Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 6997190, 8 pages
https://doi.org/10.1155/2022/6997190

Research Article

Internet of Things-Based Data Hiding Scheme for Wireless Communication

A. Shobanadevi,[1] **G. Maragathm**,[2] **Syam Machinathu Parambil Gangadharan**,[3] **Mukesh Soni**,[4] **Rohit Kumar**,[5] **Tien Anh Tran**,[6] **and Bhupesh Kumar Singh**[7]

[1]*Department of Data Science and Business Systems, SRM Institute of Science and Technology, Chennai, India*
[2]*Department of Computational Intelligence, SRM Institute of Science and Technology, Chennai, India*
[3]*Sr General Mills, 1 General Mills Blvd, Golden Valley, Minnesota 55426, USA*
[4]*Senior IEEE Member, Bhopal, India*
[5]*Institute of Management Studies, Noida, Uttar Pradesh, India*
[6]*Vietnam Maritime University, Haiphong, Vietnam*
[7]*Arba Minch University, Ethiopia*

Correspondence should be addressed to G. Maragathm; maragatg@srmist.edu.in
and Bhupesh Kumar Singh; dr.bhupeshkumarsingh@amu.edu.et

Received 7 November 2021; Revised 6 December 2021; Accepted 11 December 2021; Published 17 January 2022

Academic Editor: Shalli Rani

Copyright © 2022 A. Shobanadevi et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

The substantial rise of information technology has facilitated the methods of access to digital information and internet of things (IOT). Digital image processing handles the digital material to store and distribute more effectively with decreased time and space complexity. However, these tactics undermine the privacy of digital materials. A recent study focuses on shielding digital materials from illicit use and distribution by making reversible data strategies to tackle the risk of privacy breaches for digital content. In this study, a composite reversible data hiding (CRDH) approach is suggested. CRDH employed the integer wavelet transform (HAAR transform) with the HH band's eigenvalue decomposition. The suggested CRDH first performed the IWT transformation on the cover image (CI) and parsed it into four consecutive frequency subbands, namely, LL, HL, LH, and HH. Sensitive data of the proposed approach are incorporated by merging the HH band of the cover image's individual values with the encrypted eigenvalues of the confidential data. The choosing of casing art is such a method that values are within a range. The confidential data picture and HH band's frequency band are roughly the same; thus, modifying the individual values will not affect the quality of the confidential data image and the HH band's content. The suggested strategy's primary purpose is to design a data concealing technique that hinders the verification of digital information by maintaining a high rate of peak signal-to-noise ratio (PSNR). The PSNR of the existing technology is less than 50 per cent of the total accessible data set. The PSNR value shows the picture's visual quality, where the PSNR increases the better image quality. Therefore, concealing data is essential for the technique that inhibits authentication and keeps a high rate of PSNR. The suggested approach fulfils this aim, gets a PSNR rate of above 50 per cent, and hits 59 per cent for line.

1. Introduction

The internet of things (IoT) is aimed at connecting every device to the Internet so that these devices can be accessed anytime, anywhere, and from any path (i.e., any network). This concept has been defined as a new communication system that connects the Internet with the physical world via wireless sensor devices. As a result, everyday devices have become a network component that collects information about their environment and generates reports. Thus, every object with wireless technology can provide data to a large number of applications and users. However, to realize this

potential, wireless devices with different communication standards and hardware limitations need to work in harmony with each other and with existing internet protocols.

Today, wireless sensor networks are used in smart home, health, agriculture, and industrial applications primarily work in local area networks to provide information to a certain number of users. Since application protocols running on TCP/IP stacks designed for traditional wired networks cannot be used directly on devices with limited hardware resources, these networks are connected to the Internet via a gateway between the user and the sensor devices. TCP/IP is also called the Internet protocol suite, which is a set of communication protocols used by the internet or the networks which are parallel to it. It allows large-distance communication by creating a virtual network. This situation is time-consuming and laborious since each new application requires modifications to the existing protocols defined on the wireless sensor network. Therefore, wireless sensor networks cannot be directly integrated into the internet infrastructure. In wireless sensor networks, CoAP, MQTT, STMP, etc., application protocols have been proposed. These application protocols work on the IP protocol as simplified versions of the HTTP protocol and require each device to have an IP address. Considering that the number of devices connected to the Internet will be over 29 billion in 2023 and IoT devices will manage the internet traffic (Cisco, 2020), needs such as addressing a large number of devices and supporting the traffic generated by the existing infrastructure arise.

