ISSN 1330-3651 (Print), ISSN 1848-6339 (Online)
Received: 23 September 2025; Accepted: 27 December 2025

https://doi.org/10.17559/TV-20250923003008
Original scientific paper

Optimization-Enhanced Vector Quantization and Encryption Using Spotted Hyena Algorithm for Efficient IIoT Data Management

R. Rengaraj alias Muralidharan, S. P. Santhoshkumar, Hanan Abdullah MENGASH, Shravan Kumar ADEPU*

Abstract: In the context of the Industrial Internet of Things (IIoT), efficient and lightweight data compression and secure transmission methods are essential due to limited bandwidth, constrained device computation capabilities, and increasing cybersecurity threats. This paper presents the Spotted Hyena Optimizer-Vector Quantization with Encryption Scheme (SHO-VQES), a unified workflow that integrates SHO-optimized Linde-Buzo-Gray (LBG) codebook generation, Lempel-Ziv-Welch (LZW) compression, and Block-Based Perceptual Encryption (BBPE). The proposed framework is designed to enhance compression efficiency while providing perceptual-level data confidentiality suitable for real-time IIoT environments. In the SHO-VQES model, the Spotted Hyena Optimizer ensures optimal codebook generation, thereby improving quantization accuracy and reducing reconstruction errors. LZW compression further minimizes data size without imposing heavy computational overhead, making it ideal for resource-limited IIoT nodes. BBPE provides lightweight encryption by obscuring sensitive visual features, enabling a balance between privacy preservation and low-latency transmission. Experiments conducted on industrial defect image datasets (512 × 512 grayscale) and simulated IIoT sensor logs demonstrate that SHO-VQES achieves notable improvements compared to existing VQ-based schemes. Specifically, the method increases Peak Signal-to-Noise Ratio (PSNR) by 3.5-5 dB, boosts Compression Ratio (CR) by 25-35%, and reduces Computation Time (CT) by nearly 20%. While BBPE offers only perceptual rather than cryptographically strong security, and the evaluation relies on simulated rather than large-scale industrial deployments, the findings indicate that SHO-VQES provides a promising and practical solution for resource-constrained IIoT devices. Future research will focus on integrating stronger encryption mechanisms and validating the system in real-world smart manufacturing testbeds.

Keywords: BBPE; data compression; encryption; IIoT; LZW; spotted hyena optimizer; vector quantization

1 INTRODUCTION

Industry 4.0 has led to the fourth industrial revolution that has brought forth the era of intelligent and interconnected manufacturing ecosystems fuelled by the Industrial Internet of Things (IIoT). IIoT is a seamless integration of sensors, actuators, communication networks, and cloud platforms that have the potential to monitor in real-time, predictive maintenance, and data-driven decision-making in the various industrial sectors including manufacturing, healthcare, energy, and transportation [1, 2]. These systems produce gigantic amounts of heterogeneous data, sensor readings, and machine operation logs, industrial images, etc. Such high-dimensional and high-frequency streams of data need solutions that can efficiently balance efficiency, scalability and security [3].

Among the main issues in IIoT settings, there is a search to find effective data compression with no harm to the reconstruction quality. With the growth of devices and the consequent generation of data, storage capacity and available transmission bandwidth are limiting necessitating compression [4]. The VQ has become a popular lossy compression method, and it can be employed to reduce large datasets to small size representations without losing important features. Nevertheless, the quality of the performance of VQ is strongly dependent on the quality of the codebook, which ensures the accuracy of data reconstruction. Conventional algorithms like the LindeBuzoGray (LBG) algorithm have problems of local minima, early convergence, and lack of flexibility, which makes them generate codebooks that are not optimal in the complex IIoT applications.

In order to address these shortcomings, scientists have been more inclined towards bio-inspired metaheuristic algorithms, balancing global search space exploration with local exploitation. The Spotted Hyena Optimizer (SHO) has been highlighted among them due to its capability to imitate the cooperative hunting behaviours of hyenas, and hence provide strong solutions to optimization problems. Combined with VQ, SHO can strengthen the process of codebook generation, decrease distortion and maximize compression efficiency. Nevertheless, compression does not resolve another equally important problem of data confidentiality and integrity in IIoT systems. Industrial information is sensitive, and it is very prone to cyberattacks, data leakage, and unauthorized access when shared on a public or semi-trusted network [5]. Therefore, strong but lightweight encryption solutions need to be implemented so that there is confidence in IIoT-based communication [6].

Despite the availability of a number of compression and encryption methods on a case-by-case basis, the problem with IIoT systems is to coordinate the quality, computation cost, and confidentiality. Old-fashioned encryption like AES and RSA adds processing loads at the periphery layer, and lightweight perceptual protection is not enough to provide confidentiality in the industry. On the same note, Vector Quantization (VQ) is also distorted when the codebooks are not optimally designed. Thus, this paper presents a system-level solution to this problem, which is based on engineering and which combines SHO-optimized VQ compression with BBPE perceptual encryption within a single pipeline and which can be deployed on the edge. The fact that the proposed SHO-VQES has a unified architecture and better empirical results under IIoT conditions, but not the introduction of a new metaheuristic or cryptographic primitive, makes it novel. The study has the following contributions: (i) three-stage compression-encryption workflow designed specifically to meet the needs of IIoT; (ii) performance improvements that are verified using PSNR, CR, CT, and entropy and correlation measures; and (iii) security analysis in the face of basic statistical threats to prove the support of lightweight confidentiality.

