SEMARAK ILMU
PUBLISHING
202103268166(003316878-P)

Journal of Advanced Research in Applied Sciences and Engineering Technology

Journal homepage:
https://semarakilmu.com.my/journals/index.php/applied_sciences_eng_tech/index
ISSN: 2462-1943

Reliable and Secure Data Transfer in IoT Networks using Knight-Tour and PHLSB Method

V. Anjana Devi[1,*], I. Bhuvaneshwarri[2], C. Santhosh Kumar[3], V. Chandrasekar[4], V. Kalaichelvi[5], E. Anitha[6], Jogendra Kumar[7]

[1] Department of CSE, Rajalakshmi Institute of Technology, Kuthambakkam, Chennai, Tamil Nadu, India
[2] Department of Information Technology, Government College of Engineering, Erode, Tamil Nadu, India
[3] Department of Information Technology, Sona College of Technology, Salem, Tamil Nadu, India
[4] Department of CSE, Faculty of Engineering and Technology, Jain (Deemed-to-be) University, Bangalore, Karnataka, India
[5] Department of Computer Science and Engineering, SRC, Sastra Deemed University, Kumbakonam, Tamil Nadu, India
[6] Department of Artificial Intelligence and Data Science, Sri Eshwar College of Engineering, Coimbatore, Tamil Nadu, India
[7] Department of Computer Science and Engineering, G.B.Pant Institute of Engineering and Technology, Pauri Garhwal Uttarakhand, India

ARTICLE INFO

Article history:
Received 3 April 2023
Received in revised form 22 June 2023
Accepted 27 June 2023
Available online 9 September 2023

Keywords:

Internet of Things (IoT); Steganography; Knight- Tour; Polynomial based Hash Least Significant Bit (PHLSB); human visual system (HVS)

ABSTRACT

Data security has recently become the most pressing problem for corporate owners and even regular people due to the continual development in the speed of data transmission over the entire Internet, and stricter regulations have been made for data protection. Secure key management is now essential for securing information exchange due to the Internet of Things (IoT) and the rapidly advancing mobile device technologies. Smart home and healthcare IoT apps, for instance, offer automated services to users with little user involvement. Data transmission delays and intrusions can affect existing security solutions that use a single link. In this paper, we propose a novel distributed key management scheme for IoT ecosystem. The methods Knight-Tour and polynomial-based hash least significant bit (PHLSB) that take use of flaws in the human visual system (HVS) are combined to form a hybrid approach to image steganography in this research. The Knight's trip path is a chess board layout that follows the route of a horse without stopping at any of the nodes again. In order to create the scrambled image, this travel path pattern is employed to permute the original image's pixel positions. Prior to being masked behind a cover image, this technique makes sure the communication has been encrypted. A strong mathematical tool is a polynomial equation. The cover object's data was hidden using these equations as a secret key. The suggested solution efficiently secures IoT devices by assigning the resource-intensive encryption processing to local organisations. As a result of the proposed framework's simulation findings, network lifetime PDR (Packet Drop Ratio) has improved, throughput has increased, energy consumption has decreased, and latency has decreased.

[*] *Corresponding author.*
E-mail address: anjanadevi.aby06@gmail.com

https://doi.org/10.37934/araset.32.2.107118

1. Introduction

The demands for information security for data transmission and data storage are rising steadily in the new era due to the explosive rise of Internet usage on a global scale and the new information technology trend [1]. Therefore, protecting sensitive data from unauthorized access and intrusions is crucial. In the area of information security, cryptography and steganography play significant roles. The requirement for data privacy is significant since the necessity for data security has grown to be a constant worry for governments, people, and business owners. A popular technique for achieving data security is encryption and decryption. Decryption returns ciphertext to its original state, or plain text, after encryption has transformed it into ciphertext. When data is encrypted and decrypted, it is done using a cryptographic algorithm, or cypher [2].

In recent years, the Internet of Things has realized a unified communication environment and realized respective platforms from the standpoint of distributed systems in the virtual and real worlds [3]. The Internet of Things is a hub of completely linked sensor gadgets. In order to speed up patient treatment, a company named HIE (Health Information Exchange) has implemented medical data transfer. Today, hospitals routinely collect medical data. Security is the first concept that comes to mind when the phrase Internet is used. When it was first brought to the Internet, security was one of the primary concerns. Although still in the public eye, HTTP is a security issue. The secure transmission of medical data in an IoT environment therefore requires the development of technologies. The solution to this issue is to combine steganography with encryption and decryption techniques [4].

