SIN-CHN SCIENTIFIC PRESS PTE.LTD.

Molecular & Cellular Biomechanics 2024, 21(2), 367.
https://doi.org/10.62617/mcb.v21i2.367

Article

Media image transmission and privacy protection for internet of things security

Huibao Wen

College of humanities and law, Harbin University, Harbin 150086, China; huibaow@hrbu.edu.cn

CITATION

Wen H. Media image transmission and privacy protection for internet of things security. Molecular & Cellular Biomechanics. 2024; 21(2): 367. https://doi.org/10.62617/mcb.v21i2.367

ARTICLE INFO

Received: 14 September 2024
Accepted: 30 September 2024
Available online: 6 November 2024

Abstract: Internet of Things (IoT) is becoming more popular with the increase in advancements of technology and is widely used in various sectors. The data are collected from the real environment and then transmitted over the networks. Due to their restricted resources, processing capacity, and memory, IoT gadgets are susceptible to certain security risks. Several encryption methodologies were established to provide safe communication between IoT devices with minimal computing cost and bandwidth consumption, due to the rise in media date. This research proposes a revolutionary compact pixel crypto (CPC) technique that can accommodate the modest transmission speeds of IoT gadgets. The suggested techniques reduces the computational burden and data quantity by encrypting the image data using pixel driven selective encryption and bloke scanning compression. The suggested method's effectiveness is examined using the network simulator (NS-2) platform. According to the findings of the experiments, the suggested method outperforms the previous approaches in terms of both packet rate and energy usage. The proposed approach shortens the time needed for node side encryption and decryption operations with improving the system's energy effectiveness and connectivity performance.

Keywords: index terms-security; Internet of Things (IoT); encryption; compact pixel crypto (CPC); energy usage; transmission speed

1. Introduction

Multimedia data exchange has increased dramatically because of the growth of social media networks, creating a new area in the Multimodal IoT. Due to the combination of various formatting types such as media, data sources, and resolutions, multimedia communication is portrayed to be complex in nature. But security considerations related with data confidentiality and privacy is of low priority and unmanaged. For end-to-end secure communication on devices with low resources, compact algorithms for encryption have been devised to guarantee confidentiality [1,2].The IoT is a network of interconnected devices used in various applications, like intelligent transportation and healthcare. They communicate with physical things using sensors, communication units, radio frequency identification tags, and digital actuators, but often have low bandwidth and limited processing power [3,4]. Attacks and hackers pose a significant threat to the confidentiality, anonymity, and reliability of audiovisual information transfer and preservation, which is crucial for applications that use multimedia on networked devices, as it restores uniqueness and protects privacy [5,6].Global interactions, communication exchange, decision-making, news collecting, social engagement, and information distribution are made easier by social networking networks. Digital images are the main form of communication; people share billions of images every day [7]. Digital electronics and Bluetooth

communications have made it possible to build low-cost, multipurpose sensor nodes that consume little energy for the IoT device [8,9]. Collectively, these dispersed nodes facilitate the transmission of information in the monitoring area. Depending on the various sensor networks it connects with, the destination node has the option to use the aggregated data locally [10]. Plain text input, cipher text output, and keys make up a traditional cryptography system. The cipher code is produced during the encryption procedure phase, and the plain text is extracted during the decryption step [11]. To protect data, respond to threats, and reduce data load size, a variety of cryptographic techniques are employed. Consideration is given to reliability, which is demonstrated by elements including scaling and cropping. To safeguard data while it is being sent, many mathematical computations must be performed [12]. However, due to constraints in analyzing, energy, storage, and communication capacities, cloud-based bulk storage and intense calculations are frequently wasteful. As a result, Mobile Cloud Computing (MCC) has emerged as a cutting-edge solution that combines several technologies to optimize the functionality and capacity of current infrastructure [13]. The IoT and mobile edge computing (MEC) may have difficulty fulfilling future demand as a result of technological advancements aimed at lowering network traffic and data transfer. In the IoT, wireless sensor networks (WSNs) are a major source of large data and employed in smart cyber-physical systems (SCPS). To entering a new era of intelligent IoT applications as wireless sensor technologies advance. Because the IoT has made it possible to connect to devices worldwide, it is crucial for IoT applications [14,15].The aim of the study suggest an approach that blocks images and takes pixel correlation into account to shorten encryption execution time, lower node power consumption, and enhance service quality. In comparison to the basic approach, the suggested algorithm uses less energy and packets, improves service quality and energy consumption, and shortens node execution times.

Key contributions

- In this research we proposed a new compact pixel crypto (CPC) technique for transmitting the image data to the IoT gadgets.
- The study used block scanning compression and pixel-driven selective encryption to encrypt the standard test pictures in a secure data transmission procedure approach that lowers the amount of data and computing load.
- The image is encrypted in the model of block and scan based encryption technique, then the data are transmitted. The quality of the transmitted image is analyzed by the various techniques.

The next portion of the study is Portion 2: Literature Review of Secured Image Transmission Method and Encryption Schemes, Portion 3: The recommended data reduction process is given, along with an explanation of the single-round light-weight cryptography algorithm's architecture. Portion 4: Result with Discussion of the research and Portion 5: Conclusion of the study.

2. Literature review

Kaur et al. [16] focused on protecting biomedical image transmission and retrieval via IoT networks and proposed an energy-efficient and secure IoT paradigm

for e-health. The model is limited by a hyper-parameter tuning issue and employs compressive sensing and five-dimensional hyper-chaotic map encryption. To overcome this problem, a θ-non-dominated sorting genetic algorithm III (θ-NSGA-III)-based Five-Dimensional Hyper-Chaotic Map (FDHC) is suggested. The method works better than the recent image encryption approaches and sensitive to input images, which makes it appropriate for secure communication in green IoT networks. Li et al. [17] suggested a Self-Supervised Dynamic Learning (SSDL)technique for high-fidelity, long-term optical field transfer via unstable Multimode Fibers (MMFs). Robust image recovery is ensured by using several networks that adaptively update and ensemble to carry Long- and short-term memories (LSTM) of changes made to the transmission model. Static Optic Diffusion Simulation using a calibrated, the transmission Matrix, which is utilized for multi-mode fiber pathways is prone to degradation over time. Wang et al. [18] suggestedprivacy-preserving cross-media retrieval (PPCMR) on encrypted data in cloud computing. This method enhances protection by encryption data before transferring it to the cloud. Convolutional neural networks (CNNs) are used for extracting cross-media features from data that is encrypted, which solves the "semantic gap" problem. The user decrypts the encoded retrieval information to receive the cross-media unencrypted results. On mobile devices and vast, constantly updated databases in the cloud, PPCMR performs better than plaintext retrieval techniques and provides effective cross-media encrypted retrieval.To solve storage space waste and enable the decryption of some portions in encrypted images before the complete information is decrypted; Jang and Lee [19] proposed a technique for partly encrypting private information in images using FF1 stands for Format-Preserving Encryption (FPE) 1 and FF3-1 stands for FPE 3. **Table 1** summarizes the overall literature reviews on this transmission of media images and safeguarding privacy for the security of the IoT.