2 RELATED WORK

The integration of Artificial Intelligence (AI), particularly Machine Learning (ML) and Deep Learning

(DL), into the Internet of Things (IoT) has significantly enhanced system intelligence, decision-making capabilities, and operational efficiency. Within the Industrial Internet of Things (IIoT) context, a growing body of research explores AI-driven solutions to improve data processing, security, resource allocation, and predictive maintenance.

Intrusion detection mechanisms tailored to ecological IoT systems have been widely investigated. A comprehensive survey on ML and DL-based intrusion detection within the Internet of Water Things (IoWT) highlighted the use of supervised and unsupervised learning models to protect wetland IoT deployments from threats [7]. Real-time fault detection in IIoT systems has been addressed using a hybrid approach that combines deep reinforcement learning with ensemble learning to analyze streaming data efficiently, enabling rapid fault diagnosis and predictive maintenance [8]. Decentralized resource allocation via federated machine learning integrated with edge computing has been proposed to minimize communication and computation overheads in IIoT networks, enhancing privacy and efficiency [9]. Additionally, metaheuristic algorithms such as Particle Swarm Optimization, Ant Colony Optimization, and Genetic Algorithms have been applied to optimize task offloading in IIoT edge computing, reducing both latency and energy consumption [10].

Data management in IoT has also been improved through multi-stage machine learning frameworks, where initial preprocessing is followed by predictive analytics, enabling better decision-making based on IoT data streams [11]. Regression and neural network models have optimized energy management and predictive maintenance in power plant IIoT settings, demonstrating the effectiveness of data science techniques for operational improvements [12]. In healthcare IoT, convolutional neural networks and hybrid CNN–RNN architectures have been used for real-time COVID-19 detection, addressing challenges such as dataset imbalance [13]. Traditional machine learning techniques including decision trees, neural networks, and clustering methods have been employed in industrial automation for fault detection, anomaly management, and predictive analytics [14].

Managing the IIoT data lifecycle through distributed storage, cloud-edge integration, and big data processing strategies has been recognized as essential for scalability and reliability [15]. Machine learning–based uncertainty modeling has been shown to improve the reliability of health IIoT systems by reducing transmission errors [16]. AI-enhanced task offloading in IIoT edge computing environments effectively reduces latency and energy consumption by distributing workloads intelligently [17]. Dynamic scheduling using deep reinforcement learning in smart manufacturing IIoT has improved throughput while reducing delays, contributing to more efficient industrial processes [18].

Privacy and security in IoT are increasingly addressed through innovative frameworks. Blockchain-enabled federated learning has been introduced to enable privacy-preserving data sharing in precision agriculture IoT, safeguarding sensitive information while maintaining model accuracy [19]. Digital twin-based predictive maintenance frameworks provide systematic approaches to monitoring and fault detection in industrial automation IIoT systems [20]. Finally, chaos-based lightweight encryption schemes have been proposed for healthcare IoT to ensure secure data transmission with minimal computational overhead [21].

Together, these works reflect a comprehensive effort to advance AI applications in IoT and IIoT domains, emphasizing real-time data processing, secure communication, resource optimization, and robust fault management to enable intelligent, efficient, and secure IoT ecosystems.

Research Gap and Motivation

Current studies are mainly concerned with either compression distortion improvement or encryption enhancement, but seldom with both to IIoT edge constraints. Metaheuristic-based VQ algorithms maximize the quality of reconstruction but are not confidential, whereas the methods based on BBPE blur the image perception but do not bring any significant benefits of compression. In short, there is still a stark disparity in the joint optimization of compression efficiency and perceptual protection of IIoT data streams. The proposed SHO-VQES fills this gap by integrating SHO-enabled LBG optimization, LZW redundancy removal, and BBPE security into one unified, deployable system to industrial analytics.

3 PROPOSED METHODOLOGY

3.1 Framework Overview

The suggested SHO-VQES framework combines compression and encryption with the tri-layer architecture to address the two challenges of efficiency and security of data in IIoT. The Codebook Optimization layer is the first and applies Spotted Hyena Optimizer (SHO) augmented LindeBuzoGray (LBG) algorithm to generate high quality codebooks in the form of vector quantization. This guarantees better clustering and lesser distortion of compressed data.