In this context, the adaptation layer and IPv6/6LoWPAN protocol stack enable wireless sensor devices to connect to external IP networks using IPv6 addresses. However, since the IPv6 method supports end-to-end communication, unfortunately, different solutions are required against the traffic bottleneck caused by IoT devices. The second layer of TCP/IP model is a transport layer. This is an end-to-end layer which is used to deliver messages to the host. Moreover, it provides point-to-point connection between the source host and destination host for delivering services efficiently. In this context, the most striking solution proposal in recent years as an alternative to end-to-end communication is information-centered network architecture (ICN (information-centric networks). This architecture proposes a network model that focuses on content/data instead of address-based communication between destination and source nodes. Therefore, methods such as naming, routing, caching, and securing ICN provide advantages for IoT applications. For example, the data is provided by the naming of the data, regardless of the address where it is located. In addition, fast and efficient content provision is ensured by caching data by wireless devices on the same network, regardless of the data source. Thus, the information-centered approach has become a strong candidate in incorporating wireless sensor networks into the Internet by eliminating the necessity of establishing and maintaining the end-to-end connection required by the traditional Internet architecture.

With the global expansion of the Internet, the Internet has become a powerful and accessible platform for data transmission. Unfortunately, sensitive information can be stolen and tempered on the Internet. In recent times, information security has attracted the focus of the researcher as a data hiding scheme. Data hiding [1] plays a vital role in Internet and multimedia-based secure communication. The primary purpose of data hiding is to secure the confidentiality of the message and share the sensitive news safely. If there is any splash in the confidential message or its media during data transmission, the secret message cannot be reorganized entirely after receiving it. Data hiding schemes for sharing confidential data in intelligence, buro, paramilitary, military, and company financial reports would have played a significant role in recent times and lead to focus research in reversible data hiding schemes in recent years [1].

The reversible data hiding [2, 3] uses images as an input tool because of their easy access. Images can be downloaded with a scanner, digital camera, or directly online. Depending on the encryption method, the most recent algorithm data can be divided into three areas: location, currents, and pressure points. Encryption method offers various advantages. It is cheap to apply in algorithms. It increases the integrity factor of our data. Moreover, it allows sharing your files safely. Algorithms in the field section include encryption by changing the pixel value directly. However, algorithms in the network area begin to convert the image to coefficients [4, 5]. Then, the coefficient changes include individual messages [6, 7]. Pressure algorithms accept images generated by a series of compressed codes as their intervening medium. Inclusive details are achieved by modifying the computer code [8, 9].

This paper presents a composite reversible data hiding (CRDH) scheme that employs integer wavelet transform (HAAR transformation) with eigen decomposition over both cover and confidential data images [10]. The proposed data hiding scheme significantly improved the extracted hidden data measure as MSE and PSNR and acquired higher PSNR and lower MSE.

2. Internet of Things

IoT is a system that allows all objects in the ecosystem to connect to the Internet. In addition to the ability to communicate with each other, these tiny objects can send data directly to the Internet or act by taking commands on the data coming from the Internet. Therefore, IoT allows objects with different properties to be accessible from the Internet for data collection, resource sharing, analysis, and management. As a result, in transportation, health, environment, agriculture, etc. smart devices used in various business areas and having sensors and actuators have become intelligent internet components. IoT is aimed at transforming the data collected from these devices into information with methods used in application areas such as artificial intelligence and data mining and serve this information to many applications or users. In addition, standardization studies have been carried out so that wireless sensors with different hardware/communication sources can be used in large-scale applications.

Most applications carrying various information obtained from sensor devices to users with existing internet protocols

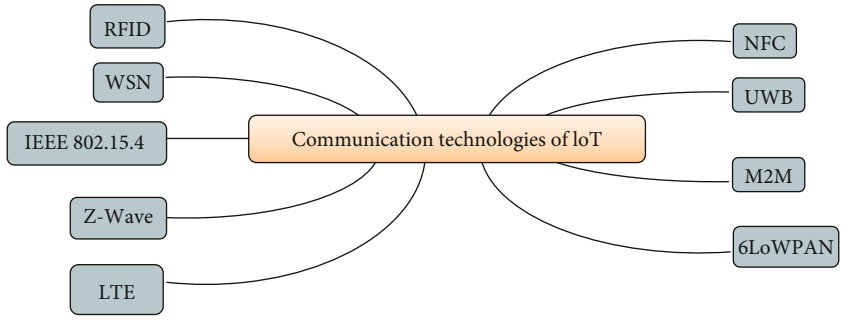

Figure 1: Internet of things: communication technologies and applications [5].

work in local area networks (LAN (local area networks)). On the other hand, IoT is aimed at providing information to many users and services by measuring the information obtained from sensor nodes depending on their application areas. In this direction, IoT applications and currently used technologies are examined in 5 different layers in Figure 1: object/device layer, connection layer, management layer, data processing and analysis layer, and application layer. With this architecture, the data provided by the sensor nodes over the internet in real-time or periodically can be used by many applications and users. The sharing of secret keys of nodes is provided by symmetric and asymmetric encryption mechanisms. The fundamental difference between these two types of encryption is that symmetric uses one key for both encryption and decryption, while the later one uses a public key for encryption and a private key for decryption.