Secret value and algorithm are two crucial factors in cryptography that are taken into account when encrypting and decrypting data. Data encryption employs a key element that is added as part of the algorithm [5, 6]. When a single algorithm is used to encrypt a collection of data, a unique key is needed for every piece of data. It might be challenging for senders to specify who should get information securely when designers are working with multiple algorithms. As a result, key material is crucial to data decryption and can be easily decrypted by someone with similar key material [7, 8].

Steganography is a technique used to transfer information securely, hide data, and evade being intercepted by others by hiding it in images and transmitting them invisibly. The discrete wavelet transform is crucial for phenomenal spatial localization because to its multi-resolution characteristics and frequent diffusion. The shape of the human visual system closely resembles that of DWT [9, 10]. Steganography is important because it may be used to detect and remove suspicious material that has been concealed by hackers. A sensitive message should be sent by text in an undetectable manner. Both stealth and imperceptibility are achieved through the use of steganography. It is just as challenging to improve capacity while remaining undetectable in steganography to strike a balance between these two criteria [11, 12].

With the use of the polynomial- and Knight-Tour-based PHLSB (Hash Least Significant Bit) technique, this research seeks to improve the security model of image steganography transmission. These are this task's main contributions:

- Created an adaptive bionic model for encrypting medical information for safe transmission across the Internet of Things.
- Another data encryption method known as steganography conceals sensitive information within other digital content, often known as a masked object.
- The approaches of polynomial-based hash least significant bit (PHLSB) and Night-Tour are combined to provide a hybrid approach to image steganography in this research.

- The amount of security certificates created over time will be affected by the plan after it is put into action and evaluated.
- In a diverse Internet of Things ecosystem, these certificates are used to verify IoT devices. We show that it is possible to swiftly and safely setup IoT devices to carry out particular activities by creating multiple security credentials at a time.

Section 2 extensively covers the in-depth examination of recent models, while Section 3 presents comprehensive details about the proposed model. In Section 4, the experimental setup and analysis are elaborated to evaluate the performance of the proposed model. Finally, Section 5 concludes by discussing potential avenues for future improvements in the current work.

2. Literature Survey

A thorough investigation into IoT security vulnerabilities was done in 2018 by Wang *et al.*, [13]. For various concerns like authentication, confidentiality, etc., it describes security controls. A paradigm for ensuring security for effective data transmission in IoT networks, the three-color image steganography technique, was put up by Murthy *et al.*, [14]. In the first and third of the three techniques, further security is provided via red, blue, and green channels, whilst green and blue are used in the second. The model was evaluated by Siva *et al.*, [15] using a dataset of medical photos, and they also suggested a method for obtaining images from intrusions. For encrypting medical photos, the AES encryption algorithm has long been a favorite method. But in terms of availability, authorization, and integrity, the suggested architecture aids in achieving security. Various streaming vulnerabilities and risk factors were described in a smartphone application that was released, which is vulnerable to medical streaming [16].

Using encryption and steganographic data concealment techniques, Meshram *et al.*, [17] suggested a secure data communication model. Secret text communications are encrypted through the use of a filter group encryption technique. For cover picture encryption in steganography, the discrete wavelet transform (DWT) is taken into consideration. The binary bit stream of text messages is transformed. The wavelet coefficients of the cover image conceal the transformed binary data. The performance of the reference design is examined using the histogram and PSNR values of the Stego image. We get to the conclusion that the model created utilizing the DWT function and filterbank encryption method boosts all data security on open channels and enhances system performance.

Qin *et al.*, [18] developed a novel solution. Information is kept within this system by LSB permutation at a particular place of a certain block. A polynomial with numerous coordinates is used to determine a specific block and position in order to get setting information. The secret key is used to solve the polynomial in this case. This strategy lessens the use of LSBs that are unstable. The payload can be raised by employing this strategy.

WSN energy harvesting application scenarios are another area of interest for research by Ge *et al.*, [19]. To help increase the security of energy harvesting in sensor networks and make the most of the energy that is already accessible, a trust-based secure routing solution is created in this work. To enable independent data verification and security, this procedure enables sources and sinks to communicate through different pathways. Furthermore, a probability-based backtracking technique is used to find malicious nodes.

