Journal of Theoretical and Applied Information Technology
28th February 2026. Vol.104. No.4

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

END-TO-END SECURE COMMUNICATION IN FOR WIRELESS MULTIMEDIA SENSOR NETWORKS VIA MODIFIED GORILLA TROOPS OPTIMIZER DRIVEN DATA COMPRESSION WITH ENCRYPTION APPROACH

K. VINAYAKAN, V. ALAMELU MANGAYARKARASI, Dr. A. DINESH KUMAR, M. VASUKI, R. JAYAKUMAR

Assistant Professor, Department of Computer Science, Khadir Mohideen College, Adirampattiam. Tamil Nadu, India (Affiliated to Bharathidasan University), Assistant Professor Department of Computer Applications, S.T.E.T Women's College (Affiliated to Bharathidasan University), Mannargudi, Tamil Nadu

Assistant Professor & Research Supervisor, PG & Research Department of Mathematics, Khadir Mohideen College, Adirampattinam. Assistant Professor, Department of Mathematics, Srinivasan College of Arts and Science, Perambalur, Tamil Nadu

Professor, Department of Computer Application, Mahendra Engineering College, Namakkal DT

E-mail: k.vinayakan@gmail.com, vsalamu@gmail.com, dradineshkumar@gmail.com, vasuki.scas@gmail.com, mymailjsjk@gmail.com

ABSTRACT

Wireless Multimedia Sensor Networks (WMSNs) have shifted the focus from traditional scalar wireless sensor networks (WSNs) to networks equipped with multimedia devices capable of capturing images, audio, video, and scalar sensor data. WMSN can provide multimedia content owing to the availability of low-cost CMOS microphones and cameras in addition to the considerable progress in multimedia source coding and distributed signal processing techniques. In comparison to a compressed image, an uncompressed image transmission consumes more energy, and, as a result, it becomes a necessity to establish an energy-aware compression technique to prolong the sensor node and the network lifetime. Simultaneously, security encryption systems can be used to protect the data being transferred, which ensures integrity and confidentiality against tampering and unauthorized access. This study develops an Integrated Approach for Secure and Energy-Efficient Data Transmission in Wireless Multimedia Sensor Networks (IASEE-DTWMSN) technique. The purpose of the IASEE-DTWSN method is to ensure security and maximum energy efficiency in WMSN via data compression and encryption algorithms. Initially, the IASEE-DTWSN technique compresses the images captured by WMSN using a discrete cosine transform (DCT) approach. Besides, the secure transmission of the compressed data can be accomplished using an advanced encryption standard (AES) model. Furthermore, the IASEE-DTWSN technique involves the design of a Modified Gorilla Troops Optimizer (MGTO) for optimizing the DCT and AES models. The MGTO approach is applied for determining the optimum quantization parameters of the DCT methodology and encryption key selection of the AES model in such a way that the compression ratio and PSNR are maximized. To validate the performance of the IASEE-DTWSN methodology, a broad array of simulations was involved. The experimental outcomes inferred that the IASEE-DTWSN model resulted in enhanced energy efficiency and security in the WMSN.

Keywords: *Wireless Multimedia Sensor Networks; Advanced Encryption Standard; Gorilla Troops Optimizer; Data Compression; Encryption*

1. INTRODUCTION

The fast growth and development of sensors, MEMS, embedded computing, as well as the accessibility of low-cost CMOS microphones and cameras united by the major development in dispersed signal handling and multi-media source coding models, permitted for the advent of wireless multi-media sensor network (WMSN) [1]. As a consequence, WMSN is a system of wirelessly unified sensor nodes provided with multi-media gadgets like microphones and cameras, and efficient in recovering audio and video streams, still imageries, and scalar sensor data [2]. WMSN secures a huge array of latent uses in both military and civilian regions which need audio and visual data like law-enforcement reports, traffic control systems, surveillance sensor networks, innovative health care distribution, automatic aid to old telemedicine, and manufacturing procedure control [3]. These uses of multi-media support contain latent of improving the stage of data collected, increasing the variety of coverage, and allowing multi-resolution visions (that is, in contrast to the dimensions of scalar data). WMSN also contains further features and tasks, furthermore to those of WSN, because of real multi-media data like real delivery, higher bandwidth demand, acceptable endwise delay, and appropriate jitter and frame rate of loss [4]. Furthermore, there are numerous dissimilar resource constrictions in WMSN including bandwidth, memory, energy, buffer size, rate of data, and processing ability due to the smaller size of sensors and multi-media application in nature normally generating a vast quantity of data [5]. So, in order to sustain the QoS needs and to utilize the network scarce sources in a reasonable and effective method, these features of WMSN besides other study problems like security and coverage [6].

In the present scenario, compressive sensing (CS) has been commonly utilized, permitting the complete signal to be defined from moderately few linear dimensions [7]. It is employed to capture and signify compressible signals at a rate considerably under the rate of Nyquist. It simultaneously intellects and compresses the data at a lower difficulty. Generally, WMSNs may face numerous safety threats, and much research work has been applied in order to find safety problems in these networks [8]. Amongst the accessible safety protection devices for WMSN, cryptography is an effectual model that can deliver integrity, confidentiality, and authenticity to sensor nodes and sensed data. Briefly, cryptography is the set of models for altering new unprotected data into a set of unreadable secure data, which can only be correctly read by the accurate recipient. Cryptography generally trusts safety keys for data encryption, delivering flexibility for the decryption and encryption procedure, but also inserting concerns associated with the organization of such keys [9]. Depending upon dissimilar mathematical systems and utilizing dissimilar models, cryptography techniques will naturally have dissimilar performances in handling and memory costs, as well as resistance to assaults, creating the selection of the most suitable systems as a related design selection [10].

This study develops an Integrated Approach for Secure and Energy-Efficient Data Transmission in Wireless Multimedia Sensor Networks (IASEE-DTWMSN) technique. In the IASEE-DTWSN technique, the IASEE-DTWSN technique compresses the images captured by WMSN using the discrete cosine transform (DCT) approach. Besides, the secure transmission of the compressed data can be accomplished by the use of an advanced encryption standard (AES) model. Furthermore, the IASEE-DTWSN technique involves the design of a Modified Gorilla Troops Optimizer (MGTO) for optimizing the DCT and AES models. The MGTO algorithm is used to define the optimum quantization parameters of the DCT model and encryption key selection of the AES model, in such a way that the compression ratio and PSNR are maximized. The experimental results inferred that the IASEE-DTWSN model resulted in enhanced energy efficacy and security in the WMSN.

1.1 Problem of the Statement

Wireless Multimedia Sensor Networks (WMSNs) are widely used in applications such as surveillance, healthcare, and traffic monitoring, where large volumes of multimedia data must be transmitted efficiently and securely. However, WMSNs suffer from severe resource constraints, including limited energy, bandwidth, memory, and computational capability. Transmitting uncompressed or poorly optimized multimedia data significantly increases energy consumption, reduces network lifetime, and degrades Quality of Service (QoS).

Furthermore, the open nature of wireless communication exposes WMSNs to security threats such as eavesdropping and data tampering. Although conventional encryption techniques ensure data confidentiality and integrity, they often introduce high computational and energy overhead, making them unsuitable for resource-constrained environments. Existing studies typically address compression and security separately or use static configurations, failing to balance compression efficiency, image quality, security strength, and energy consumption in an integrated manner. Hence, there is a need for an optimized, energy-efficient end-to-end framework that jointly performs secure data compression and encryption in WMSNs.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

2. RELATED WORKS

2.1 Proposed Study from Existing Literature

Although several studies have addressed multimedia data compression, security, and energy efficiency in Wireless Multimedia Sensor Networks (WMSNs), the present work differs from existing literature in several important aspects. Most prior research treats **data compression and encryption as independent processes**, applying security mechanisms after compression without considering their combined impact on energy consumption and reconstruction quality. In contrast, this study proposes a **fully integrated end-to-end framework** in which compression and encryption are jointly optimized.

Existing approaches commonly employ **static parameter settings** or optimize a single performance objective, such as compression ratio or security strength, which limits adaptability under varying multimedia and network conditions. The proposed study introduces a **Modified Gorilla Troops Optimizer (MGTO)** that dynamically optimizes both DCT-based compression parameters and AES encryption settings, enabling simultaneous improvement in compression efficiency, image quality, and energy consumption.

Furthermore, many optimization-based techniques reported in the literature focus primarily on reducing data size or computational complexity, with limited emphasis on **perceptual image quality and power-saving metrics**. This work explicitly incorporates multiple evaluation criteria, including PSNR, SSIM, MSE, encryption/decryption time, and power-saving efficiency, providing a more comprehensive performance assessment.

Unlike earlier studies that validate performance using limited datasets or isolated scenarios, this research conducts a **comparative experimental analysis using standard benchmark multimedia images**, ensuring reproducibility and fair comparison with state-of-the-art methods. Overall, the novelty of this study lies in its **adaptive, optimization-driven integration of compression and encryption**, which effectively balances security, energy efficiency, and Quality of Service in Wireless Multimedia Sensor Networks.