In Figure 1, each layer represents the area of production and use of information. In the object layer, each device collects information about its environment. At the same time, the identification and tracking of objects in this layer are provided by RFID technology, proximity, smoke, temperature, light, etc. The information that needs to be measured can be identified with other sensing devices. The connection layer is where devices with different technologies are named, and the produced measurement data (temperature, light, etc.) is transmitted. In this layer, each device uses its communication technology (Zigbee (IEEE 802.15.4), 6LoWPAN, NFC, Bluetooth, etc.)

It carries the information it produces to the upper layers of management and data processing. Security, media access control, installation, and configuration of devices are done at the management layer. This layer is where the periodic operating times of wireless devices and discovery and configuration protocols are set in the local network area. The generated information can be used by end-users in the application layer, and it also provides information to different application areas in the data processing and analysis layer. At the application layer, the information obtained from the devices and meaningful information can be used for suspicious event detection, efficient energy consumption, occupational safety, etc. It can be used in many applications (Ersin & Öz, 2020), e.g., the electricity consumption information measured by the sensor nodes used in smart homes, and innovative grid applications can be used by electricity companies to optimize supply and demand and make savings and consumption plans by the consumer.

Another application area emerging within the Internet of things with body area sensor nodes is intelligent health systems—physical measurement information obtained from body area sensor nodes, Bluetooth, etc. With the help of communication technology, it can be monitored in real time via a smartphone, or these measurements can be controlled by doctors with cloud technology. In addition, elderly surveillance systems can be given as an example. Remote real-time surveillance of the patient can be provided, and physical measurements such as blood value and heartbeat can be followed with the help of sensor nodes. As an application that can be used shortly, it can be used for smart homes, building, cities, etc. Any sensor node will transmit the values it produces to social networking sites periodically, and this information will be followed by many users and end systems. Along with applications such as smart houses and buildings, innovative agriculture/forest systems and transportation systems define new application areas that emerge within the Internet of Things.

3. Communication Features

Sensor devices used in various applications of IoT have different communication technologies such as IEEE 802.11, IEEE 802.15.4, IEEE ZigBee, IEEE Bluetooth, and RFID. In the IoT communication model, wireless sensor devices are connected to a gateway connected to the Internet. The gateway can query data from nodes at specific intervals or transmit data to nodes. Data generated in wireless devices are transmitted with IEEE 802.15.4 or a similar wireless technology standard with low data transmission capacity (kb/s). The data transmission capacity of the IoT environment is limited by the resource constraints (energy, computing power, and memory) of the sensor devices and the insecure nature of the transmission environment. For this reason, reliable communication protocols have taken into account the limited data rate and power capacity of the devices while minimizing energy consumption at the same time.

4. Data Security in IOT

The accessibility of data by many users and applications has made it more critical to ensure the security of devices that

collect sensitive information about almost every environment and this sensitive information. The processor power, storage space, and energy constraints of wireless sensor devices used in the IoT cause these devices to be inherently vulnerable. At the same time, problems such as the loss and corruption of packets containing sensitive information are frequently experienced in these environments. Therefore, ensuring security in a complex and dynamic system such as the IoT is critical. For this, in applications where wireless sensor networks are used, the security requirements are determined as data confidentiality, source authentication, data integrity, and availability of data.

Security models integrated with the data itself are not supported in IP-based Internet applications. Instead, in IP networks where end-to-end communication is established, the security of the communication channel between the two ends is provided with TLS/DTLS/SSL security protocols for the formation of a secure session. In addition, mechanisms such as content integrity and authentication were added to the upper layers later. The high messaging requirement of these protocols causes packet delay, reducing network and application performance. The energy consumed by wireless devices with limited resources to provide a secure communication channel is more than the energy spent for encryption algorithms. In this case, security methods integrated with the content itself can be an efficient solution for restricted devices. One mechanism that makes the knowledge-centric network approach a strong candidate for IoT applications and future internet architecture is providing the content itself. In ICN, the safety of the data is ensured by the control of integrity, accuracy, and privacy. Completeness check consists of the name–data pair. In this case, the information itself is accessed by the given word. Accessing the data with the signature-based naming method also provides the accuracy condition. Privacy control is provided at the transmission and application layers. In addition, the security of devices must be ensured in various IoT applications. In this case, authentication and authorization checks are required. For example, machines that send commands to an actuator may need to be authenticated. However, ICN focuses on the security of interest and data messages. Therefore, additional security mechanisms should be used for different service models using wireless devices. Cryptography is the study of secure communication techniques that allow only the sender and the intended recipient of a message to view its contents. The term is derived from the Greek word kryptos, which means hidden. If the message is intercepted, a third party has everything they need to decrypt and read the message.