Table 1. Image transmission security enhancement-based literature review.

Reference	Transmission Method	Domain of the Research	Purpose of the Research
Kaur et al. 2021 [16]	FDHC, θ-NSGA-III, and Permutation and Diffusion	E-Health	Develop a secure, energy-efficient IoT model for e-health. Secure biomedical image transmission and retrieval. Improve FDHC performance with θ-NSGA-III. Outperform current image encryption techniques in green IoT networks.
Li et al. 2024 [17]	SSDL, Data-Driven Learning and Static Optic Diffusion Model with Set up Emission Matrix	Optical Communication	Long-Term Transmission in MMF Addresses variability and scattering in MMF channels. Proposes SSDL approach for high-fidelity transmission. Offers insights for enhanced optical communication and remote imaging.
Wang et al. 2023 [18]	PPCMR and CNN	Cloud Computing and Data Security	Improves retrieval of cross-media information from huge, changing datasets. Transfers intricate computational duties from user to cloud server.
Jang and Lee (2020) [19]	FF1and FF3-1 for encryption and NIST SP 800-22 for analysis	Image Security And Privacy Applications	Enhancing Image Security and Privacy. The technique selectively decrypts encrypted images. Encrypts sensitive information without data expansion.

Jayaraman et al. [20] tackled the problem of IoT privacy preservation by putting up creative ideas, presenting a privacy-preserving IoT architecture, and putting in a

place productive proof of concept system. To protect data privacy, the methods make use of many IoT cloud data repositories. Open IoT extensions, a popular open-source platform for IoT application development, serve as the foundation for both the design and the proof-of-concept implementation. This guarantees the privacy of IoT data. Ma et al. [21] presented a privacy-preserving thumbnail-preserving encryption (TPE) strategy for JPEG image retrieval that guarantees excellent TPE for cipher text images and minimal file expansion while improving efficiency and accuracy. The TPE approach combines information embedding and Huffman coding techniques to enable precise and excellent decryption of encrypted images. For better format compatibility and to minimize cipher text file expansion, the approach additionally takes JPEG compression into account. Key storage is reduced and security is improved by the adaptive encryption key generation. For submitted TPE-encrypted images, the cloud creates preview thumbnails. Elhoseny et al. [22] utilized a cryptographic model and optimization techniques to study the security of medical images in the IoT. They emphasized the importance of security as the hospital patient data is stored on cloud servers. They chose a new framework using hybrid swarm optimization, combining particle swarm and grasshopper swarm optimization in elliptic curve cryptography (ECC), to enhance encryption and decoding security, thereby protecting medical images in the IoT framework. Jadaun et al. [23] provided a symmetric key lightweight (SKLW) approach that uses a reversible data concealing mechanism and image encryption to provide safe data transfer of text and images. With a graphical user interface for real-time image capture, the system is built to support a variety of image formats. Salim et al. [24] utilizing the multi-field image, the Advanced Encryption Standard (AES) single key encryption of images leaves them open to attack. To increase the security of images exchanged over the IoT, this research suggests the multiple key AES algorithm. **Table 2** summarizes the overall literature reviews on this transporting media images encryption method-based IoT device.

Table 2. Image transmission encryption-based literature review.

Reference	Encryption Method	Domain of the Research	Purpose of the Research
Jayaraman et al. 2019 [20]	Privacy-Preserving Techniques, Paillier Cryptosystem, and Quantization	Creating IoT Privacy Solutions	Addressing privacy preservation in IoT systems. Preventing unwanted access to sensitive data. Guaranteeing privacy protection throughout the data lifecycle.
Ma et al. 2023 [21]	TPE with Huffman coding techniques	privacy-preserving JPEG image retrieval scheme	Proposal for Privacy-Preserving JPEG Image Retrieval Scheme Enhances efficiency and accuracy. Ensures low-file expansion. Provides excellent thumbnail-preserving accuracy.
Elhoseny et al. 2020 [22]	Hybrid swarm optimization, combining particle swarm and grasshopper swarm optimization in ECC	Medical Image Processing	Proposing innovative cryptographic model. Utilizing optimization strategies for secure patient information transmission and storage.
Jadaun et al. 2021 [23]	SKLW	IoT Data Transmission	Implementing SKLW algorithm. Utilizing image encryption and reversible data hiding systems.
Salim et al. 2021[24]	AES and MECCAES	Multimedia IoT	MECCAES Enhances IoT Image Security Increases confidentiality. Encourages effective use across IoT fields.

3. Methodology

The proposed encryption technique intends to preserve media security while increasing data transmission efficiency by reducing the transfer of information between nodes and lowering encryption difficulty by emphasizing essential image pixels-driven. The main contributions are a method for removing significant portions of an image and reducing transmitted data by correlating insignificant data with important ones, a lightweight combined method of image cryptography that uses separate techniques to encrypt both significant and insignificant pixels, and a performance evaluation using NS2 simulations. A drawing presenting the suggested strategy is provided, with further information in the parts that follow. The image encryption process in both receiver and transmitter nodes occurs after key sharing. **Figure 1** illustrates the method flow of this research.