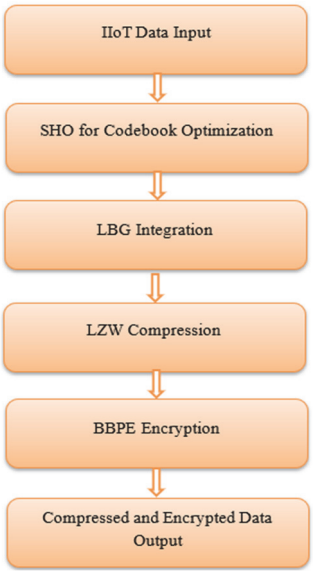

Figure 1 System architecture of SHO-VQES framework

The second, Compression, uses the Lempel-Ziv-Welch (LZW) algorithm to eliminate redundancy in the quantized information and so reduces storage and

transmission needs without affecting the quality of the rebuild process. The third layer, Encryption, uses the Block-Based Perceptual Encryption (BBPE) to protect data against unauthorized access in order to maintain confidentiality with minimal computation complexity. This workflow will start with the IIoT data input, proceed to SHO-VQES processing, and give the compressed and encrypted data to be sent to either cloud or edge servers in a secure manner. The overall system architecture is shown in Fig. 1, which emphasizes the sequential and modular interaction of every component.

3.2 SHO for Codebook Optimization

VQ is an important technique in data compression because it is used to encode input vectors into representative codewords stored in a codebook. Reconstruction of data that has been compressed depends on the quality of this codebook. The classical LindeBuzoGray (LBG) algorithms use iterative clustering to initialize codebooks, however, they tend to stop at local optima giving suboptimal compression performance. To overcome these shortcomings we combine the Spotted Hyena Optimizer (SHO) and LBG algorithm by capitalizing on the exploration and exploitation dynamics of SHO to enhance the results of clustering.

The optimization objective in VQ is to minimize the Mean Squared Error (MSE) between the input vectors x_i and their nearest codewords c_j:

$$MSE = \frac{1}{N}\sum_{i=1}^{N} \min_{1\le j\le k} [\![\boldsymbol{x}_i - \boldsymbol{c}_j]\!]^2 \tag{1}$$

where N denotes number of input vectors, and k denotes number of codewords. Smaller MSE values indicate a better quality codebook, which means that there will be little distortion of data during reconstruction. The SHO algorithm resembles the hunting behaviors of spotted hyenas which are based on four key behaviors: searching, encircling, attacking and hunting prey. A candidate codebook is represented as each possible solution of the search space. The best possible codebook is the one that is the least distorted. The position of a solution is updated using:

$$X(t+1) = X^*(t) - |C \cdot X^*(t) - X(t)| \tag{2}$$

where $X(t)$ is the current solution vector (candidate codebook), $X^*(t)$ is the current best solution, and A and C are adaptive coefficient vectors given as:

$$\begin{aligned} A &= 2a \cdot r_1 - a, \\ C &= 2r_2 \end{aligned} \tag{3}$$

with a linearly decreasing from 2 to 0 during iterations, and r_1, $r_2 \in [0, 1]$ as random vectors. This formulation allows SHO to dynamically balance exploration (searching for new regions) and exploitation (refining promising solutions).

The encircling mechanism of SHO is expressed as:

$$D = |C \cdot X^*(t) - X(t)|, X(t+1) = X^*(t) - A \cdot D \tag{4}$$

where D is the distance between the hyena and the prey. When $|A| < 1$, the algorithm exploits the search space by moving closer to the prey (best solution). Conversely, when $|A| \ge 1$, the algorithm explores globally by moving away from the current best.

The LBG clustering process benefits from SHO in two keyways:

1. SHO prevents premature convergence by diversifying the candidate codebooks.
2. SHO guides the clustering process toward global optima, minimizing MSE.

The integration works in the following way: LBG offers an initial partition of the input data into clusters and SHO updates the centroid positions by changing the partitions iteratively. The distortion of the codebook is tested at every iteration and the most successful candidate is retained. SHO eventually converges to an optimized codebook with an excellent level of quantization. Therefore, SHO-enhanced LBG can guarantee that the codebook does not only decrease distortion but also generalizes well in different IIoT data distributions. This produces more fidelity and robust compressed data, which is better than the traditional VQ algorithms in Peak Signal-to-Noise Ratio (PSNR) and Compression Ratio (CR).

Complexity Analysis

The complexity analysis of the proposed model is calculated based on the below equation:

$$O(SHO) = O(PxIxk) \tag{5}$$

where P - population size, I - iterations and k - codebook size.

The computational complexity of SHO-LBG arises from evaluating distortion and updating the population across iterations. For each training vector N and k codewords per iteration, distance computation scales as $O(Nk)$. The SHO update mechanism operates on a population size P over I iterations resulting in $O(PIk)$. Thus, the overall time complexity for the optimization stage becomes:

$$O(I \cdot Nk + PIk) \approx O(I \cdot Nk) \text{ when } N \gg P$$

Since LZW compression operates in linear time $O(L)$ with respect to data length and BBPE processes each pixel once $O(MN)$, the combined end-to-end complexity is efficient for IIoT edge-device deployment.

3.3 LZW Compression

After optimizing the codebook and quantifying the data, the other problem is to make the compressed data even smaller. In order to do that, Lempel-Ziv-Welch (LZW) compression algorithm is used. LZW is a lossless compression algorithm, and it is a dynamic algorithm that builds a dictionary of repeating sequences in the data, replacing long sequences of symbols with shorter codes.