In traditional ICN networks, the public critical cryptography method is used, and encryption information is added to the end of data/interest packets. Cryptography can be described as the study of secure communications which will allow only the sender and the intended recipient of a message to see the content. For example, if the message is being intercepted, then the third party will have anything they require to decrypt and to read the message. In wireless sensor networks, data confidentiality is provided with key-sharing AES, Blowfish, and Triple DES using various encryption algorithms. However, key usage and encryption alone are not enough. In the wireless environment, suspicious nodes can quickly get into the communication scope of other nodes, eavesdropping on sensitive data and decrypting them. Source authentication is used by the sending and receiving nodes to distinguish between malicious fake packets and original packets. The sharing of secret keys of nodes is provided by symmetric and asymmetric encryption mechanisms. However, the increase in the use of the processor and the size of the communication packets by the encryption mechanisms reduces resource-constrained wireless sensor devices (Tourani et al., 2018). The elliptic curve encryption method provides security with lower processing power with the fundamental structure produced smaller than other methods and can be applied in limited IoT devices. However, this method requires the critical exchange and sharing keys between nodes which adds a burden on communication. Data integrity is essential in detecting data damage or loss caused by the conditions of the wireless transmission environment. However, malicious nodes can inject incorrect data or modify data inside communication packets.

For this reason, the integrity of the data is essential not only for error control mechanisms but also for ensuring security. Data availability is essential when wireless sensor nodes or a group of nodes in the network are exposed to a denial of service (DoS) attack. Security mechanisms have been developed for each type of attack in the literature. These mechanisms, which take attack-based security measures, should be designed specifically for application requirements.

5. Reversible Data Hiding

With the rapid advancement of communication through the Internet, the information exchanged could tamper intentionally or accidentally through unprivileged access. In recent years, reversible data hiding (RDH) has become an active research domain in data replication. In reversible data hiding, the bits hidden are embedded in the cover file (image) on the sender side. Confidential data and original cover media are extracted without distortion to the receiver. The data hiding technique is divided into immutable data hiding and reversible data hiding. In the immutable data hiding, the information in a database cannot be changed or deleted. One cannot overwrite the previous data when the new data is available. However, in the reversible data hiding technique, the data is embedded in the image in such fashion that the original data can be restored. The embedding ability to hide immutable data is high. However, while the original cover media is destroyed, the embedding capacity in RDH is low, but the original cover media can be recovered [11, 12].

Some of the present data hiding schemes are not invertible, the presence of truncation error and round-off error in spread spectrum technique makes it nonreversible, because of the bit replacement without memory, and the least significant bit plane scheme is taken into account to be non-reversible and because of the quantization error quantization-index-modulation rendered as invertible. RDH also links two data

sets, and a group belongs to the embedded information [13]. This reversible data handling technique has some advantages like the scheme offers the embedding capacity which is directly proportional to the number of pixel in image. Moreover, the reversible technique inherited from this scheme provides functionality that allows recovery of the cover image. Another set belongs to the cover media data such that the cover media will be lossless recovered once the hidden information has been extracted out. Confidential data is embedded by modifying the frequency coefficient of the cover image by using some standard methods like discrete Fourier transform (DFT), discrete cosine transform (DCT), discrete wavelet transform (DWT), and integer wavelet transform [14, 15]

5.1. Proposed Work. This paper presents a composite reversible data hiding (CRDH) scheme. CRDH competitively applied integer wavelet transform (HAAR transformation) with eigen decomposition over the cover image's cover image and brand of the cover image. CRDH decomposed the cover image (CI) into four subbands, namely, LL, HL, LH, and HH, and evaluated the HH band's eigen decomposition value for data hiding.

In the proposed reversible data hiding scheme, integer wavelets transform the cover image (CI) by decomposing, namely, into lower-lower (LL), higher-lower (HL), lower-higher (LH), and higher-higher (HH) frequency subband as shown in Figure 2.