ECC courtesy of Combine RSA security with reduced key sizes to implement safe key distribution or data exchange [20]. Additionally, the approach suggests that the aggregation node and base station server carry out mutual authentication. For the two-factor authentication process, the receiver's identity, random registration, and timestamp values are employed. The suggested approach improves the security of WSN-based medical equipment by detecting replay attacks.

Kumar *et al.*, [21] proposed an authentication system dependent on ECC for IoT and cloud servers in Smart Cities. The suggested system accomplishes mutual authentication and supports fundamental safety necessities. The informal security examination, performance analysis and contrast of the suggested system with existing systems prove that the suggested method is powerful, effective and stout as a counter to manifold security threats faced by Smart Cities. The formal confirmation of the suggested procedure is performed by AVISPA tools, which affirms its safety strength within the sight of a conceivable invader.

According to Batcha *et al.*, [22], safety and security system warn their guardian in person via GPS (Global Positioning System) and GSM (Global System for Mobile communication) security system in the case of an unpleasant or unforeseen incident. This system has a location tracker so that messages can be shown or asked for help.

3. Proposed Method

As cover items, the suggested method makes use of colored graphics. RGB color components from color pictures are created. Every component of color has information. Polynomials are employed as keys in the suggested system to conceal data. Before embedding, symmetric encryption should be used; then, the extraction procedure should be reversed to encrypt the secret. The HLSB (Hash Least Significant Bits Based) technique is used for embedding.

3.1 Steganography

Steganography is typically understood as a technique for concealing a secret message or its existence so that it cannot be recognized or detected. Steganography has several advantages over encryption, one of which is that it conceals the existence of a secret message, making a potentially hidden message less of a security target. However, modern steganography is far more complex and enables users to conceal enormous amounts of data in image, audio, and video files. This type of steganography is frequently combined with encryption to give double protection for data. It first encrypts the secret message and then hides it, requiring an opponent to first locate the message (sometimes a challenging operation in and of itself) and then decrypt it as demonstrated.

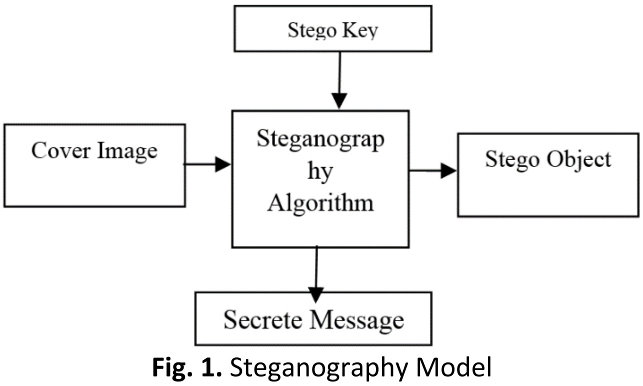

Fig. 1. Steganography Model

3.2 Knight Tour Algorithm

Several secret bitstreams can be created using the unique mathematical technique, Night Tour. The Knight algorithm employs the 8x8 segmented blocks from the cover picture to discover the Knight path in the input image. Left Square, Right Square, Right Diamond, and Left Diamond are the four groups of 4x4 blocks. Getting one square closer to the center of the board or each group of images is the basic goal of Night Tour. Replicate these actions for the remaining squares after finishing one. Photo of a single 4 by 4 block night tour is depicted in Figure 2.

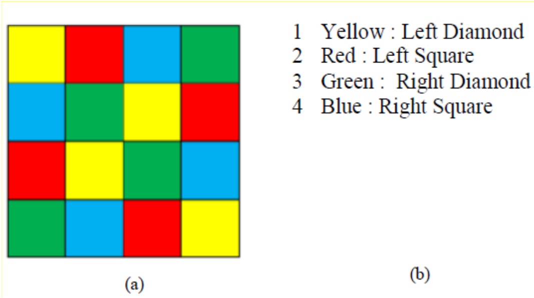

Fig. 2. Knight Tour (a) 4×4 Blocks of Pixels; (b) Pixel Name Plates

The working stages of the Night Tour algorithm are displayed in Algorithm 2.