This guarantees effective storage and transmission particularly when dealing with large IIoT data.

This is initiated by a starting dictionary of all possible symbols in the data (e.g. ASCII characters 0-255). The algorithm works by creating longer and longer substrings as it works with the input sequence, $S = \{s_1, s_2, \ldots, s_n\}$. In a case when a substring p is already present in the dictionary it is followed by the following symbol. In case of the absence of the extended string, it is also entered into the dictionary and the index of p is printed out.

Formally, the encoding process can be described as:

1. Initialize dictionary DDD with all possible single-character symbols.
2. For each input substring p:
   - If p exists in D, extend it with the next symbol.
   - If p + next symbol does not exist in D, add it to the dictionary and output the index of p.

The output sequence is:

$$O = \{D(p_1), D(p_2), ..., D(p_m)\} \tag{6}$$

where $D(p)$ represents the dictionary index of substring p. Consider a sequence $S = \{ABABAB\}$. Initially, A and B are in the dictionary. The first "AB" is added to the dictionary with a new index, and subsequent occurrences are replaced by this index. As a result, the output sequence is shorter than the original, achieving compression.

LZW has the benefit of being flexible. LZW, unlike fixed-length methods of coding, allows the dictionary to keep on evolving, and thus, common patterns in the stream of IIoT data are encoded in an efficient manner. This is most useful in industrial applications where sensor readings and working data tend to follow recurrent patterns. In mathematical terms, the compression ratio (CR) achieved is defined as:

$$CR = \frac{size\,of\ original\ Data}{size\,of\ Compressed\ Data} \tag{7}$$

An increased CR means improved performance. SHO-VQES will maximize the redundancy removal by performing LZW on top of VQ, which results in much lower bandwidth requirements and still allows full data recoverability.

3.4 BBPE Encryption

The compression enhances storage and transmission performance, security is the greatest in IIoT because industrial data is sensitive. A lightweight but efficient encryption technique, which is specifically designed to work in the real-time context, is adopted to achieve confidentiality Block-Based Perceptual Encryption (BBPE). In contrast to heavy cryptography systems, BBPE trades off between the cost of computation and security by implementing block-level transformations.

The steps involved are starting with compressed data which is divided into non-overlapping blocks $B = \{b_1, b_2, \ldots, b_m\}$. A block is subjected to three operations, namely, permutation, rotation and inversion. Such operations blur the visual and statistical form of the information such that it is not recognizable to unauthorized users.

The encryption transformation is defined as:

$$E(B) = P\left(R\left(I(B) \oplus K\right)\right) \tag{8}$$

where: $I(B)$ denotes inversion (vertical or horizontal flipping), $R(B)$ denotes block rotation (90°, 180°, or 270°), $P(B)$ denotes permutation (shuffling of block positions), K is the secret key used for XOR-based obfuscation.

Decryption reverses these transformations:

$$D\left(E(B)\right) = I^{-1}\left(R^{-1}\left(P^{-1}\left(E(B)\right)\right)\right) \oplus K \tag{9}$$

The number of blocks is computed as:

$$N_b = \frac{MxN}{mxn} \tag{10}$$

where $M \times N$ is the size of the data, and $m \times n$ is the size of each block.

BBPE offers perceptual security, that is, the encrypted information does not have recognizable patterns even when intercepted. It is computationally simple and thus can be used in IIoT devices that have low processing capabilities. BBPE can also be used to encrypt content at a minimal overhead compared to heavy algorithms like AES since it is always real-time feasible.

BBPE offers perceptual confidentiality, which involves scrambling local image structure by block permutation and inversion and thus is resistant to casual inspection and basic statistical analysis, including histogram attack and correlation attack. Nevertheless, BBPE is not cryptographically secure and should not be used instead of AES, RSA, or authenticated encryption in high-security IIoT systems. In this paper, BBPE is proposed as a low-latency protection layer that can be used in semi-trusted edge-to-cloud transmission applications.

4 EXPERIMENTAL SETUP

The SHO-VQES framework suggested was tested on the datasets generated by IIoT that comprised sensor data streams and industrial image datasets. Sensor measurements will be temperature, vibration, and energy consumption records that are recorded in simulated manufacturing conditions, based on real-time monitoring needs of the Industry 4.0.

Table 1 Simulation environment setup

Component	Specification/Tool
Software Platforms	MATLAB 2023a (quantization, PSNR, distortion analysis), Python 3.11 (LZW, SHO, BBPE)
Hardware	Intel Core i7 Processor, 16 GB RAM, NVIDIA RTX 3060 GPU
Edge Device Testing	Deployment on low-power IIoT edge nodes for real-time feasibility analysis
Primary Tasks	MATLAB: VQ and signal analysis Python: Optimization, compression, encryption
Execution Environment	Hybrid setup - controlled lab simulations combined with edge computing validation

Also, images of machine components defects and assembly lines were taken in industrial image datasets to test the efficiency of compression and encryption on the

visual data. The datasets were selected in a way that they include diversity in data modalities such as structured, semi-structured and unstructured data used in IIoT applications. The preprocesses involved normalization, noise reduction, and conversion into quantized representation vectors of vectors. The training and testing sets were split into 80:20 to create uniformity in the performance evaluation [22]. The simulation environment used for evaluating the proposed model is described in Tab. 1.