Khashan et al. [11] presented an advanced PRE system that is exactly modified for WSN to improve the safe communication among nodes in the system and exterior data server. The developed PRE structure enhances efficacy by combining lightweight asymmetric and symmetric cryptographic models, minimalizing computation costs throughout PRE processes and preserving energy for resource-constrained nodes. Furthermore, this technique includes refined key organization and digital permits to safeguard safe key distribution and generation that enables unified authentication and scalable information distribution amongst the units in WSN. In [12], an energy-enhancing safe routing scheme is projected for the application of IoT in heterogeneous WSNs. In this developed scheme, a safe route is recognized for the personal data of IoT over SNs with assorted energy utilizing the multi-path link routing protocol (MLRP). Next creating the safe route, the network, and energy lifespan are enhanced by utilizing the protocol of hybrid-based TEEN (H-TEEN) and contain load balancing (LB) capacity. Biswas et al. [13] developed an Energy Efficient Secure Multi-path (EESM) routing protocol to firmly build effective routes and convey data packets. EESM attains energy efficacy over the least task allocation between SN while every task computation-intensive like routing table generation, network data collection, and network maintenance are executed by BS.

In [14], the Network Adaptive Multi-Mode Transmission (NAMT) technique is specially intended to enhance QoS by dynamically altering transmission methods in real based on the conditions of the network. Constructing on the initial principles of the LEACH protocol, the NAMT technique improves it by including real-time network observation, adaptive modulation, and predictive analytics. The improved protocol, named NAMT-LEACH, especially finds the restrictions of traditional LEACH by incorporating many parameter-based cluster head (CH) selection and topology-AMT abilities. Kethireddy et al. [15] projected an optimum cooperative relay selection (OCRS) model. Furthermore, an energy-effective cooperative multi-media transmission (EECMT) model is developed. This method uses the auto-correction code feature existing in the QR code for enhancing the execution of MWMSN. Majeed et al. [16] projected an energy-efficient distributed congestion control protocol (DCCP) to diminish congestion and increase endwise delay. Initially, congestion is perceived by utilizing dual congestion indicators. Next, every node totals the usual data and constructs a traffic congestion

Journal of Theoretical and Applied Information Technology
28th February 2026. Vol.104. No.4

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

map. Then it is employed to compute the finest track.

In [17], safe data transmission is proposed. For IDS, Fuzzy logic, and ANN are developed. At first, the nodes were arbitrarily positioned in the network and set to collect data. Similarly, LEACH selects CH at random and assigns this part to the numerous nodes depending on a round-robin management device. In WSN, a Fuzzy interference rule has been employed. Then, an ANN has been deployed to differentiate the destructive nodes from suspicious nodes. Vimala and Manikandan [18] proposed an elliptic curve cryptography-enabled cipher text policy attribute-based encryption (ECC-CP-ABE) model. In this research work, a reliable node-based value of trust mechanism is chosen. In proposed technique, the CH and CM nodes use CP-ABE for the message encryption utilizing an access policy calculated from an AND-OR operation over numerous sets of features.

3. RESEARCH METHODOLOGY

In this paper, we have developed an innovative IASEE-DTWMSN approach. The major intention of the IASEE-DTWSN methodology is to ensure security and maximum energy efficiency in WMSN via data compression and encryption algorithms. Fig. 1 represents the workflow of the IASEE-DTWMSN technique.

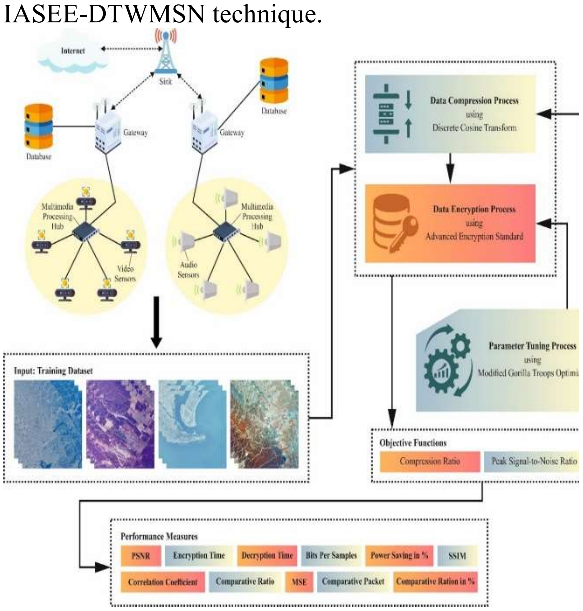

Fig. 1. Workflow Of IASEE-DTWMSN Technique

3.1 Design of the Work

This study adopts a comparative experimental research design, consistent with prior research in Wireless Multimedia Sensor Networks (WMSNs) that integrates data compression, security, and optimization techniques. Earlier studies have demonstrated that transform-based compression methods such as Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) are effective in reducing multimedia data size while preserving reconstruction quality in WMSNs. Similarly, lightweight cryptographic algorithms, particularly AES-based encryption, have been widely used in previous works to ensure data confidentiality and integrity under resource constraints.

Recent studies have further shown that metaheuristic optimization algorithms, including Particle Swarm Optimization, Genetic Algorithms, Ant Colony Optimization, and Gorilla Troops Optimizer (GTO), are effective in tuning compression parameters and reducing energy consumption in sensor networks. However, most of these studies either optimize compression or security independently, or apply static parameter configurations that fail to adapt to varying multimedia and network conditions.

Following the experimental frameworks of these earlier studies, the present research is designed to (i) develop an integrated compression–encryption model, (ii) incorporate an optimization mechanism to adaptively tune system parameters, and (iii) evaluate performance through simulation-based experimentation. Benchmark multimedia images commonly used in earlier research are employed to ensure fair comparison and reproducibility. The proposed Modified Gorilla Troops Optimizer (MGTO) is used to simultaneously optimize compression and encryption parameters, extending existing GTO-based designs reported in recent literature.

Performance evaluation follows criteria widely adopted in similar studies, including compression ratio, PSNR, MSE, SSIM, encryption/decryption time, and energy consumption. Comparative analysis with state-of-the-art approaches reported in earlier studies is conducted to validate the effectiveness and novelty of the proposed research design.

3.2. Image Compression via DCT

Initially, the IASEE-DTWSN technique compresses the images captured by WMSN using the DCT approach. The basic method of JPEG image compression is the DCT [19]. The DCT transform can map a block of pixel value within spatial to frequency domains. The DCT can mathematically model in any size but an image is

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

a 2D surface hence the 2D-DCT transform can be utilized.

$$T[i,j] = c(i,j) \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} V\,[x,y] \times \cos\frac{(2y+1)i\pi}{2N} \times \cos\frac{(2x+1)j\pi}{2N} \quad (1)$$

Now

$$c(i,j) = \frac{2}{N}, i \; and \; j \neq 0$$

$$c(i,j) = \frac{1}{N}, i \; and \; j = 0.$$

The DCT is better on small images. Once the DCT can be used for larger images, the rounding effect, if the floating-point number is kept in the computer system, leads to the DCT coefficient keeping inadequate accuracy. As the image size increases, the count of computations disproportionately upsurges. For this reason, the images are divided into 8x8 blocks. The images are padded with white pixels (additional pixels can be added such that the images are sub-divided into an integral number of 8x8 block) where the images are not an integral number of 8x8 block. The 2D-DCT can be used for all the blocks such that 8x8 matrices of the DCT coefficient are generated for all the blocks. This is called a DCT matrix. The top left components of the DCT matrix are taken as a background color of the block. The residual 63 components are termed as "AC" component. Fig. 2 represents the structure of DCT.

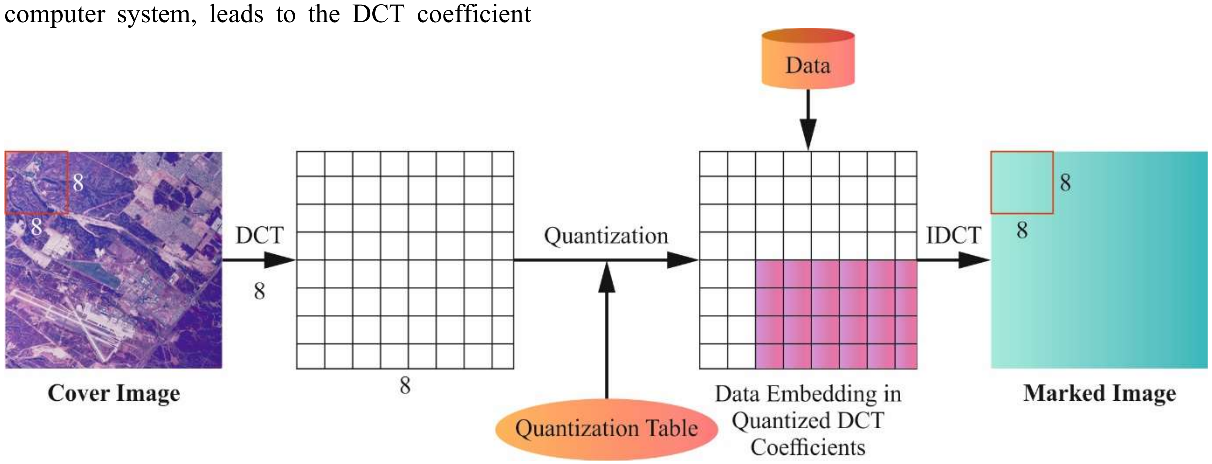

Fig. 2. Structure Of DCT

In the DCT matrix, all the components indicate the frequency in an image. The high-frequency component is lesser visible to the human eye, and it is a property that is utilized in JPEG this higher-frequency component is removed or attenuated with less noticeable effects on the image quality. Therefore, the smoothness property of the SVM is used for modelling the DCT coefficient. The new image blocks are improved from the DCT coefficient through the inverse DCT (IDCT), as follows

$$T[i,j] = c(i,j) \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} V\,[x,y].\cos\frac{(2y+1)i\pi}{2N} \times \cos\frac{(2x+1)j\pi}{2N} \quad (2)$$

Where

$$c(i,j) = \frac{2}{N}, i \; and \; j \neq 0$$

$$c(i,j) = \frac{1}{N}, i \; and \; j = 0.$$

3.2. Encryption using AES

Next, the secure transmission of the compressed data can be achieved by the utilization of the AES technique. AES is used to encrypt the plaintext having lb bytes, whereas $lb = 16, 24$, or 32 [20]. The plaintext is a $a(4\text{x}Nb)$ array (a_{ij}), $0 \leq i < 4, 0 \leq j < Nb - 1$, in which $= 4,6,8$, based on lb values. The n^{th} bytes of the plaintexts are kept in byte $a_{i,j}$ with $i = n$ mod 4, $j = \left\lfloor \frac{n}{4} \right\rfloor$.