Algorithm 2: Knight Tour System

```
Step 1: Take a look at an image of size nxm and break it down into blocks of 8x8 pixels.
Step 2: Visit each square in each block in accordance with the rules.
Step 3: You must cover 4 squares each time you move from one to the next.
Step 4: Repeat step 2 for the following group after fully advancing one colour.
Step 5: Carry out the exact same procedure for each pixel value.
```

3.3 Polynomial Equations

Polynomials are a powerful numerical tool. Polynomials are mathematical formulas with variables and locations that are only concerned with the work of addition, subtraction, repetition, and non-negative integer exponents. The following order is used to describe a polynomial of degree *n*.

$$ax^n + bx^{n-1} + \cdots + rx^1 + s = y \tag{1}$$

where *y* is the result for *x*, while *a*, *b*, *r*, and *s* are referred to as coefficients.

3.4 Symmetric encryption

By searching from the original form backwards, we can change knowledge in novel ways by using the cryptographic index, and so on. Knowledge may be encrypted and decrypted with the help of XOR, a fantastic tool.

The encrypted message will be "01010010" if we take the message "01011101" and the encryption key "00001111". "01011101" was the message found after searching.

3.5 LSB Method

The LSB method is one of the clearest and well-known steganographic methods. The hidden data in this method spells out the LSB component of each pixel in the covered object. Direct detection of implanted particles via a planned search approach is made possible by the LSB method's simplicity.

It used an 8-bit color scheme, with 24 bits used to describe each pixel. 3 bits are covered by each pixel. As a covering object for knowledge, imagine a grid of three pixels in an image.
The following list shows the values of each pixel that correlate to the color components.

	R	G	B
P1	39	64	152
P2	48	229	178
P3	186	75	25

The pixels are represented as binary data by
(00100111 01000000 01111101
00110000 11100101 10110010
10111010 01001011 00011001)
The letter A, which has the binary representation '10000011', is ingrained in the LSBs of the pel, and the ensuing grid is as a result.
(00100111 01000000 01111100
00110000 11100100 10110010
10111011 01001011 00011001)
The highlighted three are warped in accordance with the concealed message, but the characters are fixed to the top 8 of the grid. On average, half of the image bits are altered to obscure the hidden message.

3.6 Hash LSB

The HLSB technique is used to define the location where the data should be protected. The position of the bit of pel is determined by the hash function. To distinguish the location LSB of the pel, equation (2) is used.

$$q = b\%m \tag{2}$$

where q is the bit position of pel. b represents the pixel position and m represents the number. If the q = 0 bit is stored in the 0th position of the pixel, the q = 1 bit is placed in the 1st position of the pixel, and the q = 2 bit is recorded in the 2nd position of the pixel, then the 7th bit is the MSB and the 0th Bits are LSB.

Embedding Process

Let I be the original 8-bit color image as cover of size m x n and characterized as

$$I = \begin{cases} x(i,j,k)\ 0 \le i \le m, 0 \le j \le n, 0 \le k \le 2 \\ \qquad\qquad x(i,j) \in \{0,1,2,\dots,255\} \end{cases} \tag{3}$$

where the color component of the color image is represented by k, the row by i, and the column by j.
Step 1: To choose the hidden message and convert it to binary using ASCII.

$$M = \{m_i | 0 \le i \le N, m_i \in \{0,1\}\} \tag{4}$$

N denotes the quantity of hidden information in this situation.
Step 2: Use the encryption key K to encrypt the message. It is defined as follows:

$$K = k_i \big| 0 \le i \le N, k_i \in \{0,1\}\big\} \tag{5}$$

The ultimate secrete information $\widehat{M}$ for hiding is obtain by XOR operation of M and K represented as

$$\widehat{M} = \widehat{m_\imath} | \widehat{m_\imath} = m_i \otimes k_i \tag{6}$$

Where $\otimes$ denotes XOR operation.
Step 3: mn x 3 matrix shape from the cover image.

$$C = \big\{c_{ik} \big| 0 \le i \le mn, 0 \le k \le 2, c_{ik} \in \{0,1,2,\ldots,255\}\big\} \tag{7}$$

The cover is divided into colour components here. Each layer is m x n in size, and after being transformed into a vector, we concatenate all the vectors that correspond to the colour components.
Step 4: Create polynomial data using a polynomial equation that serves as a secret key. The G order polynomial equation has the following form:

$$P(x) = ax^G + bx^{G-1} + \cdots + rx^1 + s \tag{8}$$

Where a, b, r and s are scalars and Determine whether the secret information's size exceeds the picture vector's by how much, and then choose the most appropriate cover item.
Step 5: Determine P(x) for each element in the image vector that needs to have information hidden.