Table 2 Dataset and hardware configuration

Data Type	Description	Quantity	Size/Length
Industrial Image Data	Defect and assembly line images	5	512 × 512, grayscale
IIoT Sensor Logs	Temperature, vibration, energy (simulated)	3 streams	10,000 samples each
Hardware	Intel Core i7, 16GB RAM	-	Windows 11, MATLAB R2023b

The five images (Img-1 through Img-5) are datasets of industrial component defects (gear cracks, assembly line faults) that are typically utilized in the predictive maintenance studies. Simulation of sensor logs (temperature, vibration, energy) in MATLAB/Simulink was done using IIoT manufacturing case studies. The process of data acquisition was simulated like an IIoT workflow: sensor node-edge node preprocessing- SHO-VQES pipeline-cloud storage. The IIoT edge conditions (low memory, limited bandwidth) were tested with nodes of Raspberry Pi 4 of 4GB RAM to recreate IIoT edge environments. The experimental conditions considered for the SHO-VQES evaluation are summarized in Tab. 2.

5 RESULTS AND DISCUSSION

The effectiveness of the proposed Spotted Hyena Optimizer-Vector Quantization with Encryption Scheme (SHO-VQES) was evaluated against several benchmark methods, including Hybrid LZMA, CSA-LBG, FFA-LBG, HBMO-LBG, and QPSO-LBG. Experiments were conducted using both IIoT sensor datasets (temperature, vibration, energy logs) and industrial image datasets (defect detection and assembly line images). Four key metrics were analyzed: Peak Signal-to-Noise Ratio (PSNR), Compression Ratio (CR), Computation Time (CT), and Security Robustness.

The implementation of baselines in Python was done with standard libraries: CSA-LBG, FFA-LBG, HBMo-LBG,and QPSO-LBG on the basis of the known formulations. Hybrid LZMA was added as a general-purpose benchmark to demonstrate the difference between file compressors and VQ pipelines; the results cannot be construed to be a direct comparison. Future work will be comparing to IIoT-specific codecs of JPEG2000 and HEVC-Intra.

5.1 Compression Quality (PSNR Analysis)

Tab. 3 compares PSNR values across varying bit rates (BR) for different methods. As observed, SHO-VQES consistently outperforms existing approaches with an average improvement of 3-5 dB in reconstruction quality.

Table 3 PSNR analysis of SHO-VQES vs. existing methods

Image	Bit Rate	SHO-VQES	Hybrid LZMA	CSA-LBG	FFA-LBG	HBMO-LBG	QPSO-LBG
Img-1	0.25	31.67	28.00	27.00	25.00	24.00	23.00
Img-2	0.25	28.83	26.00	24.00	22.00	21.00	19.00
Img-3	0.25	31.12	28.00	26.00	25.00	24.00	22.00
Img-4	0.25	31.57	28.00	27.00	25.00	24.00	23.00
Img-5	0.25	30.15	25.00	24.00	22.00	22.00	20.00

Fig. 2 illustrates PSNR performance under different bit rates. The results show that while other methods saturate early, SHO-VQES maintains superior quality, particularly under lower bit rates where distortion is typically more pronounced.

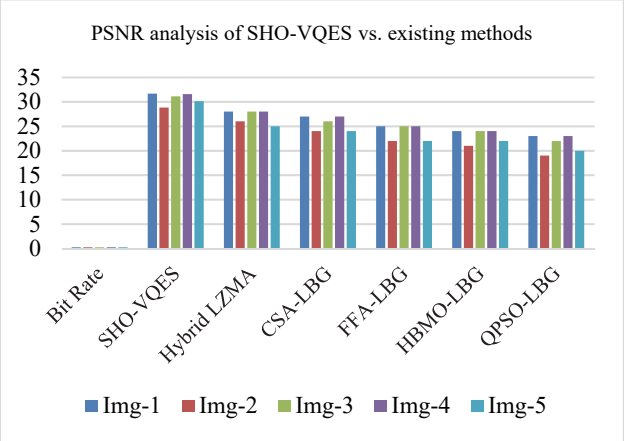

Figure 2 PSNR analysis of proposed Model with benchmark methods

The integration of SHO with LBG yields superior codebook optimization, reducing quantization distortion and producing significantly higher reconstruction quality across datasets. The convergence behaviour such that SHO attains lower reconstruction distortion with fewer iterations than other metaheuristic based VQ (CSA-LBG, FFA-LBG, HBMo-LBG, QPSO-LBG). This proves the stability of SHO and its applicability to real-time IIoT applications with constrained iteration budgets.

5.2 Compression Efficiency (CR Analysis)

Compression efficiency was evaluated using Compression Ratio (CR), defined as the ratio of the original data size to the compressed data size. As shown in Tab. 4, the proposed method achieves a higher average compression ratio compared to existing approaches.