AES makes use of a secret key, known as cipher key (CK), having lk bytes, where $= 16,24$, or 32. Any group of lb and lk rates can be allowable. The CK is a $4\text{x}Nk$ array (k_{ij}), $0 \leq i < 4, 0 \leq j \leq Nk - 1$, where $Nk = 4,6,8$, based on the lk value. The n^{th} key bytes are stored in byte k_{ij} with $i = n$ mod 4, $j = \left\lfloor \frac{n}{4} \right\rfloor$.

The process of AES encryption consists of *rounds*. Excepting the final round, all the rounds have four transformations known as AddRoundKey, ByteSub, ShiftRow, and

MixColumn. The transformation MixColumn is neglected in the final round. The transformation functions on intermediate outcomes known as *state*. The state is a 4xNb array (a_{ij}) of bytes. Firstly, the plaintext that encrypted. Nr refers to the round counts set to 10, 12, or 14, based on max$\{Nb, Nk\}$. AddRoundKey is used to the plaintext before the first round together with the transformation implemented in the Nr round.

The transformation AddRoundKey. The input state (a_{ij}), $0 \le i < 4, 0 \le j < Nb$, and a round key (RF) that is an array of bytes (rk_{ij}), $0 \le i < 4, 0 \le j < Nb$. The resultant of AddRoundKey is the (b_{ij}), $0 \le i < 4, 0 \le j < Nb$, whereas

$$b_{ij} = a_{ij} \oplus rk_{ij}.$$

The RK is attained in the *CK* by extending the *CK* array (k_{ij}) into an array (k_{ij}), $0 \le i < 4, 0 \le j \le Nr.Nb$, known as the expanded key (EK). The exact process whereby the *EK* is attained from the *CK* has no significance for the attack. The RK for the *AddRoundKey* is considered as the initial Nb column of the *EK*. Therefore, the RK for the initial round is considered a *CK*. Generally, the RK for the AddRoundKey application in the m^{th} rounds of AES is $mNb, \ldots, (m+1)Nb - 1$ of the *EK*, $1 \le m \le Nr$.

The transformation $ByteSub$. Assume the state (a_{ij}), $0 \le i < 4, 0 \le j < Nb$, the transformation ByteSub employs invertible function: $\{0,1\}^8 \to \{0,1\}^8$ to byte a_{ij}. S has no significance for the attacks. S is nonlinear, and the only nonlinear part of the AES encryption technique and realized often by the *S-box* or substitution table. Fig. 3 defines the structure of AES encryption.

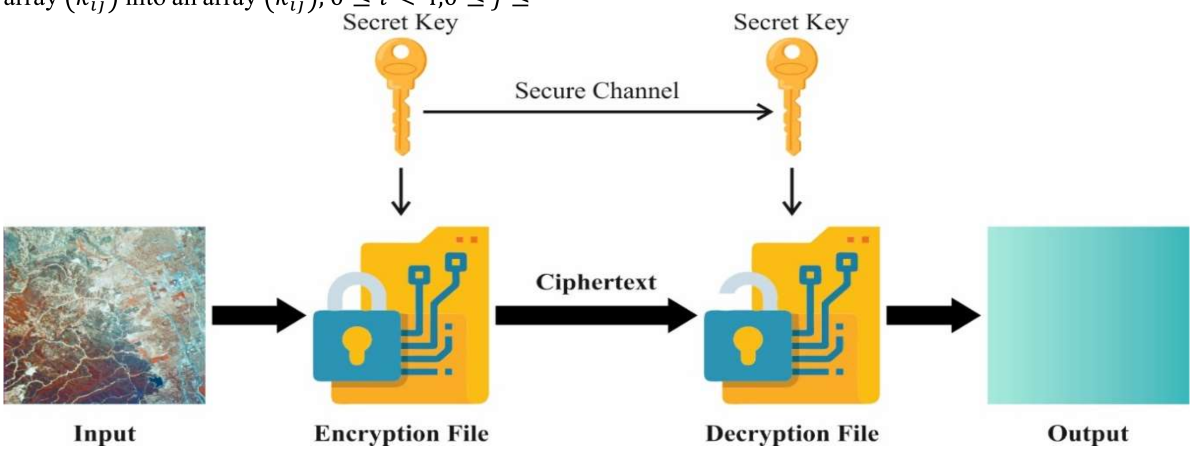

Fig. 3. Aes Encryption

The transformation ShiftRow is used to shift all the rows of a state (a_{ij}) to the left. Row 0 is not shifted. Rows 1, 2, and 3 are shifted through the C_1, C_2, *and* C_3 bytes, correspondingly, where C_i value depends on Nb.

The transformation MixColumn is vital to the attacks that function on the column of a state. A linear conversion is utilized for all the columns. Bytes are taken as elements in the field F_{2^8}. MixColumn is applied to all the rows of state.

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \quad (3)$$

The operation xtime. The multiplication in F_{2^8} is essential for computing the transformation MixColumn that has significance to the attack.

$$F_{2^8} = \frac{F_2[x]}{x^8 + x^4 + x^3 + x + 1}. \quad (4)$$

The F_{2^8} is polynomial over F_2. The multiplication and addition of both polynomials is performed $x^8 + x^4 + x^3 + x + 1$ polynomial. The byte $a = (a_7, \ldots, a_1, a_0)$ is corresponding to the $a_7x^7 + \cdots a_1x + a_0$ polynomial. The multiplication of $a = (a_7, \ldots, a_1, a_0)$ component in F_{2^8} are realized by multiplying the $a_7x^7 + \cdots a_1x + a_0$ polynomial with the 1 polynomial, $0x + 1$, correspondingly, and modulo $x^8 + x^4 + x^3 + x + 1$

$$01 \cdot a = a$$

$$03 \cdot a = 02 \cdot a + a.$$

The column of state is multiplied by Eq. (1) and is decreased to several additions modulo 2 and multiplication by 02. The multiplication of byte is considered as 02 by $xtime(a)$.

$$a = (a_7, \ldots, a_0)$$

$$xtime\ (a) = \begin{cases} (a_6, \ldots, a_0, 0) if\ a_7 = 0 \\ (a_6, \ldots, a_0, 0) \oplus (0,0,0,1,1,0,1,1)\ if\ a_7 = 1 \end{cases} \quad (5)$$

3.3. Modelling of MGTO for DCT and AES Optimization

Finally, the IASEE-DTWSN technique involves the design of MGTO for optimizing the DCT and AES models. The artificial gorilla group optimizer method is a meta-heuristic model based on the behaviour of the gorilla group [21]. Generally, the gorilla is the biggest and most robust chimpanzee. Moreover, Gorillas are considered as social creatures. Every group is directed by a mature gorilla male and contains a sturdy intellect of land. It is because, the back hair of a few male gorillas is white in color, so this kind of gorillas were named silverback gorillas.

A gorilla group generally contains numerous mature male gorillas, female gorillas, and their children. As a leader, mature male gorillas take up the duties of caring for land, decision-making, and managing other gorillas to discover their nutrition. Male gorillas can able to enlarge their land over struggle, and opposition between female and male gorillas is predictable. Likewise, the link amongst female and male gorillas is near, while the link among female gorillas is cold.

3.4 Exploration Phase

During this phase, the optimizer procedure is defined. In the group of gorillas, we recognize that there is a silverback gorilla who directs every verdict. Mostly, gorillas move to locations to search for food, which may be also odd. The silverback gorilla is measured as the optimum candidate performance at every optimizer of this phase. Also, this fragment presents 3 mechanisms, which start at this phase.