$$H = \big\{\vdash c_{ik} \dashv \big| j = P(x),\ 0 \le k \le 2, c_{\downarrow ik} \in \{0,1,2,\ldots,255\}\big\} \tag{9}$$

where j is a component of a pixel and H is a representation in an intensity vector of the color component of the corresponding component of an element in the image vector.
Step 6: Choose three pieces from the previous secret to hide in a row. For information concealment in H, use HLSB.
Step 7: Image vector m x n x k should be reordered. The following definition of a steganographic image:

$$I = \begin{cases} x(\imath,\jmath,k)\ 0 \le \imath \widehat{\le m, 0} \le \jmath \le n, 0 \le k \le 2 \\ \qquad\qquad \hat{x}(\imath,\jmath) \in \{0,1,2,\ldots,255\} \end{cases} \tag{10}$$

Extracting process

The hidden information can be inferred throughout the extraction process without any connection to the primary cover item. In the extraction process, there are the following steps.
Step 1: Convert the Stego image $\hat{I}\hat{I}$ into mn x 3 matrix form as

$$\hat{C} = \big\{\hat{c}_{ik} \big| 0 \le i \le mn, 0 \le k \le 2, \hat{c}_{ik} \in \{0,1,2,\ldots,255\}\big\} \tag{11}$$

Step 2: Create P(x) polynomial data.
Step 3: To find the corresponding element in the image vector that contains the concealed information for x using the P(x) function.

Step 4: Use HLSB extraction to separate the three sequential pieces of the ultimate secret information. The most closely guarded knowledge is

$$\hat{M} = \{\widehat{m_i} | 0 \leq i \leq N\} \tag{12}$$

Step 5: Utilize encryption key K to decrypt the data. K is specified as

$$K = \{k_i | 0 \leq i \leq N, k_i \in \{0,1\}\} \tag{13}$$

Step 6: As a result of the XOR operation between and K, the secret information is obtained after decryption and expressed as

$$M = \{m_i | m_i = \widehat{m_i} \otimes k_i\} \tag{14}$$

4. Result and discussion

The performance of steganography is otherwise reported and evaluated in this section. RKGM, ECC, CPAB-KSDS, and the suggested approach (Knight-tour with PHLSB) that was simulatively tested using the NS-2 simulator are among the methods that are being compared. Throughput, energy use, end-to-end latency, and network durability are among the metrics used for comparison. Table 1 is a listing of the simulation parameters that were employed.

Table 1
Simulation Parameters

Parameter	Values
No. of Nodes	100
Area Size	1100×1100 m
Mac	802.11
Radio Range	250m
Simulation Time	60 sec
Packet Size	80 ytes

4.1 End-to-End Delay

The average amount of time it takes for a packet to travel through a network from its source to its destination.

$$End - to - End\ delay = \frac{\sum_{i=1}^{n}(t_{ri} - t_{si})}{n} \tag{15}$$

where tri is the time at which the i-th data packet is received, tsi is the time at which the i-th data packet is sent, and n is the total number of data packets.

The evaluation comparison for end-to-end latency performance is shown in Table 2 with the nodes on the x-axis and the end-to-end latency value on the y-axis. RKGM, ECC, CPAB-KSDS, and the suggested approach with decreased end-to-end latency are the methods that are being compared. As a result, the suggested system chooses good repeater nodes based on the fitness value. Table 6 displays the findings of an end-to-end latency performance analysis employing Knight-tour and PHLSB, as well as the more well-known methods RKGM, ECC, and CPAB-KSDS. Send packets to the most effective intermediary nodes for optimal functionality. RKGM, ECC, and CPAB-KSDS are common methods for finding endpoint nodes fast. Additionally, the present technique only forwards the response message to the source node once the destination node has been determined. In contrast, the Knight-tour with PHLSB method is faster end-to-end than systems that are connected to the internet. The table makes it abundantly evident that the suggested solution has a shorter time delay than traditional ways.

