenges and Innovations in Embedded System Design." SCCTS Journal of Embedded Systems Design and Applications 1.1 (2024): 33-36.

[15] Do-Vinh, Quang, and Insoo Koo. "Energy-efficient data encryption scheme for cognitive radio networks." IEEE Sensors Journal 18, no. 5 (2018): 2050-2059.

[16] Kavitha, M. "Environmental Monitoring Using IoT-Based Wireless Sensor Networks: A Case Study." Journal of Wireless Sensor Networks and IoT 1.1 (2024): 32-36.

[17] Muyanja, A., Nabende, P., Okunzi, J., & Kagarura, M. (2025). Metamaterials for revolutionizing modern applications and metasurfaces. Progress in Electronics and Communication Engineering, 2(2), 21–30. https://doi.org/10.31838/PECE/02.02.0