In CRDH algorithm, the hidden data is integrated into the host image by changing the band of high-frequency coefficients described in Figure 3, that is, the HH subband. As shown in Figures 1, 2, and 4, the proposed reversible data hiding scheme is based on both integer wavelet transform and eigen decomposition with encryption [16, 17]. Initially, integer wavelet transform divides the host image into four frequency subfields as LL, HL, LH, and HH bands. The LL tape works with rough details, the HL band deals with horizontal elements, the LH provides vertical information, and the HH band contains diagonal image information. The HH band uses the HH band to embed sensitive data because you lose data on the image energy [18, 19]. In this way, an embedded confidential data will not affect the perception accuracy of the cover image. The proposed reversible data hiding scheme has two steps with hiding and sending and receiving as extraction steps.

5.2. Hiding Phase of Composite Reversible Data Hiding (CRDH) Scheme. Once the cover image decomposes into four subsequent frequency subbands, CRDH uses the HH band to hide confidential data (CDI), as its accounted minimum noise level. The proposed data hiding scheme evaluates the eigen decomposition of HH band confidential data followed by encryption [20]. Encrypted eigen decomposition then superimposes over HH band of IWT (CI) after applying inverse eigen decomposition operation. Finally, we apply the inverse integer wavelet transform to generate an embedded cover image (ECI).

5.3. Extraction Phase of Composite Reversible Data Hiding (CRDH) Scheme. The extracting phase of the proposed

Figure 2: IWT transform of cover image.

scheme uses exactly the inverse operation of the hiding phase; in extracting, the proposed scheme is used to apply integer wavelet transform over the embedded image (ECI) to get the HH band confidential data (CDI) is hidden, as shown in Figure 4. The CRHD scheme enforces eigen decomposition on HH frequency band of the received data. The retrieved eigen decomposition compositely contains eigen decomposition on the cover image's HH frequency band and confidential data. As the image dimension of covered data is already shared between the sender and receiver before the established data communication, the extracting phase compared the shared cover image with the received image. The received image contains both the cover image and confidential data. The extraction step's subtracting returns the eigenvalue of encrypted confidential data and subsequently applies all inverse operations to get confidential data at the receiver side.

6. Result Analysis

The proposed works have tested on various data set images of size 512×512. These entire data set images are gray scale. The gray scale is defined for digital images. It means the value of each pixel will represent information about the intensity of the light. In other words, the image which has only black, white, and gray colors than gray will have multiple levels. Here, the data set images are used as Fruits, Elaine, Lena, and Tiffany. The size of the confidential image is also the same as the original image. To simulate the proposed work, the implementation is done in MATLAB. The i3 processor is executed with 4 GB RAM and 500 GB HDD.

6.1. Performance Parameter. PSNR is an image factor used to determine the quality of an image by comparing quality differences between the original image and the resulting image.

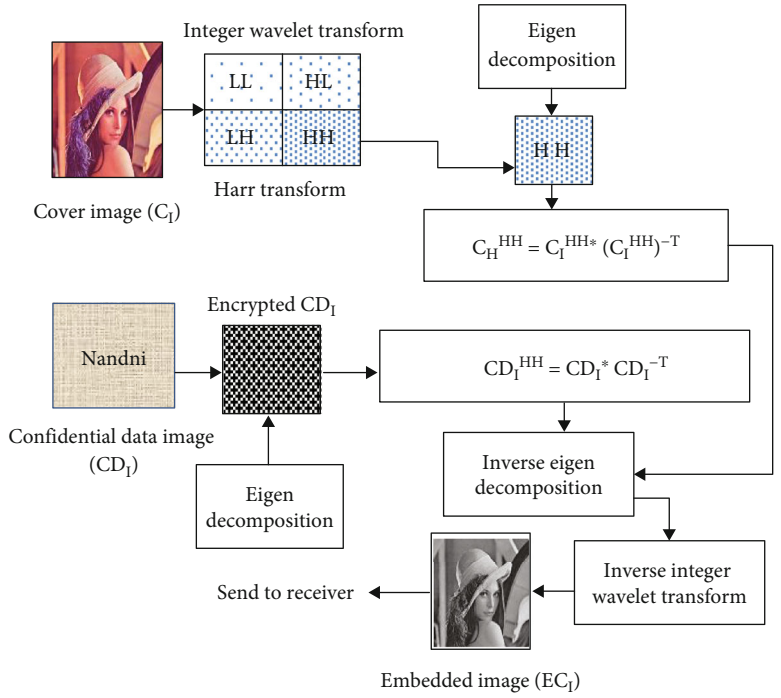

Figure 3: Reversible data hiding embedding procedure.