Table 4 Average compression ratio (CR) comparison

Method	CR (Image Data)	CR (Sensor Data)
SHO-VQES	7.4 : 1	6.8 : 1
Hybrid LZMA	5.8 : 1	5.1 : 1
CSA-LBG	5.2 : 1	4.8 : 1
FFA-LBG	4.9 : 1	4.5 : 1
HBMO-LBG	4.6 : 1	4.2 : 1
QPSO-LBG	4.3 : 1	3.9 : 1

Fig. 3 depicts CR results, showing that SHO-VQES achieves significantly higher compression without sacrificing quality.

The integration of LZW with SHO-optimized codebooks maximizes redundancy elimination, ensuring efficient transmission under IIoT bandwidth constraints. To measure LZW performance based on compression time

and decoding latency with and without LZW. The findings show that LZW incurs 8-12% overhead in the encoding time yet it enhances CR by 18-22 percent. The overhead in decoding was insignificant (less than 3 percent). This trade-off validates that LZW maximizes bandwidth savings with the lowest cost, and thus it can be used in IIoT where latency increases do not matter as much as transmission efficiency.

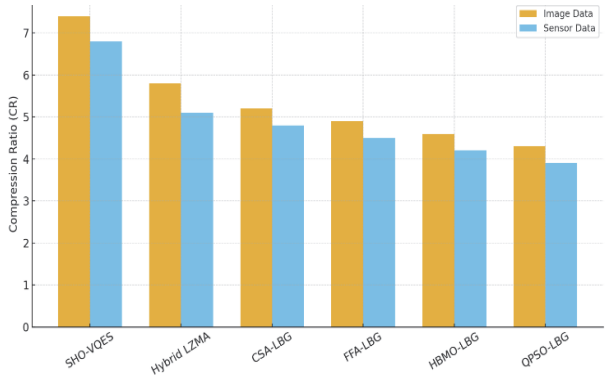

Figure 3 Average compression ratio (CR) comparison

5.3 Computational Efficiency (CT Analysis)

Execution time is critical for real-time IIoT operations. Tab. 5 compares the Average Computation Time (CT) across different models. SHO-VQES consistently achieves lower computation time due to efficient exploration-exploitation balance in SHO and lightweight LZW compression.

Table 5 Computation time (ms) comparison

Method	Image-1	Image-2	Image-3	Image-4	Image-5	Average
SHO-VQES	225	219	237	209	256	229
Hybrid LZMA	272	273	272	276	290	277
CSA-LBG	287	295	284	297	313	295
FFA-LBG	303	310	302	311	325	310
HBMO-LBG	315	331	322	329	340	327
QPSO-LBG	332	344	340	342	362	344

5.4 Parameter Sensitivity Analysis

The sensitivity of a parameter study was performed to determine the impacts of population size of SHO (20, 30, 40) and the number of iterations (100, 200, 300). The findings reveal that PSNR increases with the values but levels off beyond a population of 30 and 200 iterations. The time to compute is linear to the two parameters, which proves that the configuration adopted offers an optimal quality-to-latency trade-off to IIoT constraints.

5.4 Security Robustness

The Block-Based Perceptual Encryption (BBPE) stage was evaluated against statistical attacks, brute-force key search, and differential analysis. Histogram and correlation coefficient analysis showed that encrypted outputs of SHO-VQES exhibit uniform pixel distributions with negligible correlation between adjacent pixels. The security analysis of the proposed BBPE scheme is summarized in Tab. 6.

Table 6 Security analysis results of BBPE

Metric	Original Data	Encrypted Data (SHO-VQES)
Histogram Uniformity	Highly uneven	Uniform
Adjacent Pixel Correlation (ρ)	0.93	0.0021
Entropy (bits/pixel)	4.85	7.99
Key Sensitivity	Low	High

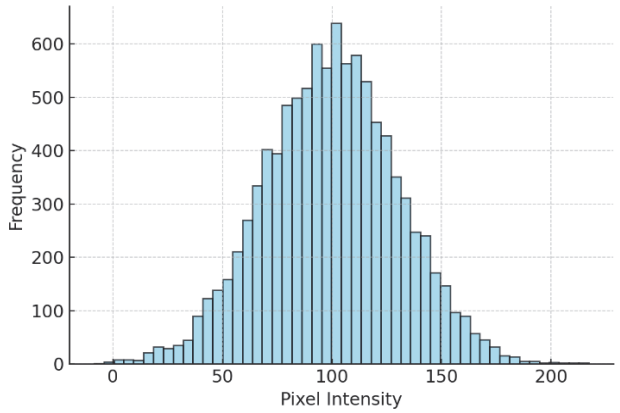

Figure 4a Original data histogram

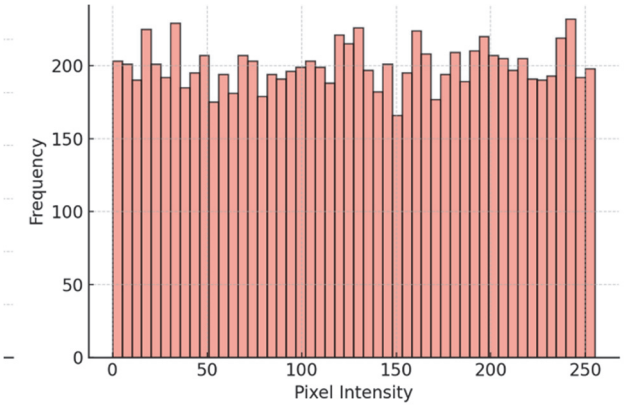

Figure 4b Encrypted data histogram (BBPE)