In this stage, the 3 mechanisms are stated in Eq. (6), whereas p denotes the parameter among 0 and 1 that influences the migration tactic of unknown locations. If $< p$, the present gorilla's location will travel to a location of unknown. This allows the GTO model to observe the complete space of the problem, which creates the allocation of solutions completer and more spread. In contrast, if $\geq p$, dual other devices will be selected. Next, if ≥ 0.5, the gorilla will travel to the track of other gorillas. If < 0.5, the gorillas travel to the well-known location. This enhanced the capability of GTO method to evade from local optimum solution. Eq. (6) is mentioned below:

$$GX(t+1) = \left\{\begin{matrix} (UB - LB) \times r_1 + LB, rand < p \\ (r_2 - C) \times X_r(t) + L \times H, rand \geq 0.5 \\ X(t) - L \times \left(L \times \left(X(t) - GX(t)\right)\right) + r_3 \times \left(X(t) - GX_r(t)\right), rand < 0.5 \end{matrix}\right\}, r\ and \geq p \quad (6)$$

Whereas, $GX(t+1)$ signifies the site vector of the gorilla, and $X(t)$ denotes the existing place of a gorilla. The location vector size is definite by the problem size. r_1, r_2, r_3, and $rand$ signify the randomly generated numbers among 0 and 1 made with an even distribution. UB and LB signify the upper and lower bound, correspondingly. GX_r and X_r are the site vectors of nominated gorillas at random. The calculation for computing L and H is given in Eq. (6):

$$C = F \times \left(1 - \frac{t}{Max\ It}\right) \quad (7)$$

Here, t refers to the present iteration count and $MaxIt$ indicates the maximal iteration count. Throughout the first phase, the C value contains a huge alteration in the initial stage and a slight alteration in the future phase. This means the initial phase has better randomness to increase the sort of exploration, and in the future phase, it gets less to accomplish the result of fast convergence. F is intended below:

$$F = \cos(2 \times r_4) + 1 \quad (8)$$

Here, r_4 denotes a randomly generated number 0 and 1 to guarantee the arbitrariness of the hunt which is helpful in discovering the global optimum performance.

L denotes the parameter, which is employed to pretend the silverback gorilla control that is intended in the below-given calculation:

$$L = C \times l \quad (9)$$

Whereas, l represents the randomly generated number among -1 and 1. Silverback gorillas will create faults in discovering nutrition or handling clusters owing to an absence of experience. So, they can get dependable experience and risky constancy below the control of leaders. Simultaneously, Eq. (9) is exploited to simulate the leadership of the silverback gorilla. While H in Eq. (6) is computed with Eq. (10). The Z in Eq. (10) is computed with Eq. (6), whereas Z denotes a randomly generated value and in the interval of $-C, C$.

$$H = Z \times X(t) \quad (10)$$

$$Z = [-C, C] \quad (11)$$

Finally, X and GX fitness values are intended. When the fitness value of $GX(t)$ is lesser than $X(t)$, then the location of $GX(t)$ will substitute the $X(t)$ location.

3.5 Exploitation Stage

1. Following the Silverback

During this phase, dual actions are acquired: by obeying the silverback gorilla and opposing the mature gorilla females. During the cluster of gorillas, the silverback gorilla behaviour guiding the other gorillas and challenging female gorillas are dual dissimilar actions. So, the value of C

Journal of Theoretical and Applied Information Technology
28th February 2026. Vol.104. No.4
© Little Lion Scientific
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

rules adult male gorillas and tracks the silverback gorilla or struggles with other dudes. If C faces dissimilar situations, the equivalent tactic is chosen. W denotes the parameter that fixed the earlier optimizer.

Silverback and other kind of gorillas are well capable of accomplishing their responsibilities when young. At once, male gorillas select to obey silverback gorillas. Besides, every gorilla can impact another one. So, the existing individual position solution will respect the silverback gorilla optimal solution. That is, if $C \geq W$, then the strategy will be implemented. This type of performance is pretended by Eq. (11):

$$GX(t+1) = L \times M \times (X(t) - X_{silverbak}) + X(t) \quad (11)$$

Whereas $X_{Silverback}$ signifies the optimum solution, and M can be intended with Eq. (12):

$$M = \left(|\frac{1}{N}\sum_{i=1}^{N} G\,X_i(t)|^{g} \right)^{\frac{1}{g}} \quad (12)$$

where $GX(t)$ denotes the vector location throughout the iteration. The location vector size is definite by the problematic size, N signifies the entire gorilla count, and g is computed with Eq. (13) as given below:

$$g = 2^{L} \quad (13)$$

2. Competition for Adult Females

The young gorillas' foremost action is to play with other gorillas of male for the opposed sexual role. This type of struggle is considered strong, enduring, and capable of effect other followers. The opposition among them signifies the common inspiration for a solution. The silverback gorilla optimum solution travels near the site of other solutions, so disturbing the present solution to a definite range and helping the exploration for an enhanced solution. The mathematical calculation of this behaviour is pretended in Eq. (14):

$$GX(t) = X_{silverback} - (X_{silverback} \times Q - X(t) \times Q) \times A \quad (14)$$

$$Q = 2 \times r_5 - 1 \quad (15)$$

$$A = \beta \times E \quad (16)$$

$$E = \begin{cases} N_1, rand \geq 0.5 \\ N_2, rand < 0.5 \end{cases} \quad (17)$$

Here, Q denotes the opposition power of the pretend gorilla, r_5 represents the randomly generated number among $zero$ and one in a uniform distribution, A refers to the vector of coefficient, which is employed to pretend the grade of competition, β indices the set of parameters before the optimizer process, E is employed to pretend the influence of strength, $Rand$ refers to the randomly produced integer among $zero$ and one. If $rand \geq 0.5$, then E will be equivalent to the randomly generated integer from the normal distribution; or else, E will not be identical to the randomly produced integer in the normal distribution.

The enhanced is named as the higher and lower velocity ratios [22]. This method was intended to resolve the probability that the optimal value might drop into local goals. Numerous current models have been proposed based on this approach and they have been functional for numerous optimizer issues such as the parameter of controller unite proportional-integral-derivative (PID) and fractional order control models utilizing Enhanced Runge Kutta Optimizer and size of optimum and position of numerous FACTS gadgets to attain diminishing fuel costs and minimalizing power losses utilizing Enhanced Tuna Swarm Optimizer. This development relies on dual phases. The 1st phase is the higher-velocity ratio state.

$$it < \frac{1}{3}\, Maxit \quad (18)$$

$$S = \overrightarrow{R_B} \otimes \left(E - \overrightarrow{R_B} \otimes X_i(t)\right) \quad (19)$$

$$X_i(t+1) = X_i(t) + P \cdot \overrightarrow{R_B} \otimes S \quad (20)$$

Whereas, $\overrightarrow{R_B}$ depicts a vector of randomly generated numbers from the Normal distribution, which reflects the Brownian motion. The symbol $\otimes$ signifies the entry-wise growth. A novel location was pretended by multiplying $\overrightarrow{R_B}$ with the preceding location, $P = 0.5$ signifies a value of constant, and $\overrightarrow{R_B}$ epitomizes a vector of randomly generated outcomes from 0 and 1. This state occurs throughout the 1st and 3rd of iterations if the size of the step is big, illustrating a higher level of exploratory skill. The fittest solution (E) has been chosen as the finest position to procedure a matrix by the below-mentioned calculation:

$$E = \begin{bmatrix} Xb_{1.1}^{t} & \cdots & Xb_{1.d}^{t} \\ \vdots & \ddots & \vdots \\ Xb_{n.1}^{t} & \cdots & Xb_{n.d}^{t} \end{bmatrix} \quad (21)$$

Whereas Xb denotes the finest solution that copied n times to generate the matrix of E. n refers to the amount of searching agents, while d represents the number of sizes.

The 2nd phase is called the lower ratio of velocity. This phase occurs near the end of the optimizer process that is normally linked to higher exploitation ability. Lévy is considered the finest method for lower velocity ratios. The mathematical calculation of this phase is given below:

$$it > \frac{1}{3} Maxit \quad (22)$$

$$S = \overrightarrow{R_L} \otimes \left(\overrightarrow{R_L} \otimes E - X_i(t)\right) \quad (23)$$

$$X_i(t+1) = E + P \cdot CF \otimes S \quad (24)$$

During the Lévy procedure, multiply E and R_L, while inserting the step size to position, which aids in modernizing of location. An additional characteristic of MGTO is raising the probability of evading from local least.

The MGTO algorithm optimizes the quantization parameters involved in the DCT approach in such a way that the compression ratio (CR) can be maximized. The CR is resolved as the ratio of new image size to compressed image size.

$$CR = \frac{\text{Size of the original image}}{\text{Size of the compressed image}} \quad (25)$$

Finally, the MGTO algorithm optimizes the key selection process of the AES algorithm in such a way that maximum PSNR can be obtained. It is a metric used to evaluate the quality of a compressed or encrypted image compared to the original image.

$$PSNR = 10 \cdot \log_{10}\left(\frac{MAX^2}{MSE}\right) \quad (26)$$

Where:

- MAX denotes the maximal potential pixel rate of the image (255 for an 8-bit image).
- MSE is the MSE between the original and encrypted images, calculated as the average of squared differences among corresponding pixels within 2 images.