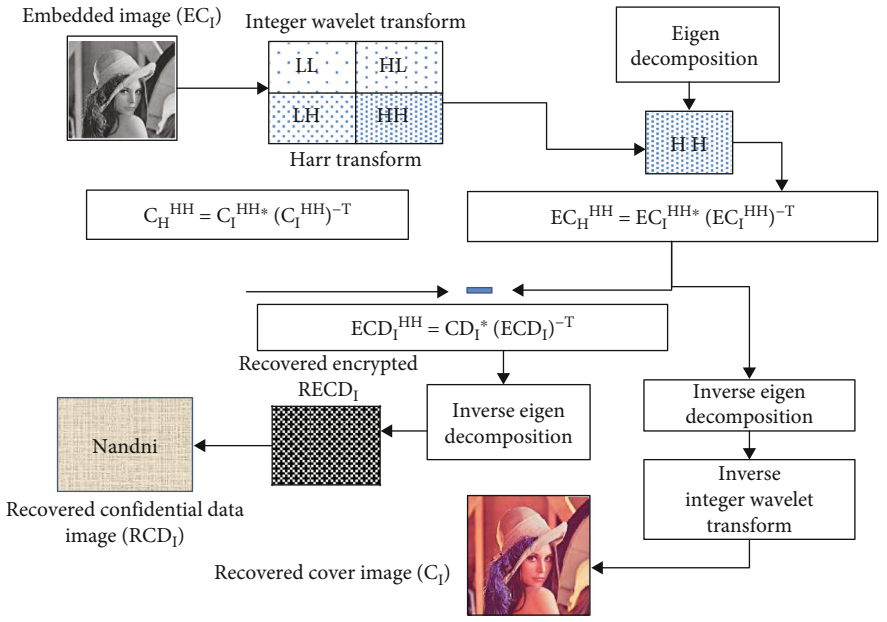

Figure 4: Reversible data hiding extraction procedure.

It is calculated using the mean square error (MSE). The following formula calculates both parameters:

$$\text{PSNR} = 10 \log_{10}\left(\frac{\text{MAX}^2}{\text{MSE}}\right), \quad (1)$$

$$\text{MSE} = \frac{\sum_{i,j}[\mathbf{I_1}(\mathbf{i},\mathbf{j}) - \mathbf{I_2}(\mathbf{i},\mathbf{j})]^2}{\mathbf{i} * \mathbf{j}}. \quad (2)$$

Table 1: Mean square error vs. noise level ratio comparison over different data images.

Images	MSE	Noise level
Fruits	0.099007	0.45
Elaine	0.127639	0.29
Lena	0.05318	0.38
Tiffany	0.243832	0.41

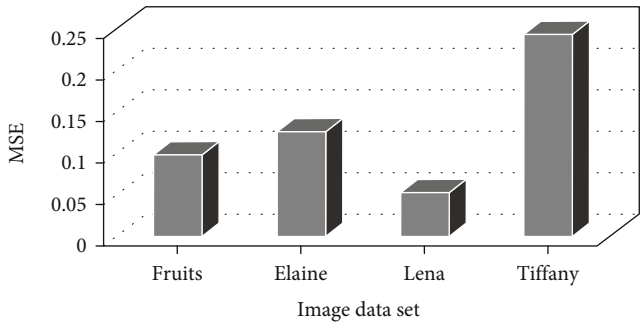

Figure 5: Comparative analysis of mean square error ratio.

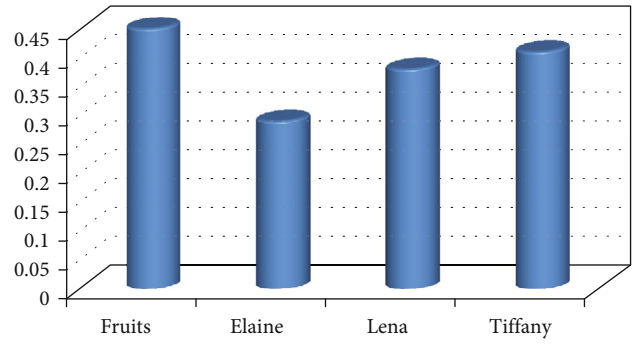

Figure 6: Comparative analysis of noise ratio.