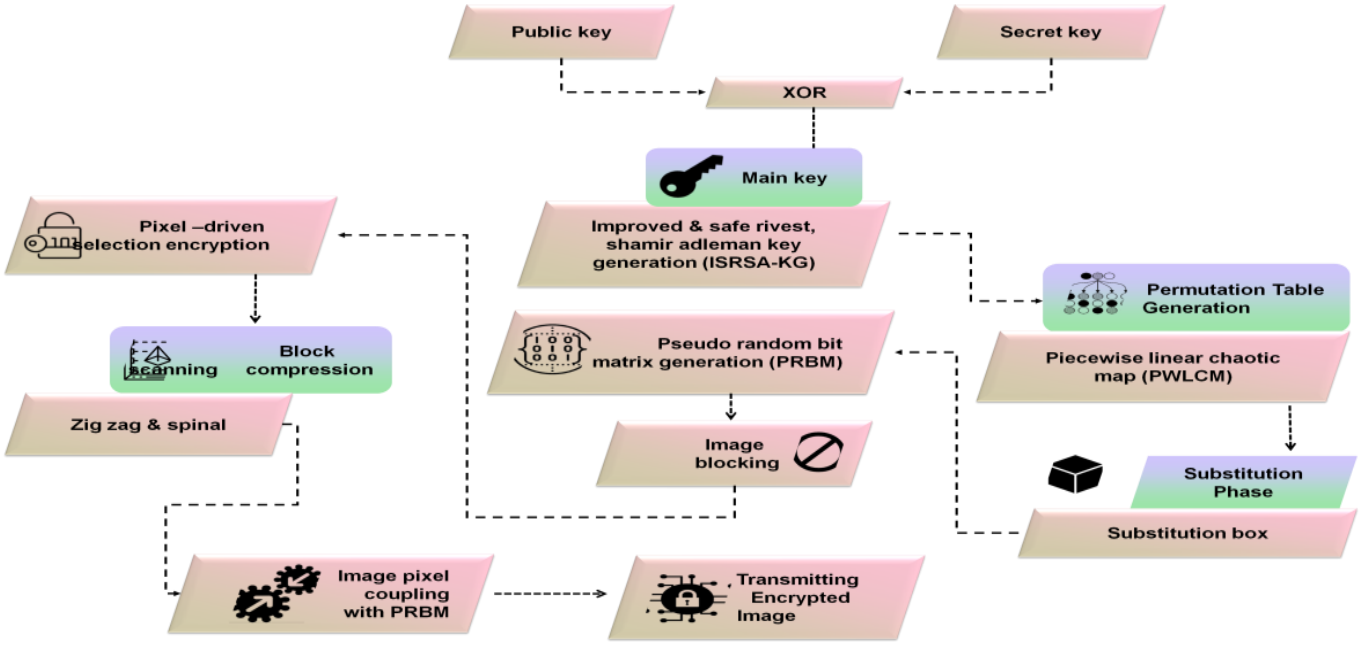


Figure 1. Overall research work.

3.1. Key generation

The proposed approach entails creating four sub-keys in addition to the main secret key, which is utilized for a distinct cryptographic function. The parties share the most recent secret key, which is changed to improve security, after authentication. For secure image transfer, the improved and safe Rivest, Shamir, Adleman key generation (ISRSA-KG) method algorithm offers a safe way to generate public and private keys. The modulus N is computed using four huge random primes, and the Euler's totient function for N and its factors is computed. The public and private key exponents are calculated using randomly generated numbers that fall in predetermined ranges by the method, which guarantees that the keys are substantially prime to the totient function depicted in Algorithm 1.

Algorithm 1 ISRSA-KG

Key Generation

1: Generation 4 large random primes as *b*, *a*, *d*, and *c* where $b \neq a \neq d \neq c$

2: Compute modulus $m = b \times a$, $n = d \times c$, $M = m \times n$

3: Analyse the Euler-totient occupation as:

$$\varphi(m) = (b-1) \times (a-1)$$
$$\varphi(m) = (c-1) \times (d-1)$$
$$\varphi(M) = \varphi(m) \times \varphi(m)$$

4: Evaluate random integer $f1$ which is such that:

$$1 < f1 < \varphi(m)$$
$$HDCof\big(f1, \varphi(m)\big) = 1$$

5: similarly, Evaluate $f2$ which is also a random integer such that:

$$1 < f2 < \varphi(m)$$
$$HDCof\big(f2, \varphi(m)\big) = 1$$

6: Now compute $F1 = f1^{\,f2} \mathrm{mod} M$

7: Finally, compute public key supporter F such that:

$$1 < F < \varphi(m) \times F1$$
$$HDCof(F, \varphi(m) \times F1) = 1$$

8: For the purpose to calculate the private key modulus *C*, $F \times C = 1 \times mod\ \varphi(M) \times F1$

9: Ultimately, the produced pairs of keys are:

Public-key = (F, m) and,

Private-key = (C, m)

3.2. Permutation step

Algorithm 2 Permutation

1: Input: Color image *J*, Secret key $l_1 = (w_0, z)$chaoticmap (1).

2: Output: Image vector that is jumbled *o*.

3: Convert the JIN image with size *M* into digital form *N*, where $M = b \times a \times 3$ and b, b are the counts of rows and columns in *M*, in turn, and N is a matrix of numbers with integer elements ranging from 0 to 255 of rank

4: Convert the matrix *M* to a one-dimensional form array $Y = \{y1, y2, \ldots, yM\}$.

5: Using the key l_1, iterate the chaotic map (1) to generate the pattern *B* = {b1, b2, ..., bM }.

6: Arrange the B sequence in an ascending sequence to create $A = \{a1, a2, \ldots, aM\}$.

7: Considering the sequencing' connection BandA, $a_j = b_{s_j}, forj = 1, \ldots, M$, the calculation of the vector of permutations is $S = \{s_1, s_2, \ldots, s_M\}$.

8: To change the positions of the items in vector *Y*, use *S*.

9: Following Y's permutations, it turns into$o = \{o_1, o_2, o_3 \ldots, o_M\}$.

The process entails using a permutation to change the color image I's pixel placements. Piecewise linear chaotic map (PWLCM), a multi-segmental map with dynamic qualities such as uniform density function, big positive Lyapunov exponent, and random behavior is used to construct the permutation array. PWLCM is helpful in cryptography. Here, $z \in (0, 0.5)$ is the controlling variable, and w_0 is the chaotic map's starting setup. $w_0 \in [0, 1)$. Ergodicity, misunderstandings, and an uneven distribution characterize the PWLCM output. Based on an external secret key, the method of operation of the components associated with the utilized chaotic map (1) is

included in l_1, which is$l_1 = (w_0, z)$, where $z \in (0, 0.5)$ and $w_0 \in (0, 1)$ represent the coefficients of (1) are depicted in Algorithm 2.

3.3. Substitution

The approach reduces the correlation between surrounding data and creates non-linearity in the encryption process by using a substitution box, or S-box depicted in Algorithm 3. This method improves defense against linear and differential cryptanalysis by masking the statistical characteristics of the data. The approach reduces the connection between nearby data by creating an S-box using a 8×8 chaotic map and utilizing a look-up table for image encryption devices in **Figure 2**. This method is essential for avoiding data corruption and improving the scheme's security.

S-Box

26	51	34	10	22	62	15	60
13	30	28	48	55	20	53	41
49	11	35	46	5	29	42	6
1	36	24	19	31	61	38	56
43	21	12	8	54	3	16	58
7	9	57	2	25	47	33	64
39	4	23	14	59	63	44	50
17	27	18	52	37	32	45	40

Figure 2. S-Box (8 × 8) structure.