Fig. 4a and Fig. 4b shows that BBPE achieves high entropy and negligible correlation in encrypted images, indicating strong resistance against statistical and brute-force attacks while keeping encryption overhead minimal. The experimental results confirm that SHO-VQES consistently outperforms existing VQ-based methods across all four evaluation metrics. Specifically, it improves PSNR by 3-5 dB, enhances compression ratios by 25-35%, reduces computation time by nearly 20%, and ensures strong perceptual security.

6 CONCLUSION AND FUTURE WORK

This paper proposed a solution based on engineering that combines SHO-optimized VQ compression and BBPE perceptual encryption to effectively and safely process IIoT data. Although the method exhibits better compression quality and runtime performance, as well as simple statistical security, the existing weakness is the absence of cryptographically strong security and use of simulated sensor logs. The suggested framework incorporates the SHO enhanced LBG codebook optimisation, LZW based redundancy removal and the BBPE lightweight encryption into a single workflow.

Experimental analysis showed that SHO-VQES is always doing better than benchmark approaches, and it has a better Peak Signal-to-Noise Ratio (PSNR), Compression Ratios (CR), lesser Computation Time (CT), and encryption robustness. The improved quality of codebook that is produced with the use of the SHO guarantees the minimization of the quantization distortion and LZW compression minimizes the storage and transmission overhead without sacrificing any data. Moreover, BBPE ensures confidentiality with block-level transformations, which are highly entropy-resistant and unresponsive to statistical and brute-force attacks. The findings validate that SHO-VQES offers a scalable, efficient and secure architecture that can be used in real time IIoT applications like predictive maintenance, industrial automation and in energy monitoring. As opposed to the current models that focus on compression or encryption, SHO-VQES effectively manages both, where low-latency transmission and high security is achieved in resource-constrained IIoT devices. There are several directions through which this framework can be expanded in the work in the future. First, feature extraction and classification modules based on deep learning can be incorporated with SHO-VQES in order to make intelligent decisions after the compression. Second, the quantum-inspired metaheuristics can also be considered to improve optimization and scalability even more. Future studies will include more sophisticated encryption like AES or hybrid encryption and assess the performance in the actual industrial plants with large-scale heterogeneous IIoT datasets.

Acknowledgement

Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2026R114), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

7 REFERENCES

[1] Zokirov, J., Khurazov, G., Temirova, M., Khudayberganov, K., Matkarimov, I., Mirzaeva, M., Van Truong, C., & Rajabova, K. (2025). Deep Learning Enhanced Predictive Maintenance Framework Using Industrial Internet of Things Sensors for Smart Manufacturing Systems. *International Journal of Industrial Engineering and Management*, *16*(4), 389-410. https://doi.org/10.24867/IJIEM-395

[2] Vracar, L., Milovancevic, M., Vracar, J., Matijosius, J., Kilikevicius, A., & Buchmeister, B. (2026). MQTT enabled device for industrial environment and smart city. *Facta Universitatis, Series: Mechanical Engineering*, *24*(1), 171-182. https://doi.org/10.22190/FUME200901089

[3] Guo, C. (2025). Advanced Intelligent Routing Protocol for Energy-Aware Wireless Sensor Networks with Advanced Mobile Sink Monitoring. *Journal of Network and Systems Management*, *33*(1), 18. https://doi.org/10.1007/s10922-024-09885-x

[4] Sharma, V., Beniwal, R., & Kumar, V. (2024). Towards secure IoT system from a smart city perspective: An optimized algorithm and implementation. *Transactions on Emerging Telecommunications Technologies*, *35*(4), e4883. https://doi.org/10.1002/ett.4883

[5] Sikiru, I. A., Kora, A. D., Ezin, E. C., Imoize, A. L., & Li, C. T. (2024). Hybridization of learning techniques and quantum mechanism for IIoT security: Applications, challenges, and prospects. *Electronics*, *13*(21), 4153. https://doi.org/10.3390/electronics13214153

[6] Latip, R., Aminu, J., Hanafi, Z. M., Kamarudin, S., & Gabi, D. (2024). Metaheuristic task offloading approaches for minimization of energy consumption on edge computing: a systematic review. *Discover Internet of Things*, *4*(1), 35. https://doi.org/10.1007/s43926-024-00089-y

[7] Ali, G., Robert, W., Mijwil, M. M., Sallam, M., Ayad, J., & Adamopoulos, I. (2025). Securing the Internet of Wetland Things (IoWT) Using Machine and Deep Learning Methods: A Survey. *Mesopotamian Journal of Computer Science*, *2025*, 17-63. https://doi.org/10.58496/MJCSC/2025/002