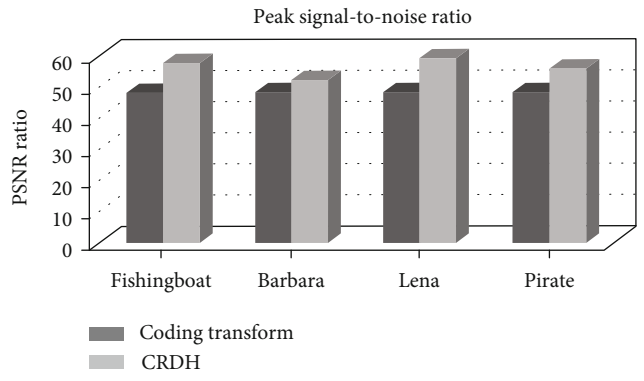

Figure 7: Comparative analysis of for PSNR.

This calculation has been gathering by the computer program. There are various testing images has been used. Some of them have been shown here with their results. Table 1 shows comparison of mean square error and noise level ratio over different data images.

For four different data sets, the mean square error is compared with noise level over the data range.

Figures 5 and 6 show the MSE and noise ratio, as the graph shows that there are some images has been used for as input. This input and the generated output image has been used for calculating the comparison ratio. The graph also shows the proposed approach shows the better results.

Figures 7 and 8 show the PSNR and SNR, as the graph shows that there are some images has been used for as input. This input and the generated output image has been used for calculating the PSNR. The graph also shows the proposed approach shows the batter results.

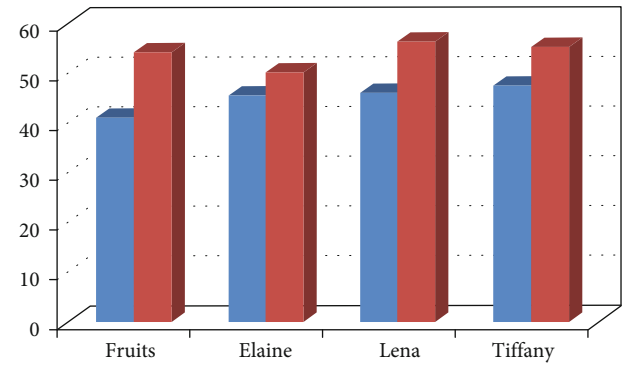

Figure 8: Comparative analysis of for SNR.

Table 2: PSNR comparison over different data images.

Images	Coding transform	CRDH
Fruits	48.36	57.85
Elaine	48.31	52.36
Lena	48.39	59.54
Tiffany	48.45	56.24

Table 3: SNR comparison over different data images.

Images	Coding transform	CRDH
Fruits	41.21	54.25
Elaine	45.63	50.26
Lena	46.35	56.54
Tiffany	47.52	55.41

As shown in Tables 2 and 3, PSNR and SNR of existing technique for all the available data set describes in Figure 8 is less than 50%. The PSNR value indicates the image's visual quality, where a higher PSNR and SNR value leads to better image quality. It is needed to develop a data hiding scheme that prevents authentication of digital information with maintaining a higher PSNR, whereas the proposed scheme significantly achieves this goal and gains PSNR greater than 50 and achieves up to 59% for Lena.

7. Conclusion

Confidential data exchange is virtually insecure in this era of wireless communication. Intentional or unintentional changes to the transmitted data are possible. Recently, researchers focused on hiding confidential data within the covered image via a reversible data hiding scheme. But the data hiding scheme still faces challenges to extract distortion less and noise-free confidential data at the receiver side. This paper presents a composite reversible data hiding (CRDH) scheme. CRDH competitively applied integer wavelet transform (HAAR transformation) with eigen decomposition

over the cover image and confidential data image. CRDH decomposed the cover image (CI) into four subbands, namely, LL, HL, LH, and HH, and evaluated the HH band's eigen decomposition value for data hiding. The discussed technique will help to design a data concealing method which impedes the verification of digital information by keeping the rate of PSNR high. The PSNR of the existing technology is less than 50 per cent for the total accessible data set. The proposed data hiding scheme significantly improved the extracted confidential data measure as the MSE and PSNR and acquired higher PSNR (up to 59%) and lower MSE. For the future researchers, it creates a gap to work on additional factors which do not directly relate to the performance of the proposed technique. It will also include reducing the size of the auxiliary file.

Data Availability

The data shall be made available on request.

Conflicts of Interest

The authors declare that they have no conflict of interest.

References

[1] G. Xuan, C. Yang, Y. Zhen, Y. Q. Shi, and Z. Ni, "Reversible data hiding using integer wavelet transform and companding technique," in *Digital Watermarking. IWDW 2005. Lecture Notes in Computer Science, vol 3304*, I. J. Cox, T. Kalker, and H. K. Lee, Eds., Springer, Berlin, Heidelberg, 2005.