4. RESULT ANALYSIS AND DISCUSSION

The performance analysis of the IASEE-DTWSN methodology can be examined using the USC-SIPI dataset [23]. The database has been separated into volumes relying on the simple character of pictures. Images in every volume are of distinct sizes like 256x256, 512x512, or 1024x1024 pixels. Each image has 8 bits/pixel for black and white images and 24 bits/pixel for color images. Fig. 4 illustrates the sample images. Fig. 5 depicts the sample of the original image and the compressed image

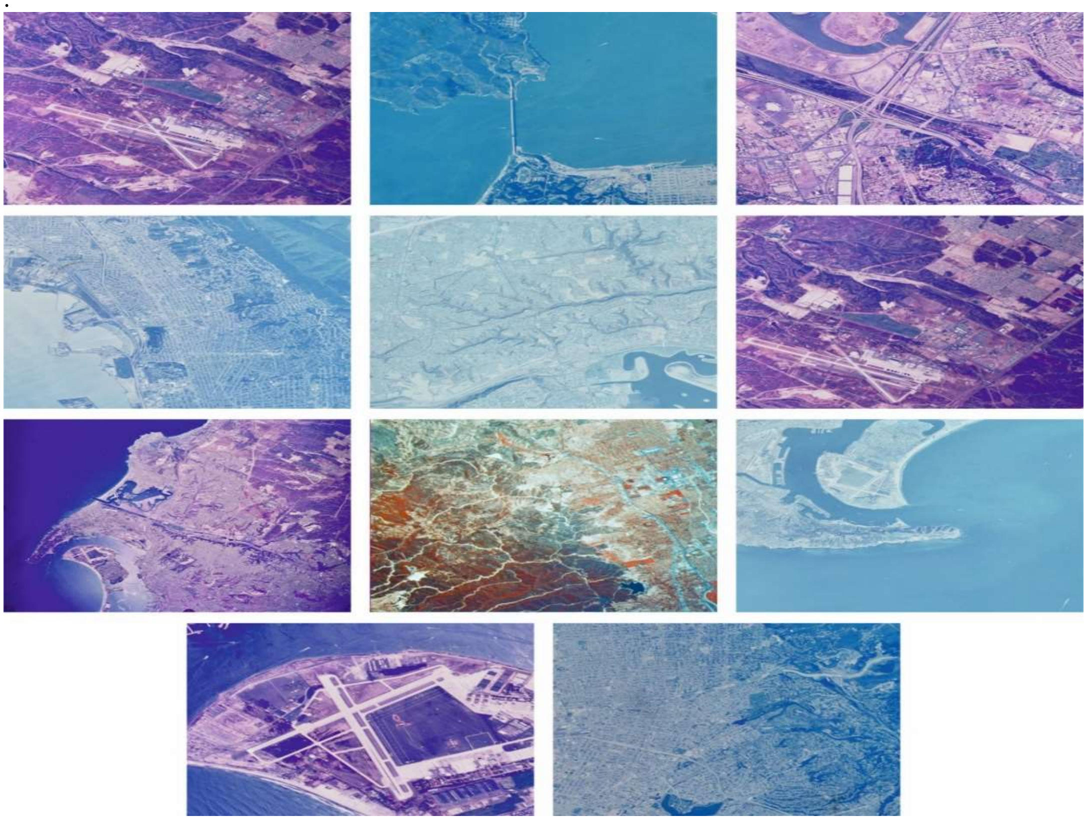

Fig. 4. Sample Images

(a)
(b)
(c)
(d)

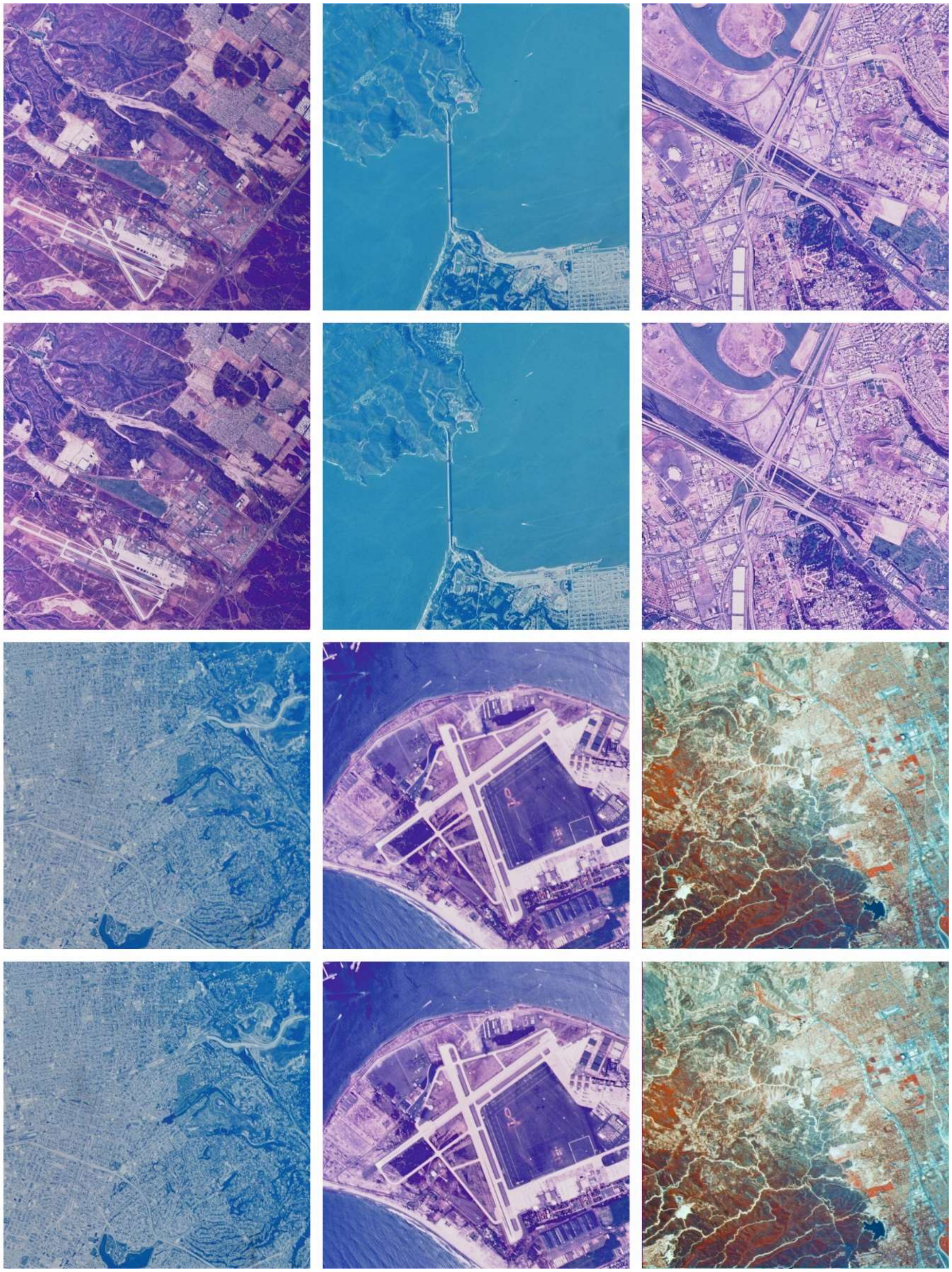

Fig. 5. (A-B) Original Image, (C-D) Compressed Image

Table 1 offers a brief encryption performance of the IASEE-DTWSN technique for encryption time (ET) and decryption time (DT).

Table 1 ET And DT Analysis Of IASEE-DTWSN Technique With Distinct Sample Images

Sample Images	Samples Size (Px)	Enc. Time (s)	Dec. Time (s)
2.1.01.tiff	262144	0.11	0.29
2.1.02.tiff	262144	0.42	0.27
2.1.03.tiff	262144	0.02	0.57
2.1.04.tiff	262144	0.31	0.81
2.1.05.tiff	262144	0.35	0.63
2.1.06.tiff	262144	0.37	0.98
2.2.01.tiff	1048576	0.82	0.24
2.2.02.tiff	1048576	0.68	0.53
2.2.03.tiff	1048576	0.47	0.96
2.2.04.tiff	1048576	0.30	0.46
2.2.05.tiff	1048576	0.66	0.55

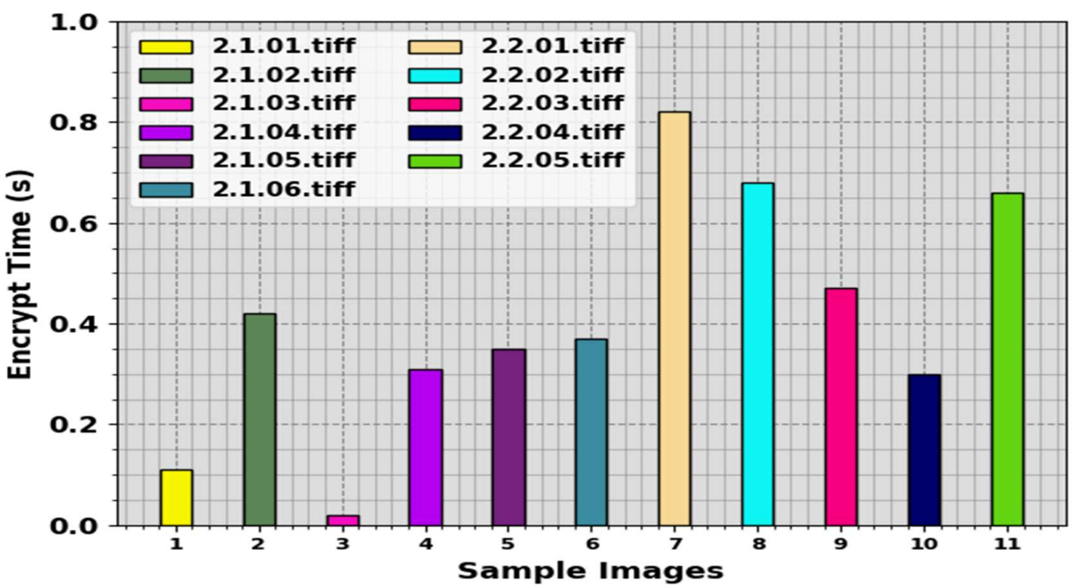

Fig. 6. ET Analysis Of IASEE-DTWSN Technique With Distinct Sample Images

In Fig. 6, the overall ET results of the IASEE-DTWSN technique under distinct images are portrayed. The figure stated that the IASEE-DTWSN technique reaches effective performance with minimal ET values. With a sample image of 2.1.01.tiff, the IASEE-DTWSN technique offers a lower ET of 0.11s. Also, with a sample image of 2.1.04.tiff, the IASEE-DTWSN approach achieves a decreased ET of 0.31s. Besides, with a sample image of 2.1.06.tiff, the IASEE-DTWSN system offers a lesser ET of 0.37s. Moreover, with a sample image of 2.2.01.tiff, the IASEE-DTWSN method offers a reduced ET of 0.82s. Furthermore, with a sample image of 2.2.04.tiff, the IASEE-DTWSN technique obtains a lower ET of 0.30s. Finally, with a sample image of 2.2.05.tiff, the IASEE-DTWSN methodology attains a minimal ET of 0.66s.