Algorithm 3 Substitution

1: Input:Permuted image integer $O = \{o_1, o_2, \ldots, o_M\}$, Secret-key$l_2$, and Chaotic map (1),
2: Output: Pre-encrypted image T'.
3: Using the chaotic map (1) as a place to begin, they build an s-box by means of subsequent phases.
4: Create 256 regions with a fixed length Δg within the interval [0.1, 0.9]. That is,

$$\Delta g = (0.9 - 0.1)/256 = 0.003125$$

Enumerate every sub-interval area as$Q_1, Q_2, \ldots, Q_{255}$
5: Utilizing the variablesw_0' and$z'$of the secret-key$l_2 = (w_0', z')$ for chaotic map (1) to create a sequence w_m of simply the principles found in [0.1, 0.9].
6: Create a blank array T at first.
7: Whenever a value$w_m$explores a certain sub-interval area Q_j ($j = 0, \ldots, 255$),save the indices for that sub-interval area j in T. Throw away values that don't belong in any sub-interval area or provide the index value for a recurring sub-interval region.
8: All of the various digits among 0 and 240 can be found in the array T.
9: Foreveryblock pi in the permuted image$O = \{o_1, o_2, \ldots, o_M\}$ replace$o_j$by(o_j)wherej $\in \{1, \ldots, 256\}$. The array that results is then represented by $T' = \{s_1, s_2, \ldots, s_M\}$.

3.4. Pseudo-Random bit matrix generation

One-dimensional chaotic maps are used in the proposed layout to map to the interval [0, 1]and employed to allocate the encrypted data and remove certain unnecessary patterns. The final $\mathcal{F}$ decimal digits of the number w_j in each iteration are extracted, and each digit$c_1, \ldots, c_{\mathcal{F}}$ is compared to the threshold value of 5 to construct a pseudo-random bit matrix generation from each map. The mean of the integers 0

through 9 is selected to be this value. There is a chance that a 0 or a 1 could pop up. To generate the F bits at regular intervals until the necessary bitstream length ℓ, only $\frac{\ell}{\mathcal{F}} + 1$ is attainediteration; the bits are merged from a row column and added to an identical bit stream shown in **Figure 3**.

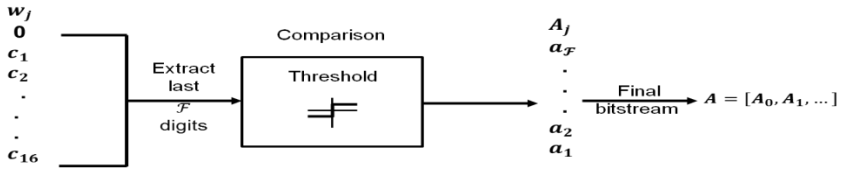


Figure 3. Random bit matrix generation.

To ensure equality for digits higher than 5, the threshold comparison approach provides a bit value of 1 if $c_j \geq 5$ and 0 if$c_j < 5$. With a double-precision 8-digit accuracy and a map accepting values between [−1, 1], this method may create up to 8 bits in each iteration. A collection of 50 × 106 bi-streams is created and examined using the statistical test suite to confirm the generated bitstream's randomness. Fifteen tests in the toolbox can confirm if a sequence is random. Every test yields a *P*-value; if it exceeds a predetermined significance threshold, the test is considered successful. A *P*-value of *P*-value > 0.01 signifies a 99% confidence level that the sequence is random. The bitstream is regenerated using the least significant $\hat{\mathcal{F}} = \mathcal{F} - 1$ digits if any of the 15 checks are not passed, and the initial decimal digit of w_j is removed. This procedure is carried out repeatedly until a stream of data passes every test.

3.5. Image blocking

The proposed encryption technique divides every image into blocks of the same size. A significant block encryption technique encrypts only a particular pixel of each block. Because the values of these chosen pixels are the lowest among the remaining blocks, the resultant image is smaller and of lesser quality. Without transmitting more pixels, the recipient will acquire the general structures of the image. The original color image is obtained, the 3D color image matrix is reshaped to a 2D gray image, the 2D image matrix is divided into equal blocks, a secret key with equal block size is selected, the key is saved for decryption, the encrypted block is obtained through an XOR operation, and the encrypted color image is obtained by reshaping the encrypted 2D matrix back to a 3D matrix. In **Figure 4**, an example 2D 8 × 8 block image is displayed.

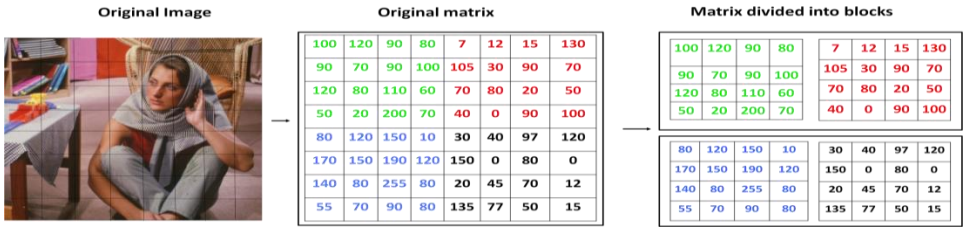


Figure 4. Blocks within a 2D image division.

3.6. Pixel-Driven selective encryption

This work proposes an efficient compact pixel crypto (CPC) technique for encrypting blocks $\varepsilon_{l,q,b,}$ the most important pixels. The selected pixels are divided through sub-matrices, whose are subsequently subjected to one session of symmetrical data encryption and decryption. The selected pixels are separated into α submatrices, each having h^2 values. The value of h can be 4, 8, 16, or 32 bits, with 32 considered in the proposed method. An equation is used to determine the value of α if there are three colored channels.

$$\alpha = \frac{blocks \times channels}{h \times h} \tag{1}$$

The CPC cryptographic method Ascon starts with a 320-bit state, a secret key$L$, and a nonce Mshown in **Figure 5**. Implementing a round transform p and an XOR of the secret key L completes the initialization procedure. To create a multiple of r bits, Ascon splits the related data B into s blocks of q bits after attaching a single 1 and the least amount of 0s. Padding is not used if B is empty. The b-round permutation O_a is applied to the state T after each block B_j with j = 1, ..., t is XORed to the first q bits of the state.

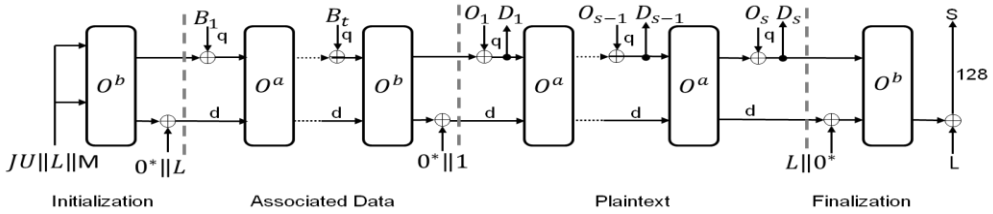


Figure 5. Pixel driven encryption method.

A 1-bit domain splitting parameter is sent S following the processing of As. Additionally, Ascon analyzes plaintext o in blocks of q bits, adding the fewest possible 0s and a single 1 to it. One padded plaintext block O_j is XORed to the primary q bits of the internal state T in each cycle, and then one ciphertext block D_j is extracted illustrated in Algorithm 4.