[2] A. Shaik and V. Thanikaiselvan, "Comparative analysis of integer wavelet transforms in reversible data hiding using threshold based histogram modification," *Journal of King Saud University-Computer and Information Sciences*, vol. 33, no. 7, pp. 878–889, 2021.

[3] J. Hou, O. Bo, H. Tian, and Z. Qin, "Reversible data hiding based on multiple histograms modification and deep neural networks," *Signal Processing: Image Communication*, vol. 92, p. 116118, 2021.

[4] Y. Fei Peng, X. Z. Zhao, M. Long, and W.-q. Pan, "Reversible data hiding based on RSBEMD coding and adaptive multi-segment left and right histogram shifting," *Signal Processing: Image Communication*, vol. 81, p. 115715, 2020.

[5] S. Weng, W. Tan, O. Bo, and J.-S. Pan, "Reversible data hiding method for multi-histogram point selection based on improved crisscross optimization algorithm," *Information Sciences*, vol. 549, pp. 13–33, 2021.

[6] G. Xuan, X. Li, and Y.-Q. Shi, "Histogram-pair based reversible data hiding via searching for optimal four thresholds," *Journal of Information Security and Applications*, vol. 39, pp. 58–67, 2018.

[7] J. Wang, N. Mao, X. Chen, J. Ni, C. Wang, and Y. Shi, "Multiple histograms based reversible data hiding by using FCM clustering," *Signal Processing*, vol. 159, pp. 193–203, 2019.

[8] X. Gao, Z. Pan, E. Gao, and G. Fan, "Reversible data hiding for high dynamic range images using two-dimensional prediction-error histogram of the second time prediction," *Signal Processing*, vol. 173, p. 107579, 2020.

[9] G. Gao, S. Tong, Z. Xia, W. Bin, X. Liya, and Z. Zhao, "Reversible data hiding with automatic contrast enhancement for medical images,," *Signal Processing*, vol. 178, p. 107817, 2021.

[10] T.-S. Nguyen, C.-C. Chang, and N.-T. Huynh, "A novel reversible data hiding scheme based on difference-histogram modification and optimal EMD algorithm," *Journal of Visual Communication and Image Representation, Volume*, vol. 33, pp. 389–397, 2015.

[11] R. M. Rad, K. S. Wong, and J.-M. Guo, "Reversible data hiding by adaptive group modification on histogram of prediction errors," *Signal Processing*, vol. 125, pp. 315–328, 2016.

[12] C.-C. Lin, W.-L. Tai, and C.-C. Chang, "Multilevel reversible data hiding based on histogram modification of difference images," *Pattern Recognition*, vol. 41, no. 12, pp. 3582–3591, 2008.

[13] M. Xiao, X. Li, Y. Wang, Y. Zhao, and R. Ni, "Reversible data hiding based on pairwise embedding and optimal expansion path," *Signal Processing*, vol. 158, pp. 210–218, 2019.

[14] E. Gao, Z. Pan, and X. Gao, "Reversible data hiding based on novel pairwise PVO and annular merging strategy," *Information Sciences*, vol. 505, pp. 549–561, 2019.

[15] W. Hong, T.-S. Chen, and M.-C. Wu, "An improved human visual system based reversible data hiding method using adaptive histogram modification," *Optics Communications, Volume*, vol. 291, pp. 87–97, 2013.

[16] Y. Shoji, K. Nakauchi, W. Liu, Y. Watanabe, K. Maruyama, and K. Okamoto, "A community-based IoT service platform to locally disseminate socially-valuable data: best effort local data sharing network with no conscious effort?," in *2019 IEEE 5th World Forum on Internet of Things (WF-IoT)*, pp. 724–728, 2019.

[17] F. T. Jaigirdar, C. Rudolph, and C. Bain, "Prov-IoT: a security-aware IoT provenance model," in *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, pp. 1360–1367, 2020.

[18] J. H. Jeon, K. Kim, and J. Kim, "Block chain based data security enhanced IoT server platform," in *2018 International Conference on Information Networking (ICOIN)*, pp. 941–944, 2018.

[19] W. Iqbal, H. Abbas, M. Daneshmand, B. Rauf, and Y. A. Bangash, "An in-depth analysis of IoT security requirements, challenges, and their countermeasures via software-defined security," *IEEE Internet of Things Journal*, vol. 7, no. 10, pp. 10250–10276, 2020.

[20] M. A. López Peña and I. Muñoz Fernández, "SAT-IoT: an architectural model for a high-performance fog/edge/cloud IoT platform," in *2019 IEEE 5th World Forum on Internet of Things (WF-IoT)*, pp. 633–638, 2019.