In Fig. 7, the overall DT outcomes of the IASEE-DTWSN algorithm under distinct images are represented. The outcome inferred that the IASEE-DTWSN system reaches effectual performance with lesser DT values. With a sample image of 2.1.01.tiff, the IASEE-DTWSN algorithm attains a decreased DT of 0.29s. Likewise, with a sample image of 2.1.04.tiff, the IASEE-DTWSN technique offers a minimal DT of 0.81s. In addition, with a sample image of 2.1.06.tiff, the IASEE-DTWSN technique offers a reduced DT of 0.98s. Moreover, with a sample image of 2.2.01.tiff, the IASEE-DTWSN system offers a minimum DT of 0.24s. Additionally, with a sample image of 2.2.04.tiff, the IASEE-

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

DTWSN approach attains a lower DT of 0.46s. Eventually, with a sample image of 2.2.05.tiff, the IASEE-DTWSN technique accomplishes a lower DT of 0.55s. In Table 2, a detailed compression outcome of the IASEE-DTWSN model is investigated briefly. In Fig. 8, the MSE and PSNR results of the IASEE-DTWSN methodology under various images are portrayed. The results highlighted that the IASEE-DTWSN approach accomplishes effectual MSE and PSNR values.

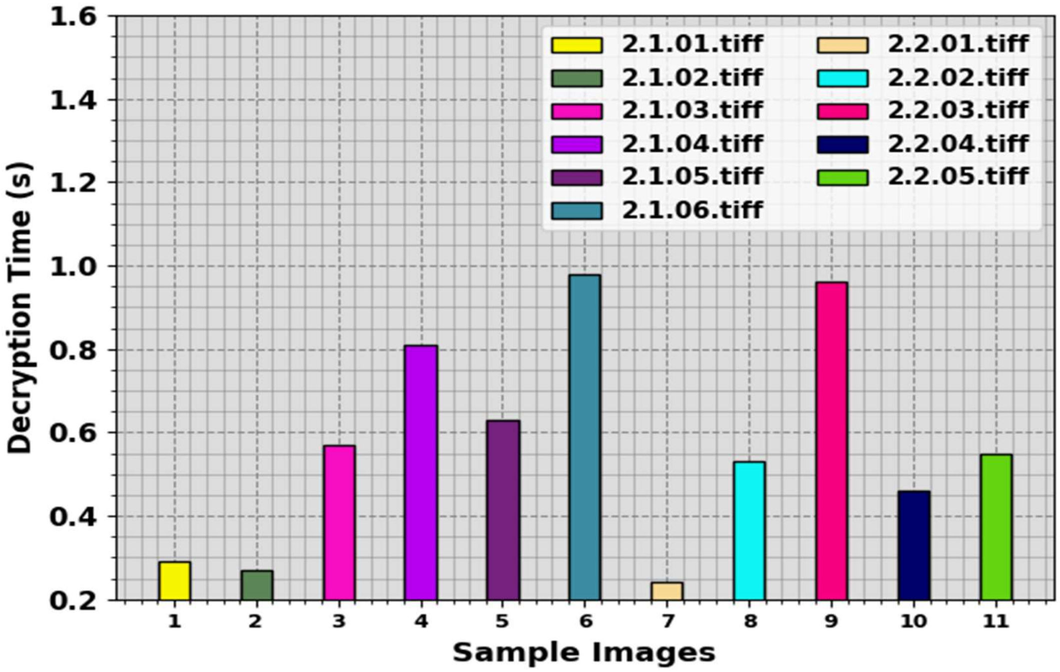

Fig. 7. DT Analysis Of IASEE-DTWSN Approach With Distinct Sample Images

Table 2 Compression Outcome Of IASEE-DTWSN Approach With Distinct Sample Images

Sample Images	MSE	PSNR (dB)	SSIM	Corr. Coeff.
2.1.01.tiff	27.52	33.73	99.00	99.00
2.1.02.tiff	31.40	33.16	99.00	99.00
2.1.03.tiff	18.13	35.55	97.00	100.00
2.1.04.tiff	33.43	32.89	99.00	99.00
2.1.05.tiff	20.27	35.06	99.00	100
2.1.06.tiff	32.94	32.95	99.00	99.00
2.2.01.tiff	25.80	34.01	99.00	100
2.2.02.tiff	14.95	36.38	97.00	100
2.2.03.tiff	16.26	36.02	98.00	99.00
2.2.04.tiff	24.01	34.33	99.00	99.00
2.2.05.tiff	27.92	33.67	99.00	99.00

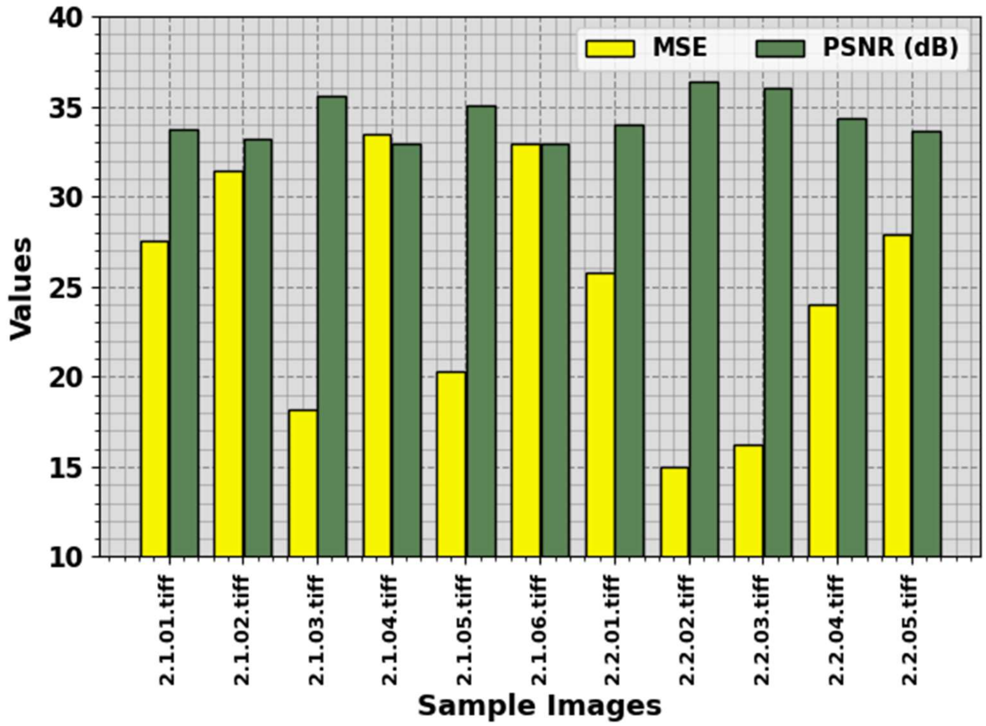

Fig. 8. MSE And PSNR Analysis Of IASEE-DTWSN Model With Various Sample Images

On the sample image of 2.1.01.tiff, the IASEE-DTWSN technique offers MSE and PSNR of 27.52 and 33.73dB, respectively. Also, on the sample image of 2.1.04.tiff, the IASEE-DTWSN approach reaches MSE and PSNR of 33.43 and 32.89dB, correspondingly. Additionally, on the sample image of 2.2.01.tiff, the IASEE-DTWSN algorithm offers MSE and PSNR of 25.80 and 34.01dB, correspondingly. Moreover, on the sample image of 2.2.05.tiff, the IASEE-DTWSN system achieves MSE and PSNR of 27.92 and 33.67dB, respectively.

In Fig. 9, the SSIM and CC outcomes of the IASEE-DTWSN method under distinct images are depicted. The outcomes exhibited that the IASEE-DTWSN system realizes effectual SSIM and CC values. On the sample image of 2.1.01.tiff, the IASEE-DTWSN algorithm reaches SSIM and CC of 99.00 and 99.00, correspondingly. Also, on the sample image of 2.1.04.tiff, the IASEE-DTWSN approach gains SSIM and CC of 99.00 and 99.00, correspondingly. Moreover, on the sample image of 2.2.01.tiff, the IASEE-DTWSN method offers SSIM and CC of 99.00 and 100, correspondingly. Additionally, on the sample image of 2.2.05.tiff, the IASEE-DTWSN algorithm offers SSIM and CC of 99.00 and 99.00, correspondingly. To further assure the compression performance of the IASEE-DTWSN technique, a brief CR analysis is made in Table 3 and Fig. 10. The results highlighted that the IASEE-DTWSN algorithm managed to obtain reasonable CR values. On the sample image of 2.1.01.tiff, the IASEE-DTWSN technique provides an enhanced CR of 76.80%.