Table 2
End-to-End Delay

No. of Nodes	RKGM	ECC	CPAB-KSDS	Proposed
100	40	30	20	15
200	38	27	17	11
300	34	23	14	9
400	30	20	10	7
500	27	18	9	5

4.2 Throughput

The frequency of successful network data packet transmission.

$$Throughput = \frac{Total\ number\ of\ Packets\ sent}{Time} \tag{16}$$

Whereas the nodes are on the x-axis and the throughput value is shown on the y-axis in Table 3, the evaluation comparison in terms of throughput performance is shown there as well. The proposed technique has a greater throughput than RKGM, ECC, and CPAB-KSDS in the comparison of the three methods. In light of the fitness value, the suggested system chooses good repeater nodes.

Table 3
Throughput

No. of Nodes	RKGM	ECC	CPAB-KSDS	Proposed
100	65	69	72	75
200	68	71	75	79
300	72	74	78	83
400	75	77	81	85
500	77	8	83	88

4.3 Energy Consumption

The amount of energy required on average to send a packet to a network node over a given time period is known as energy consumption.

$$Energy(e) = [(2 * pi - 1)(e_t + e_r)]d \tag{17}$$

where pi is the packet, et is the transmitted energy of packet i, er is the energy needed to receive packet i, and d is the distance between the transmitting node and the destination node.

Table 4 compares evaluations based on how well they affected energy consumption. Nodes are shown on the x-axis in this graph, and values for energy consumption are shown on the y-axis. The approaches up for comparison include RKGM, ECC, CPAB-KSDS, and the suggested low-energy method. In light of the fitness value, the suggested system chooses good repeater nodes. The performance analysis for energy consumption scenarios is shown in Table 4 along with night tours of the proposed PHLSB and related systems like RKGM, ECC, and CPAB-KSDS. The suggested method entangles fewer nodes during packet promotion compared to the three already known methods. More energy is kept in reserve in the nodes since the highest optimization factor is continually reached in terms of packet forwarding priority. But the extra node needs to send the equivalent packets from the current system. RKGM, ECC, and CPAB-KSDS techniques that are conventionally used thereby consume more energy.

Table 4
Energy Consumption

No. of Nodes	RKGM	ECC	CPAB-KSDS	Proposed
100	18	15	11	9
200	15	13	9	7
300	13	11	7	5
400	11	9	5	3
500	3	7	3	1

4.4 Network Lifetime

The lifetime of a network is expressed as

$$Lifetime\ E[L] = \frac{\varepsilon_0 - E[E_w]}{P + \lambda E[E_r]} \tag{18}$$

where P is the network's average sensor reporting rate, 0 is the total non-rechargeable initial energy, E[EW] is the anticipated wasted or unused energy before network termination, and E[Er] is the consumption of the energy reporting nodes.

The evaluation comparison is shown in Table 5 in terms of network lifetime performance, with the nodes on the x-axis and the network lifetime value on the y-axis. The compared methods are RKGM, ECC, CPAB-KSDS and the proposed method shows higher network lifetime. The suggested approach chooses good repeater nodes as a result based on fitness value. The Knight-Tour with PHLSB and cutting-edge RKGM, ECC, and CPAB-KSDS network lifespan performance analysis is displayed in Table 5 along with other relevant data. The proposed method outperforms the conventional methods, as demonstrated in Table 5, which is a comparison. Conventional RKGM, ECC, and CPAB-KSDS systems permit more sensor nodes to haphazardly launch packet transfers as the number of nodes in the network rises. Routing packets to the best nodes is one method that has been proposed for extending battery and network life. The comparison of the performance of packet rates is shown in Table 5. The results show that, when compared to the state-of-the-art, Knight-Tour employing the suggested PHLSB approach in Table 5 extends the network lifetime of some nodes.

Table 5
Network Lifetime

No. of Nodes	RKGM	ECC	CPAB-KSDS	Proposed
100	5	8	15	19
200	10	12	19	25
300	14	16	24	29
400	18	20	28	34
500	22	24	33	39

4.5 Packet Drop Ratio

PDR is used to express the proportion of lost packets to all packets sent.

$$Packet\ loss\ ratio = \frac{N^{tx} - N^{rx}}{N^{tx}} \times 100\% \quad (19)$$

where Ntx stands for transmitted packets and Nrx for received packets. The sizes of each transmitted and received real-time packet are extracted for this evaluation.

The evaluation comparison for PDR performance is shown in Table 6, where the nodes are on the x-axis and the PDR value is on the y-axis. RKGM, ECC, CPAB-KSDS, and the suggested approach with low PDR were the methodologies that were compared. As a result, the suggested system chooses good repeater nodes based on the fitness value.