Algorithm 4 pixel driven encryption

1: Authenticated Encryption $\varepsilon_{l,q,b,a}(L, M, B, O)$
2: Input: key $L \in \{0,1\}^l, l \leq 120$
3: Nonce $M \in \{0,1\}^{64}$
4: Plaintext $O \in \{0,1\}^*$
5: Coupled data B$\in$ $\{0,1\}^*$
6: Output: ciphertext $D \in \{0,1\}^{|o|}$
7: Tag $S \in \{0,1\}^{64}$
8: Initialization

$$T \leftarrow JU_{l,q,b,a}\|L\|M$$
$$T \leftarrow o^b(T) \oplus (0^{128-l}\|L)$$

9: Processing Associated Data
10: If $|B| > 0$ then

$$B_1 \ldots B_t \leftarrow q - bitblocksofB\|1\|0^*$$

Algorithm 4 (*Continued*)

11: For $j = 1, \ldots, sdo$

$$T \leftarrow o^{a}((T_q \oplus B_j \| T_d)$$
$$T \leftarrow T \oplus ((0^{319-l} \| 1)$$

12: Processing Plaintext

$$O_1 \ldots O_s \leftarrow q - bitblocksofO \| 1 \| 0^{*}$$

13: For $j = 1, \ldots, s-1\ do$

$$T_q \leftarrow T_q \oplus O_j$$
$$D_j \leftarrow T_q$$
$$T \leftarrow o^{a}(T)$$
$$T_q \leftarrow T_q \oplus O_s$$
$$\widetilde{D}_s \leftarrow \lfloor T_q \rfloor_{|o| mod q}$$

14: Finalization

$$T \leftarrow O^{b}(T \oplus (0^{q} \| L \| (0^{128-q-l}))$$
$$T \leftarrow \lceil T \rceil^{64} \oplus \lceil L \rceil^{64}$$

15: Return $D_1 \| \ldots \| D_{s-1} \| \widetilde{D}_s, S$

3.7. Block scanning compression

The technique classifies significant pixels as the lowest value of each block's pixels, classifying insignificant pixels as insignificant. It uses scan-based encryption to encode insignificant pixels, while other image blocks are encrypted using a complementary scan-based method. The compression process targets selected pixels, while other images are encrypted using a complementary block scanning compression method. The steps include data transfer, integration with the pseudo-random bit matrix, compression, and internal block permutation. Each segment is represented by a certain number of a single pixel and the distinction among adjacent pixels is determined and communicated. Fewer bits can be used to describe the slight variance between these values, which reduces the data volume compared to the original pixel values. An example image that demonstrates this principle is shown in **Figure 6**.

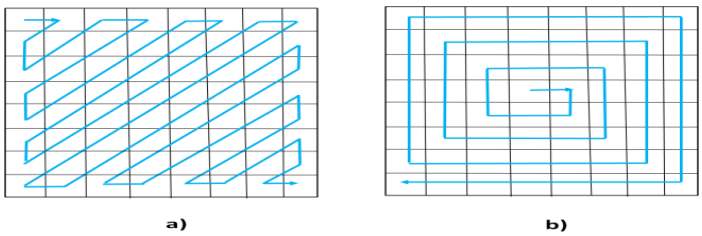


Figure 6. Image scanning method. **(a)** 8 × 8 matrix zigzag scanning; **(b)** 8 × 8 matrix spiral scanning.

Popular techniques for transforming two-dimensional matrix-like Standard Test Images into one-dimensional vectors include zigzag and spiral scanning. These techniques upend strong pixel correlations in the Standard Test Image and increase algorithm security. Two-dimensional image scanning techniques produce ($n \times n$) Scan routes, which together make up the cryptographic key. These techniques are applied to encryption, compression, and data concealment. One common method for turning a matrix-like image into a one-dimensional vector is zigzag or spiral scanning. By

destroying the connections between neighboring pixels in the input image, these technologies provide a better cryptographic algorithm. Spiral pathways begin at (4, 4), beginning from the original matrix, whereas zigzag paths begin at pixel position (1, 1). Applying spiral and zigzag scans with various initial locations can strengthen the security of the algorithm.

3.8. Coupling with pseudo random matrix

The scan-based encryption technique has to be made more sophisticated to prevent exhaustive search attacks by making it harder for attackers to anticipate potential outcomes. To achieve this, a pseudo-random bit matrix is XORed column per column and row per row with the produced data, which is the variance among the specified pixels and the remaining pixels, represented as a string.

3.9. Data transmission

Encrypted data is sent to a recipient, which decrypts it and gets the original image the bit spectrum of blocks, the dimension of the block utilized for encrypting it the initial image in both height and width, the value of α, and the number of packet required for a cryptography image should all be included in the data that is encrypted stream. An attacker would have a hard time figuring out the conclusion of each image sequence since the bits that are transferred to the recipient are concealed. The correlation between pixels, the data length interchange between nodes may vary. The receiving side decrypts the image, obtains the image characteristics, makes vacant image blocks, and uploads the values of the pixel discrepancy into the appropriate block. Selected pixels are retrieved from each block via the significant block encryption process, and they are then added to recreate the original image as shown in **Figure 7**.

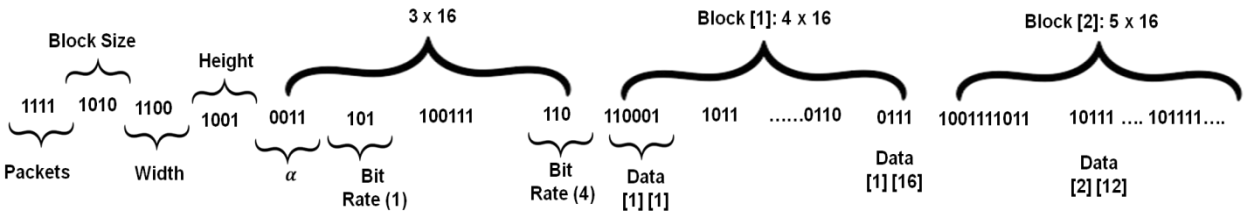


Figure 7. Image pixel coupling with pseudo random bit matrix.

4. Result and discussion

This section evaluates the suggested method's effectiveness using simulation exercises carried out in the NS2 simulator. The research set the interface type to Phy/Wireless Phy, the propagation model to Propagation/Two Ray Ground, and the channel type to Channel/Wireless Channel to accomplish image-specific pixel encryption. Antenna/Omni Antenna was the model name for the antenna, and Medium Access Control (MAC)/802-11 was the configuration for the MAC type. The study used the distance vector routing (DVR) protocol for routing, with Queue/Drop Tail/PriQueue as the queue type. The surroundings and component parameters are illustrated in **Table 3**.