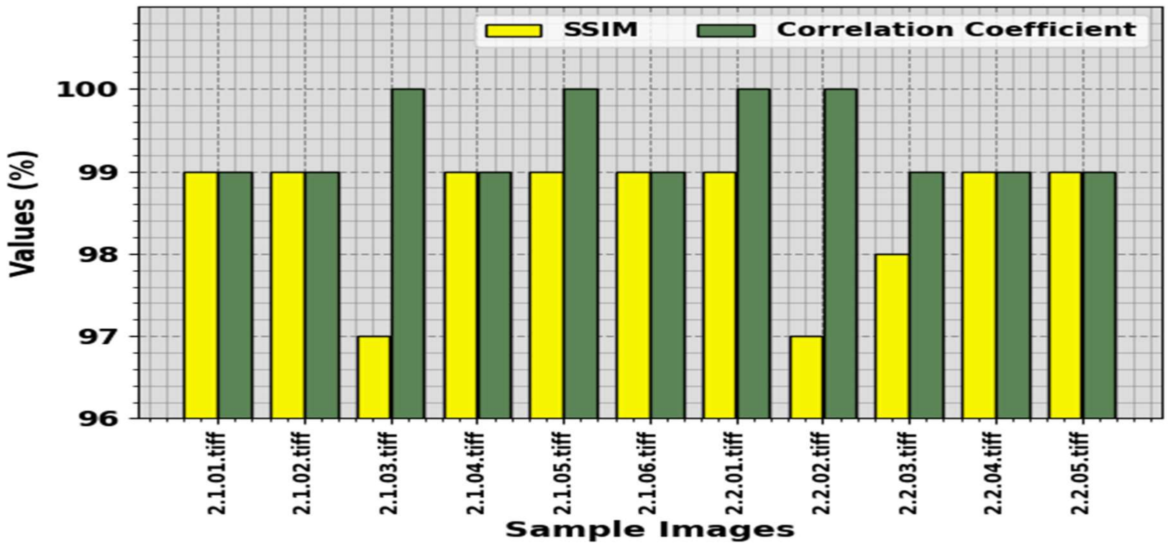

Fig. 9. SSIM And CC Analysis Of The IASEE-DTWSN System With Various Sample Images

Table 3 Compression Outcome Of IASEE-DTWSN Technique With Various Sample Images

Sample Images	Original Size (Bits)	Compressed Size (Bits)	Comp. Ratio (%)
2.1.01.tiff	786572	182480	76.80
2.1.02.tiff	786572	196928	74.96
2.1.03.tiff	786572	106752	86.43
2.1.04.tiff	786572	185376	76.43
2.1.05.tiff	786572	148128	81.17
2.1.06.tiff	786572	178624	77.29
2.2.01.tiff	3145868	660992	78.99
2.2.02.tiff	3145868	375824	88.05
2.2.03.tiff	3145868	460912	85.35
2.2.04.tiff	3145868	600128	80.92
2.2.05.tiff	3145868	623664	80.18

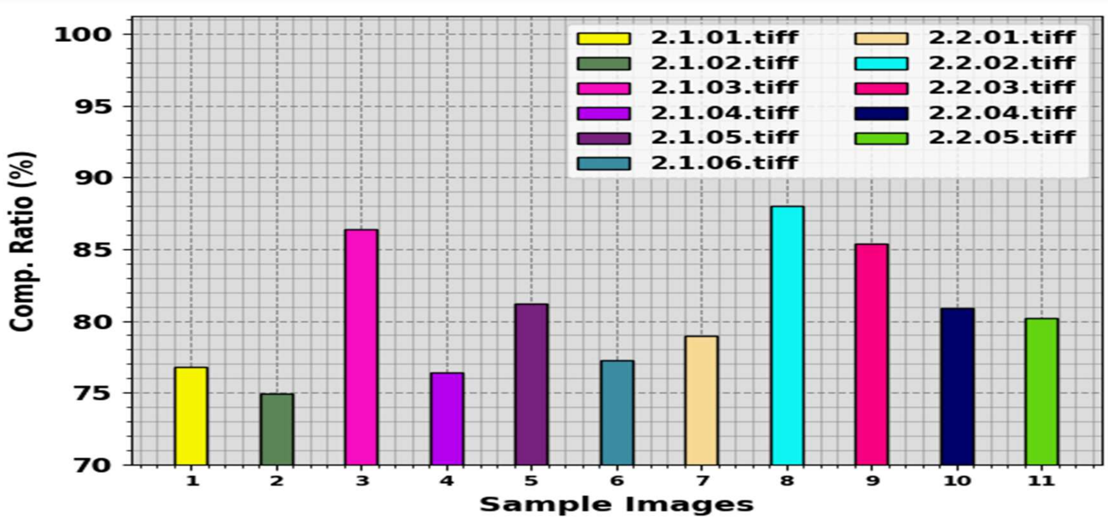

Fig. 10. CR Outcome Of IASEE-DTWSN Technique With Various Sample Images

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

At the same time, on the sample image of 2.1.04.tiff, the IASEE-DTWSN approach offers a higher CR of 76.43%. Meanwhile, on the sample image of 2.1.06.tiff, the IASEE-DTWSN technique reaches a superior CR of 77.29%. Furthermore, on the sample image of 2.2.01.tiff, the IASEE-DTWSN system attains an improved CR of 78.99%. Finally, on the sample image of 2.2.05.tiff, the IASEE-DTWSN methodology accomplishes an enhanced CR of 80.18%.

To further guarantee the compression outcome of the IASEE-DTWSN approach, a brief PS outcome is made in Table 4 and Fig. 11. The outcomes outperformed that the IASEE-DTWSN model managed to obtain reasonable PS values. On the sample image of 2.1.01.tiff, the IASEE-DTWSN method provides an enhanced PS of 97.08%. Simultaneously, on the sample image of 2.1.04.tiff, the IASEE-DTWSN system reaches a superior PS of 97.04%. In the meantime, on the sample image of 2.1.06.tiff, the IASEE-DTWSN approach offers a maximal PS of 97.17%. Furthermore, on the sample image of 2.2.01.tiff, the IASEE-DTWSN technique provides a superior PS of 97.38%. Lastly, on the sample image of 2.2.05.tiff, the IASEE-DTWSN algorithm provides a higher PS of 97.54%.

Table 4 Compression Outcome Of IASEE-DTWSN Technique With Various Sample Images

Sample Images	Original Packet	Comp. Packet	Bits Per Samples	Power Saving (%)
2.1.01.tiff	3390.4	786.55	0.70	97.08
2.1.02.tiff	3390.4	848.83	0.75	96.88
2.1.03.tiff	3390.4	460.14	0.41	98.29
2.1.04.tiff	3390.4	799.03	0.71	97.04
2.1.05.tiff	3390.4	638.48	0.57	97.63
2.1.06.tiff	3390.4	769.93	0.68	97.17
2.2.01.tiff	13559.78	2849.1	0.63	97.38
2.2.02.tiff	13559.78	1619.93	0.36	98.50
2.2.03.tiff	13559.78	1986.69	0.44	98.17
2.2.04.tiff	13559.78	2586.76	0.57	97.63
2.2.05.tiff	13559.78	2688.21	0.59	97.54

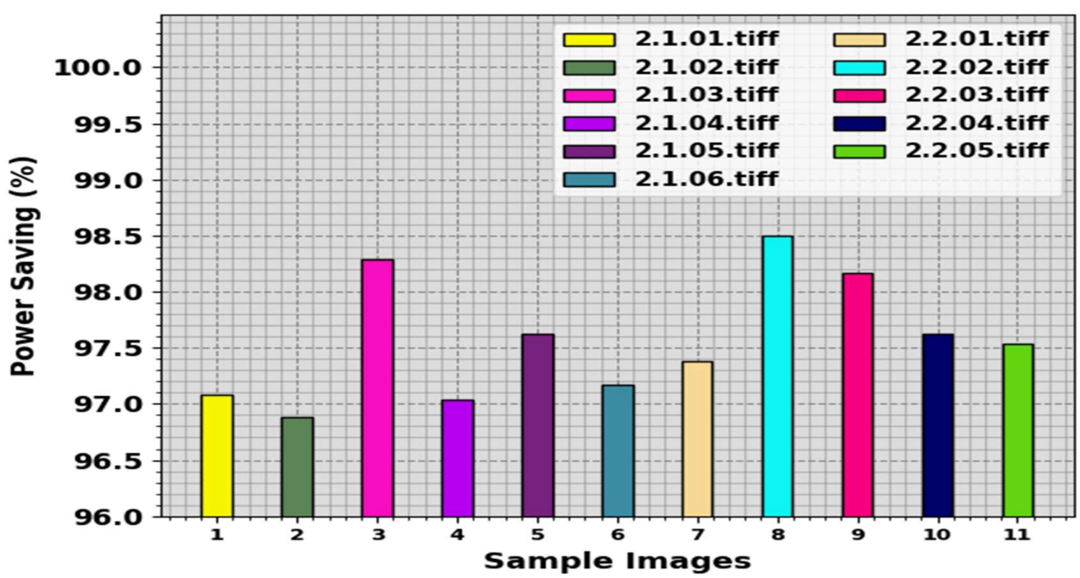

Fig. 11. PS Outcome Of IASEE-DTWSN Technique With Various Sample Images

In Table 5, the overall power saving (PS) results of the IASEE-DTWSN technique are compared with existing models [24]. The results highlighted that the ALDC and S-LZW models have accomplished worse performance with minimal PS values. Along with that, the NIS and FELACS models have obtained closer PS values. Although, the IASEE-DTWSN technique gains better performance over other models with maximum PS values. For instance, on sample image of 2.1.01.tiff, the IASEE-DTWSN technique offers better performance with a higher PS of 97.08% whereas the NIS, FELACS, ALDC, and S-LZW models obtain lower performance with PS of 95.30%, 93.64%, 92.02%, and 90.46%, correspondingly. Therefore, the IASEE-DTWSN technique can be utilized for enhanced energy efficiency in the WMSN