Table 6
PDR

No. of Nodes	RKGM	ECC	CPAB-KSDS	Proposed
100	95	93	9	85
200	98	96	92	88
300	102	99	95	92
400	106	103	98	96
500	108	106	102	100

5. Conclusion

The PHLSB and Knight-Tour steganography algorithms are nicely implemented in this work. We create a novel method for protecting data in this white paper. While security and efficiency are perceived to be high, transparency is perceived to be low. The application of Knight Tour algorithm enhances data hiding level in the cover image. According to the findings, the proposed method outperforms more established ones in terms of throughput, network lifetime, end-to-end delay, packet loss rate, and energy consumption. To support the suggested strategy, many polynomials of various orders are examined. The outcomes demonstrate the PHLSB method's superior embedding capacity. The computational complexity problem could be greatly handled in the future with the development of hybrid techniques and new encryption algorithms.

Acknowledgement

The authors wish to express their thanks to one and all who supported them during this work. The authors received no specific funding for this study. The authors declare that they have no conflicts of interest to report regarding the present study**.**

References

[1] Samara, Ghassan, and Mohammad Aljaidi. "Efficient energy, cost reduction, and QoS based routing protocol for wireless sensor networks." *arXiv preprint arXiv:1903.09636* (2019). https://doi.org/10.11591/ijece.v9i1.pp497-504.

[2] Yarinezhad, Ramin. “Reducing Delay and Prolonging the Lifetime of Wireless Sensor Network Using Efficient Routing Protocol Based on Mobile Sink and Virtual Infrastructure.” *Ad Hoc Networks* 84 (2019): 42–55. https://doi.org/10.1016/j.adhoc.2018.09.016.

[3] Natarajan, Yuvaraj, Kannan Srihari, Gaurav Dhiman, Selvaraj Chandragandhi, Mehdi Gheisari, Yang Liu, Cheng-Chi Lee, Krishna Kant Singh, Kusum Yadav, and Hadeel Fahad Alharbi. “An IoT and Machine Learning-based Routing Protocol for Reconfigurable Engineering Application.” *IET Communications* 16, no. 5 (2022): 464–75. https://doi.org/10.1049/cmu2.12266.

[4] Tabrizchi, Hamed, and Marjan Kuchaki Rafsanjani. “A Survey on Security Challenges in Cloud Computing: Issues, Threats, and Solutions.” *The Journal of Supercomputing* 76, no. 12 (2020): 9493–9532. https://doi.org/10.1007/s11227-020-03213-1.

[5] Liu, Pengtao. "Public-Key Encryption Secure against Related Randomness Attacks for Improved End-to-End Security of Cloud/Edge Computing." *IEEE Access: Practical Innovations, Open Solutions* 8 (2020): 16750–59. https://doi.org/10.1109/access.2020.2967457.

[6] Garg, Priyansha, Moolchand Sharma, Shivani Agrawal, and Yastika Kumar. "Security on Cloud Computing Using Split Algorithm along with Cryptography and Steganography." In *International Conference on Innovative Computing and Communications*, 71–79. Singapore: Springer Singapore, 2019. https://doi.org/10.1007/978-981-13-2324-9_8

[7] Pradeep, K. V., V. Vijayakumar, and V. Subramaniyaswamy. "An Efficient Framework for Sharing a File in a Secure Manner Using Asymmetric Key Distribution Management in Cloud Environment." *Journal of Computer Networks and Communications* 2019 (2019): 1–8. https://doi.org/10.1155/2019/9852472.

[8] Hidayat, Taufik, D. Sianturi Tigor Franky, and Rahutomo Mahardiko. "Forecast Analysis of Research Chance on AES Algorithm to Encrypt during Data Transmission on Cloud Computing." In *2020 2nd International Conference on Broadband Communications, Wireless Sensors and Powering (BCWSP)*. IEEE, 2020. https://doi.org/10.1109/BCWSP50066.2020.9249478

[9] Namasudra, Suyel, Debashree Devi, Seifedine Kadry, Revathi Sundarasekar, and A. Shanthini. "Towards DNA Based Data Security in the Cloud Computing Environment." *Computer Communications* 151 (2020): 539–47. https://doi.org/10.1016/j.comcom.2019.12.041.