The lightweight Ascon technique (Pixel driven encryption) and the key encrypting degree of safety are used to assess the efficacy of the proposed method. A variety of variables is taken into account, including node residual energy, packet transmission volume, and time complexity. Additionally examined are key uniformity and sensitivity. A series of simulation tests were carried out on blocks with varying sizes (4-64) to compare the results with earlier studies. To compare with the greater block size, block size 1 is utilized.

Table 3. Simulation parameters.

Parameter	Value
Maximum Queue Length	70
Initial Energy	5 j
Network Size	$150 \times 150\ m^2$
Sleeping Power	0.029 w
Transmission Power	0.35 w
Average Mobile Nodes	120
Receiving Power	0.1 w

4.1. Time complexity

The complexity and resource consumption of an encryption approach could be determined by measuring the amount of time required to encrypt or decode an image. Although blocks of sizes 8 and 16 operate faster than those of sizes 4 and 8, block size does occasionally translate into shorter execution times,Time complexity for the Elaine image based on different block sizes is depicted in the **Figure 8.**

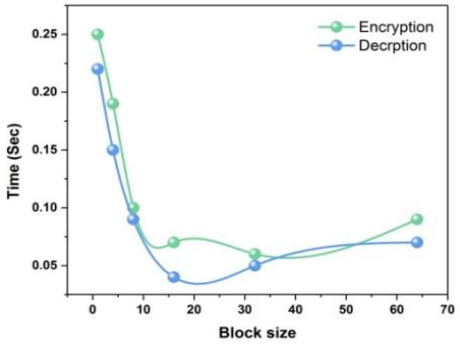
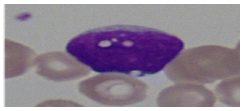


Figure 8. Execution times.

Table 4 shows the amount of packets that are required for various images that have different block dimensions.

Table 4. Number of packets in the various blocks of the image.

Number of Packets	Block Size of the Image					
	1	**4**	**8**	**16**	**32**	**64**
Barbara 	820	540	480	490	520	670
Lena 	790	680	530	590	640	720
Pepper 	780	590	440	320	470	610
Elaina 	810	720	590	540	620	670
Cell 	760	870	750	630	690	740
Indian 	740	670	450	560	480	620

4.2. Energy consumption of transmission node

To prevent considerable energy loss during the secure transmission, receiving, and encrypting of images, IoT nodes should employ Ascon's lightweight encryption approach that saves energy. For IoT nodes in simulation circumstances, a starting energy of 5 joules is assumed. Because of the great compression of unnecessary pixels accomplished through 3.7 Block scanning compression, block size 16 performs better than the rival solution with block size 8. Block size increases data delivered, but it also increases the number of bits required for pixel differences, resulting in larger data and transmission packet sizes and higher energy consumption as shown in **Figure 9**. As such, the block size ought to be regarded as appropriate.

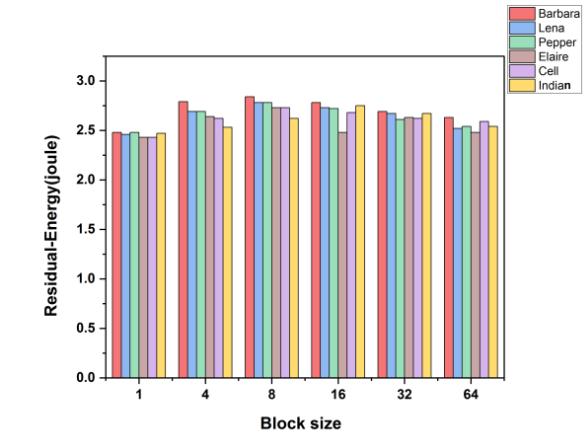


Figure 9. Energy consumption for the image transmission node.

4.3. Propagation of error

The CPC approach is to minimize modification and decrease error propagation to enhance image retrieval in noisy channels. The technique takes care of mistakes such as sub-matrices, value differences between pixels, and image characteristics. Errors in the image pixel-driven specification section can be addressed by retransmission bit insertion. **Figure 10** shows the decrypted cell images at various error rates.

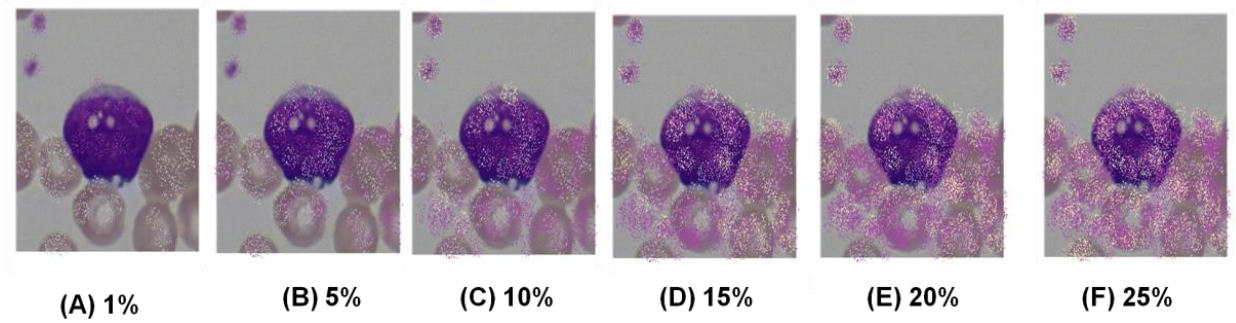


Figure 10. Error propagation.

A 8 × 8 bit-block size is used in the encryption process. **Figure 11** displays the network error propagation percentage for several blocks.

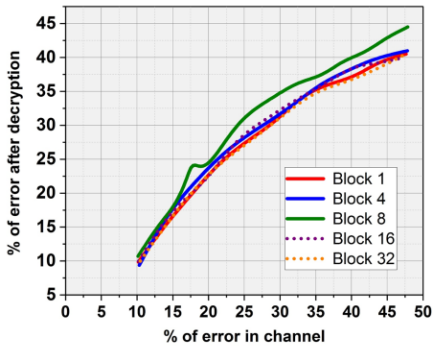


Figure 11. The network's error propagation rate.

4.4. Performance analysis

The mean square error (MSE) represents the difference in the encrypted and unencrypted images. A higher performance requires this gap to be quite large. An estimator's quality is gauged by the MSE, which is always non-negative and has superior values around zero. One measure of image quality is the peak signal-to-noise ratio (PSNR). For an adequate encrypted image, the value must be low. To compute PSNR, MSE is utilized. **Figure 12** displays the PSNR value for the image of Barbara that has blocks of various sizes.