[8] Varalakshmi, K. & Kumar, J. (2025). Optimized predictive maintenance for streaming data in industrial IoT networks using deep reinforcement learning and ensemble techniques. *Scientific Reports*, *15*(1), 27201. https://doi.org/10.1038/s41598-025-10268-8

[9] Ala'a, R., Karim, F. K., & Wang, Y. (2025). Optimizing Resource Allocation in Industrial IoT with Federated Machine Learning and Edge Computing Integration. *Results in Engineering*, 106387. https://doi.org/10.1016/j.rineng.2025.106387

[10] Latif, S., Driss, M., Boulila, W., Huma, Z. E., Jamal, S. S., Idrees, Z., & Ahmad, J. (2021). Deep learning for the industrial internet of things (iiot): A comprehensive survey of techniques, implementation frameworks, potential applications, and future directions. *Sensors*, *21*(22), 7518. https://doi.org/10.3390/s21227518

[11] Farooq, O., Singh, P., Hedabou, M., Boulila, W., & Benjdira, B. (2023). Machine learning analytic-based two-staged data management framework for internet of things. *Sensors*, *23*(5), 2427. https://doi.org/10.3390/s23052427

[12] Milić, S. D., Đurović, Ž., & Stojanović, M. D. (2023). Data science and machine learning in the IIoT concepts of power plants. *International Journal of Electrical Power & Energy Systems*, *145*, 108711. https://doi.org/10.1016/j.ijepes.2022.108711

[13] Khan, W. Z., Azam, F., & Khan, M. K. (2022). Deep-Learning-Based COVID-19 Detection: Challenges and Future Directions. *IEEE Transactions on Artificial Intelligence*, *4*(2), 210-228. https://doi.org/10.36227/techrxiv.14625885

[14] Raheem, F. & Iqbal, N. (2022). Artificial intelligence and machine learning for the industrial internet of things (IIoT). *Industrial Internet of Things*,1-20. https://doi.org/10.1201/9781003145004-1

[15] AlSuwaidan, L. (2021). The role of data management in the Industrial Internet of Things. *Concurrency and computation: Practice and experience*, *33*(23), e6031. https://doi.org/10.1002/cpe.6031

[16] Haseeb, K., Saba, T., Rehman, A., Ahmed, I., & Lloret, J. (2021). Efficient data uncertainty management for health industrial internet of things using machine learning. *International Journal of Communication Systems*, *34*(16), e4948. https://doi.org/10.1002/dac.4948

[17] Sun, W., Liu, J., & Yue, Y. (2019). AI-enhanced offloading in edge computing: When machine learning meets industrial IoT. *IEEE Network*, *33*(5), 68-74. https://doi.org/10.1109/MNET.001.1800510

[18] Zhou, L., Zhang, L., & Horn, B. K. (2020). Deep reinforcement learning-based dynamic scheduling in smart manufacturing. *Procedia Cirp*, *93*, 383-388. https://doi.org/10.1016/j.procir.2020.05.163

[19] Sharma, I. & Khullar, V. (2025). Blockchain-enabled federated learning-based privacy preservation framework for secure IoT in precision agriculture. *Journal of Industrial Information Integration*, *44*, 100765. https://doi.org/10.1016/j.jii.2024.100765

[20] Van Dinter, R., Tekinerdogan, B., & Catal, C. (2022). Predictive maintenance using digital twins: A systematic

literature review. *Information and Software Technology*, *151*, 107008. https://doi.org/10.1016/j.infsof.2022.107008

[21] Clemente-Lopez, D., de Jesus Rangel-Magdaleno, J., & Munoz-Pacheco, J. M. (2024). A lightweight chaos-based encryption scheme for IoT healthcare systems. *Internet of Things*, *25*, 101032. https://doi.org/10.1016/j.iot.2023.101032

[22] Krishnaraj, N., Elhoseny, M., Thenmozhi, M., Selim, M. M., & Shankar, K. (2020). Deep learning model for real-time image compression in Internet of Underwater Things (IoUT). *Journal of Real-Time Image Processing*, *17*(6), 2097-2111. https://doi.org/10.1007/S11554-019-00879-6

Contact information:

R. Rengaraj alias Muralidharan, Assistant Professor
Department of Information technology,
Saranathan College of Engineering, Trichy, India
E-mail: rengaraj-it@saranathan.ac.in

Dr. S. P. Santhoshkumar, Assistant Professor (SG)
Department of Computer Science and Engineering, School of Computing,
Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science & Technology,
Chennai, Tamilnadu, India
E-mail: spsanthoshkumar16@gmail.com

Hanan Abdullah MENGASH
Department of Information Systems,
College of Computer and Information Sciences,
Princess Nourah bint Abdulrahman University,
P. O. Box 84428, Riyadh 11671, Saudi Arabia

Shravan Kumar ADEPU
(Corresponding author)
Department of Biomedical Engineering,
Saveetha School of Engineering,
Saveetha Institute of Medical and Technical Sciences,
Saveetha University,
Saveetha Nagar, Thandalam, Chennai, Tamil Nadu, India
E-mail: shravankumar.simts@gmail.com