[10] Upreti, Kamal, Binu Kuriakose Vargis, Rituraj Jain, and Makarand Upadhyaya. "Analytical Study on Performance of Cloud Computing with Respect to Data Security." In *2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS)*. IEEE, 2021. https://doi.org/10.1109/ICICCS51141.2021.9432268

[11] Gupta, Rishabh, Deepika Saxena, and Ashutosh Kumar Singh. "Data Security and Privacy in Cloud Computing: Concepts and Emerging Trends." *ArXiv [Cs.CR]*, 2021. http://arxiv.org/abs/2108.09508.

[12] Luo, Wei, and Wenping Ma. "Secure and Efficient Data Sharing Scheme Based on Certificateless Hybrid Signcryption for Cloud Storage." *Electronics* 8, no. 5 (2019): 590. https://doi.org/10.3390/electronics8050590.

[13] Wang, Zhiying, Nianxin Wang, Xiang Su, and Shilun Ge. "An Empirical Study on Business Analytics Affordances Enhancing the Management of Cloud Computing Data Security." *International Journal of Information Management* 50 (2020): 387–94. https://doi.org/10.1016/j.ijinfomgt.2019.09.002.

[14] Murthy, Ch V. N. U. Bharathi, M. Lawanya Shri, Seifedine Kadry, and Sangsoon Lim. "Blockchain Based Cloud Computing: Architecture and Research Challenges." *IEEE Access: Practical Innovations, Open Solutions* 8 (2020): 205190–205. https://doi.org/10.1109/access.2020.3036812.

[15] Siva Kumar, A., S. Godfrey Winster, and R. Ramesh. "Efficient Sensitivity Orient Blockchain Encryption for Improved Data Security in Cloud." *Concurrent Engineering, Research, and Applications* 29, no. 3 (2021): 249–57. https://doi.org/10.1177/1063293x211008586.

[16] Eltayieb, Nabeil, Rashad Elhabob, Alzubair Hassan, and Fagen Li. "A Blockchain-Based Attribute-Based Signcryption Scheme to Secure Data Sharing in the Cloud." *Journal of Systems Architecture* 102, no. 101653 (2020): 101653. https://doi.org/10.1016/j.sysarc.2019.101653.

[17] Meshram, Chandrashekhar, Cheng-Chi Lee, Sarita Gajbhiye Meshram, and Muhammad Khurram Khan. "An Identity-Based Encryption Technique Using Subtree for Fuzzy User Data Sharing under Cloud Computing Environment." *Soft Computing* 23, no. 24 (2019): 13127–38. https://doi.org/10.1007/s00500-019-03855-1.

[18] Qin, Xuanmei, Yongfeng Huang, Zhen Yang, and Xing Li. "A Blockchain-Based Access Control Scheme with Multiple Attribute Authorities for Secure Cloud Data Sharing." *Journal of Systems Architecture* 112, no. 101854 (2021): 101854. https://doi.org/10.1016/j.sysarc.2020.101854.

[19] Ge, Chunpeng, Willy Susilo, Zhe Liu, Jinyue Xia, Pawel Szalachowski, and Fang Liming. "Secure Keyword Search and Data Sharing Mechanism for Cloud Computing." *IEEE Transactions on Dependable and Secure Computing*, 2020, 1–1. https://doi.org/10.1109/tdsc.2020.2963978.

[20] Huang, Hui, Xiaofeng Chen, and Jianfeng Wang. "Blockchain-Based Multiple Groups Data Sharing with Anonymity and Traceability." *Science China Information Sciences* 63, no. 3 (2020). https://doi.org/10.1007/s11432-018-9781-0.

[21] Kumar, Ajay, Kumar Abhishek, Xuan Liu, and Anandakumar Haldorai. "An Efficient Privacy-Preserving ID Centric Authentication in IoT Based Cloud Servers for Sustainable Smart Cities." *Wireless Personal Communications* 117, no. 4 (2021): 3229–53. https://doi.org/10.1007/s11277-020-07979-8.

[22] Batcha, S. Sheikameer, Pushpalatha, Nitinchand, Bhavatarini Rv, Boopathiraja, and Sanjai. "Multi-Purpose Security and Protection Padlock with a Tiny, Handheld Device Using IoT." In *2022 8th International Conference on Smart Structures and Systems (ICSSS)*. IEEE, 2022. https://doi.org/10.1109/ICSSS54381.2022.9782163