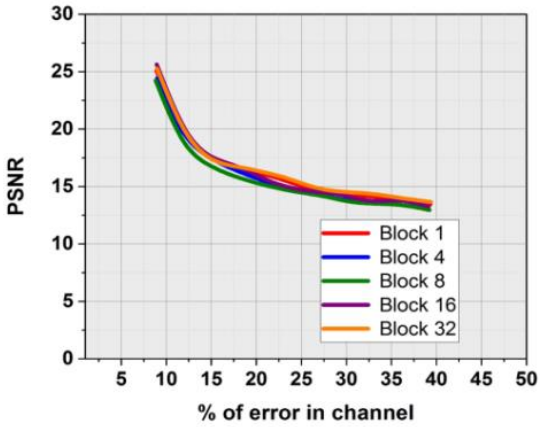


Figure 12. PSNR value in Barbara image blocks.

4.5. Error reduction analysis

The CPC method for image recovery involves using a Gaussian filter to partially fix errors in encrypted images. To remove the errors, this filter separates the image into regions and aggregates the pixels throughout the respective ranges. It won't, nevertheless, lessen the problem if the variation is equal to the size of a block as the additional pixel in that blocks would still produce the identical mistake. For the reason of image recuperation, regions greater than just one segment must be taken into account. The Gaussian filter had minimal effect on error reduction when a Lena image with a block size of 8 was placed in a noisy channel with a 7% level is illustrated in **Figure 13**. Nevertheless, the inaccuracy becomes substantially masked when the filter frequency is increased.

Figure 13. Gaussian filter analysis.

4.6. Uniformity analysis

In pharmaceutical analysis, uniformity of image assures consistent quality in every block size. To confirm the even distribution of security measures, many samples or pixels (0–250) are selected and encrypted using an appropriate technique in image encryption. Every pharmaceutical product has the right amount of active ingredient; this method guarantees that every block of the picture retains the appropriate degree of secrecy and integrity. **Figure 14** depicts the uniformity of the Barbara image in 8 × 8 and 16 × 16 blocks.

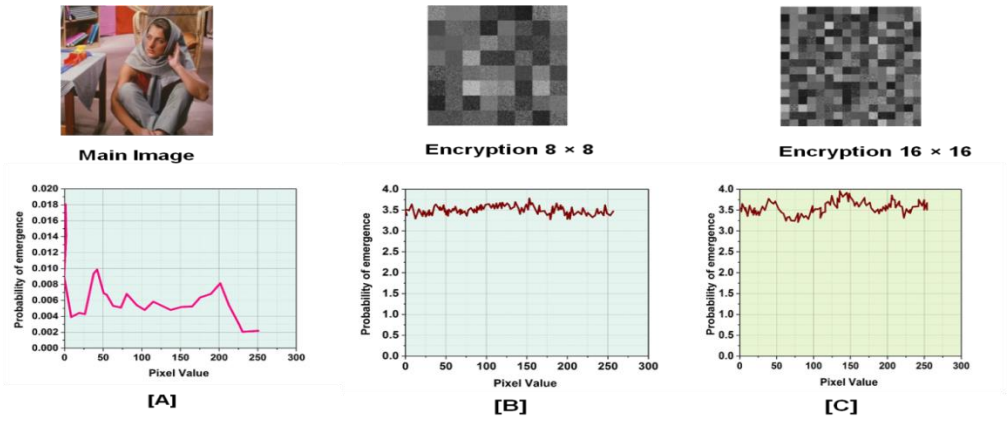


Figure 14. Uniformity of the Barbara image. **(A)** main image; **(B)** Encryption 8 × 8; **(C)** Encryption 16 × 16.

4.7. Key-Sensitive analysis

An encrypted image's vulnerability to an encryption key is measured through key sensitivity analysis. The security of the technique can be jeopardized by small modifications since adversaries can predict identical portions of the picture by listening in and extracting portions of the key requirement. It is more difficult to retrieve the original image with higher key sensitivity. To confirm sensitivity, an encrypted imagine is decrypted using a common key and an encryption key which varies by just one byte. The difference between two images is computed using the Hamming distance. **Figure 15** illustrates the key analysis of sensitivity and Hamming distance for blocks 8 through 16 in the pepper image

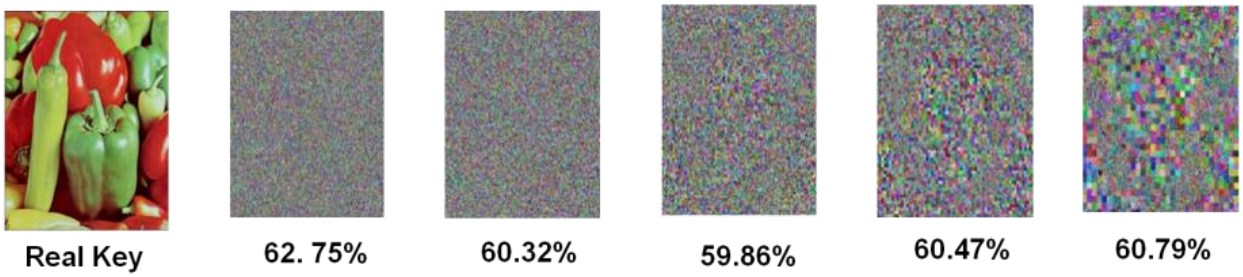


Figure 15. Key sensitivity and humming distance analysis.

5. Conclusion

Effective pixel-driven selective encryption and block scanning compression are necessary for the safe transfer of large amounts of audiovisual material since IoT nodes

have limited resources. This study proposes a CPC encryption technique that uses selective pixel encryption and scan-based block compression for multimedia IoT applications. Because the proposed approach involves continuous blocking, research showed that blocks with sizes of 8 and 16 performed better in regards to the quantity of packets delivered and method time for execution. In comparison to the competing methods, the trials also showed that using the suggested strategy led to a 20% reduction in IoT nodes' energy consumption and a 29% pepper in the number of packets transmitted. It was discovered that the suggested method produced the same results as the compared methods by looking at the error propagation on the image. The suggested method's Hamming distance was found, about 70% when the main sensitivity evaluation was applied, and suggesting that it offers a desired level of security. By providing a lightweight encryption method tailored for IoT devices, the study contributes to the overall security framework, making them less susceptible to unauthorized access and data breaches. The focus on minimizing bandwidth and computational requirements aligns with the constraints of IoT devices, promoting broader adoption of security measures. Research on the application of deep learning algorithms to enhance the CPC method can be performed as future research.

Ethical approval: Not applicable.

Conflict of interest: The author declares no conflict of interest.

References

1. Hedayati, R. and Mostafavi, S., 2022. A lightweight image encryption algorithm for secure communications in multimedia Internet of Things. Wireless Personal Communications, 123(2), pp.1121-1143.https://doi.org/10.1007/s11277-021-09173-w
2. Raza, S., Helgason, T., Papadimitratos, P. and Voigt, T., 2017. SecureSense: End-to-end secure communication architecture for the cloud-connected Internet of Things. Future Generation Computer Systems, 77, pp.40-51. https://doi.org/10.1016/j.future.2017.06.008
3. Medileh, S., Laouid, A., Euler, R., Bounceur, A., Hammoudeh, M., AlShaikh, M., Eleyan, A. and Khashan, O.A., 2020. A flexible encryption technique for the Internet of Things environment. Ad Hoc Networks, 106, p.102240. https://doi.org/10.1016/j.adhoc.2020.102240
4. Mohammad, G.B., Shitharth, S., Syed, S.A., Dugyala, R., Rao, K.S., Alenezi, F., Althubiti, S.A. and Polat, K., 2022. Mechanism of Internet of Things (IoT) integrated with radio frequency identification (RFID) technology for healthcare system. Mathematical Problems in Engineering, 2022, pp.1-8. https://doi.org/10.1155/2022/4167700
5. El-Shafai, W., Mesrega, A.K., Ahmed, H.E.H., El-Bahnasawy, N.A. and Abd El-Samie, F.E., 2022. An efficient multimedia compression-encryption scheme using Latin squares for securing Internet-of-things networks. Journal of Information Security and Applications, 64, p.103039. https://doi.org/10.1016/j.jisa.2021.103039
6. Parekh, A., Antani, M., Suvarna, K., Mangrulkar, R. and Narvekar, M., 2024. Multilayer symmetric and asymmetric technique for audiovisual cryptography. Multimedia Tools and Applications, 83(11), pp.31465-31503.https://doi.org/10.1007/s11042-023-16401-x
7. Devi, K.J., Singh, P., Thakkar, H.K. and Kumar, N., 2022. Robust and secured watermarking using Ja-Fi optimization for digital image transmission in social media. Applied Soft Computing, 131, p.109781.https://doi.org/10.1016/j.asoc.2022.109781
8. Gowda, V.D., Kumar, P.S., Latha, J., Selvakumar, C., Shekhar, R. and Chaturvedi, A., 2023. Securing networked image transmission using public-key cryptography and identity authentication.https://doi.org/10.47974/JDMSC-1754
9. Lata, K., Chhabra, S. and Saini, S., 2021. Hardware–Software Co-Design Framework for Data Encryption in Image Processing Systems for the Internet of Things Environment. IEEE Consumer Electronics Magazine, 11(4), pp.92-97. https://doi.org/10.1109/MCE.2021.3115999

10. Al Hayani, B. and Ilhan, H., 2020. Image transmission over decode and forward-based cooperative wireless multimedia sensor networks for Rayleigh fading channels in medical internet of things (MIoT) for remote health-care and health communication monitoring. Journal of Medical Imaging and Health Informatics, 10(1), pp.160-168.https://doi.org/10.1166/jmihi.2020.2691
11. Prasanalakshmi, B., Murugan, K., Srinivasan, K., Shridevi, S., Shamsudheen, S. and Hu, Y.C., 2022. Improved authentication and computation of medical data transmission in the secure IoT using hyperelliptic curve cryptography. The Journal of Supercomputing, 78(1), pp.361-378.https://doi.org/10.1007/s11227-021-03861-x
12. Wen, H., Zhang, C., Chen, P., Chen, R., Xu, J., Liao, Y., Liang, Z., Shen, D., Zhou, L. and Ke, J., 2021. A quantum chaotic image cryptosystem and its application in IoT secure communication. IEEE Access, 9, pp.20481-20492. https://doi.org/10.1109/ACCESS.2021.3054952
13. Stergiou, C., Psannis, K.E., Kim, B.G. and Gupta, B., 2018. Secure integration of IoT and cloud computing. Future Generation Computer Systems, 78, pp.964-975.http://dx.doi.org/10.1016/j.future.2016.11.031
14. Refaee, E., Parveen, S., Begum, K.M.J., Parveen, F., Raja, M.C., Gupta, S.K. and Krishnan, S., 2022. Secure and scalable healthcare data transmission in IoT based on optimized routing protocols for mobile computing applications. Wireless Communications and Mobile Computing, 2022, pp.1-12. https://doi.org/10.1155/2022/5665408
15. Lu, Y. and Asghar, M.R., 2020. Semantic communications between distributed cyber-physical systems towards collaborative automation for smart manufacturing. Journal of Manufacturing Systems, 55, pp.348-359. https://doi.org/10.1016/j.jmsy.2020.05.001
16. Kaur, M., Singh, D., Kumar, V., Gupta, B.B. and Abd El-Latif, A.A., 2021. Secure and energy efficient-based E-health care framework for green internet of things. IEEE Transactions on Green Communications and Networking, 5(3), pp.1223-1231.https://doi.org/10.1109/TGCN.2021.3081616
17. Li, Z., Zhou, W., Zhou, Z., Zhang, S., Shi, J., Shen, C., Zhang, J., Chi, N. and Dai, Q., 2024. Self-supervised dynamic learning for long-term high-fidelity image transmission through unstabilized diffusive media. Nature Communications, 15(1), p.1498. https://doi.org/10.1038/s41467-024-45745-7
18. Wang, Z., Qin, J., Xiang, X., Tan, Y. and Peng, J., 2023. A privacy-preserving cross-media retrieval on encrypted data in cloud computing. Journal of Information Security and Applications, 73, p.103440.https://doi.org/10.1016/j.jisa.2023.103440
19. Jang, W. and Lee, S.Y., 2020. Partial image encryption using format-preserving encryption in image processing systems for the Internet of Things environment. International Journal of Distributed Sensor Networks, 16(3), p.1550147720914779. https://doi.org/10.1177/1550147720914779
20. Jayaraman, P.P., Yang, X., Yavari, A., Georgakopoulos, D. and Yi, X., 2019. Privacy-preserving Internet of Things: From privacy techniques to a blueprint architecture and efficient implementation. Future Generation Computer Systems, 76, pp.540-549.https://doi.org/10.1016/j.future.2017.03.001
21. Ma, Y., Chai, X., Gan, Z. and Zhang, Y., 2023. Privacy-preserving TPE-based JPEG image retrieval in cloud-assisted Internet of things. IEEE Internet of Things Journal.https://doi.org/10.1109/JIOT.2023.3301042
22. Elhoseny, M., Shankar, K., Lakshmanaprabu, S.K., Maseleno, A. and Arunkumar, N., 2020. Hybrid optimization with cryptography encryption for medical image security in the Internet of Things. Neural computing and applications, 32, pp.10979-10993.
23. Jadaun, A., Alaria, S.K. and Saini, Y., 2021. Comparative study and design of lightweight data security system for secure data transmission in the Internet of things. International Journal on Recent and Innovation Trends in Computing and Communication, 9(3), pp.28-32. https://doi.org/10.17762/ijritcc.v9i3.5476
24. Salim, K.G., Al-alak, S.M.K. and Jawad, M.J., 2021. Improved image security in Internet of Things (IoT) using multiple key AES. Baghdad Science Journal, 18(2), pp.0417-0417.