Table 5 PS Analysis Of The IASEE-DTWSN Technique With Existing Methods Under Various Sample Images

Sample Images	**Power Saving (%)**				
	IASEE-DTWSN	**NIS Model**	**FELACS**	**ALDC**	**S-LZW**
2.1.01.tiff	97.08	95.30	93.64	92.02	90.46
2.1.02.tiff	96.88	95.22	93.66	91.86	90.27
2.1.03.tiff	98.29	96.79	95.17	93.54	92.00
2.1.04.tiff	97.04	95.45	93.92	92.21	90.58
2.1.05.tiff	97.63	95.88	94.24	92.58	91.05
2.1.06.tiff	97.17	95.63	93.97	92.22	90.69
2.2.01.tiff	97.38	95.62	93.85	92.25	90.61
2.2.02.tiff	98.50	96.96	95.37	93.85	92.19
2.2.03.tiff	98.17	96.45	94.66	92.88	91.35
2.2.04.tiff	97.63	95.87	94.21	92.67	91.02
2.2.05.tiff	97.54	96.00	94.43	92.92	91.12

5. CONCLUSION

In this manuscript, we have developed a new IASEE-DTWMSN approach. The primary goal of the IASEE-DTWSN method is to ensure security and maximum energy efficiency in WMSN via data compression and encryption algorithms. Initially, the IASEE-DTWSN technique compresses the images captured by WMSN using the DCT approach. Besides, the secure transmission of the compressed data can be accomplished using AES model. Furthermore, the IASEE-DTWSN technique involves the design of MGTO for optimizing the DCT and AES models. The MGTO algorithm is implemented to define the optimum quantization parameters of the DCT and encryption key selection of the AES model, in such a way that the compression ratio and PSNR are maximized. To validate the performance of the IASEE-DTWSN system, a wide range of simulations was involved. The experimental outcomes inferred that the IASEE-DTWSN model resulted in enhanced energy efficiency and security in the WMSN.

Data Availability Statement: The data that support the findings of this study are openly available at https://sipi.usc.edu/database/, reference number [23].

Acknowledgement

The authors would like to express their sincere gratitude to the reviewers and editors for their valuable comments and constructive suggestions, which significantly helped in improving the quality and clarity of this manuscript. The authors also acknowledge the support of their respective institutions for providing the necessary facilities and research environment to carry out this work. Special thanks are extended to the researchers and developers whose publicly available datasets and tools contributed to the experimental evaluation of this study.

REFERENCES

[1] Chakraborty, C., Othman, S.B., Almalki, F.A. and Sakli, H., 2024. FC-SEEDA: Fog computing-based secure and energy efficient data aggregation scheme for Internet of healthcare Things. *Neural Computing and Applications*, *36*(1), pp.241-257.

[2] Saleem, M.M. and Alabady, S.A., 2023. Energy-efficient multipath clustering with load balancing routing protocol for wireless multimedia sensor networks. *IET Wireless Sensor Systems*, *13*(3), pp.104-114.

[3] Devulapalli, P.K., Maganti, S.B., Gae, S.K. and Rachapogula, S., 2022. Optimal Relay

Selection Strategy for Energy-Efficient Cooperative Multi-Hop Image Transmission in Wireless Multimedia Sensor Network. *Cybernetics and Systems*, pp.1-24.

[4] Chandana, M.S., Rao, K.R. and Reddy, B.N.K., 2024. Developing an adaptive active sleep energy efficient method in heterogeneous wireless sensor network. *Multimedia Tools and Applications*, *83*(5), pp.13689-13706.

[5] Vijayalakshmi, S., Kavithaa, G. and Kousik, N.V., 2023. Improving Data Communication of Wireless Sensor Network Using Energy Efficient Adaptive Cluster-Head Selection Algorithm for Secure Routing. *Wireless Personal Communications*, *128*(1), pp.25-42.

[6] Bhatti, D.S., Saleem, S., Ali, Z., Park, T.J., Suh, B., Kamran, A., Buchanan, W.J. and Kim, K.I., 2024. Design and Evaluation of Memory Efficient Data Structure Scheme for Energy Drainage Attacks in Wireless Sensor Networks. *IEEE Access*, *12*, pp.41499-41516.

[7] Tiwari, R. and Kumar, R., 2022, July. A Novel Compression Method for Transmitting Multimedia Data in Wireless Multimedia Sensor Networks. In *Proceedings of Third International Conference on Computing, Communications, and Cyber-Security: IC4S 2021* (pp. 37-47). Singapore: Springer Nature Singapore.

[8] Raghava Rao, K., Naresh Kumar Reddy, B. and Kumar, A.S., 2023. Using advanced distributed energy efficient clustering increasing the network lifetime in wireless sensor networks. *Soft Computing*, *27*(20), pp.15269-15280.

[9] Ibraheem, M.K.I., Al-Abadi, A.A.J., Mohamed, M.B. and Fakhfakh, A., 2024. A Security-Enhanced Energy Conservation with Enhanced Random Forest Classifier for Low Execution Time Framework (S-2EC-ERF) for Wireless Sensor Networks. *Applied Sciences*, *14*(6), p.2244.

[10] Wang, N., Zhang, S., Zhang, Z., Qiao, J., Fu, J., Liu, J. and Bhargava, B.K., 2023. Lightweight and Secure Data Transmission Scheme Against Malicious Nodes in Heterogeneous Wireless Sensor Networks. *IEEE Transactions on Information Forensics and Security*.

[11] Khashan, O.A., Khafajah, N.M., Alomoush, W. and Alshinwan, M., 2024. Innovative energy-efficient proxy Re-encryption for secure data exchange in Wireless sensor networks. *IEEE Access*.

[12] Nagaraju, R., Goyal, S.B., Verma, C., Safirescu, C.O. and Mihaltan, T.C., 2022. Secure routing-based energy optimization for IOT application with heterogeneous wireless sensor networks. *Energies*, *15*(13), p.4777.

[13] Biswas, K., Muthukkumarasamy, V., Chowdhury, M.J.M., Wu, X.W. and Singh, K., 2023. A multipath routing protocol for secure energy efficient communication in Wireless Sensor Networks. *Computer Networks*, *232*, p.109842.

[14] Rani, K. and KN, M., 2024. Enhancing QoS in Wireless Sensor Networks Using Dynamic Energy-Efficient Multimode Transmission with the Network Adaptive Multimode Transmission LEACH Protocol. *International Journal of Computing and Digital Systems*, *16*(1), pp.1-15.

[15] Kethireddy, S.R., Rallapalli, P.V., Chilakala, L.R. and Devulapalli, P.K., 2023. Energy Efficient Cooperative Image Transmission in Multi-Hop Wireless Multi-Media Sensor Networks. *International Journal of Intelligent Engineering & Systems*, *16*(5).

[16] Majeed, U., Malik, A.N., Abbas, N. and Abbass, W., 2022. An energy-efficient distributed congestion control protocol for wireless multimedia sensor networks. *Electronics*, *11*(20), p.3265.

[17] Tabbassum, S. and Pathak, R.K., 2024. Effective data transmission through energy-efficient clus-tering and Fuzzy-Based IDS routing approach in WSNs. *Virtual Reality & Intelligent Hardware*, *6*(1), pp.1-16.

[18] Vimala, D. and Manikandan, K., 2023. PIRAP: Intelligent Hybrid Approach for Secure Data Transmission in Wireless Sensor Networks. *International Journal of Cooperative Information Systems*, *32*(01n02), p.2350002.

[19] Robinson, J. and Kecman, V., 2003. Combining support vector machine learning with the discrete cosine transform in image compression. *IEEE Transactions on Neural Networks*, *14*(4), pp.950-958.

[20] Blömer, J. and Seifert, J.P., 2003. Fault based cryptanalysis of the advanced encryption standard (AES). In *Financial Cryptography: 7th International Conference, FC 2003, Guadeloupe, French West Indies, January 27-30, 2003. Revised Papers 7* (pp. 162-181). Springer Berlin Heidelberg.

[21] You, J., Jia, H., Wu, D., Rao, H., Wen, C., Liu, Q. and Abualigah, L., 2023. Modified Artificial Gorilla Troop Optimization Algorithm for Solving Constrained Engineering Optimization Problems. *Mathematics*, *11*(5), p.1256.
[22] Hassan, M.H., Kamel, S. and Mohamed, A.W., 2024. Enhanced gorilla troops optimizer powered by marine predator algorithm: global optimization and engineering design. *Scientific Reports*, *14*(1), p.7650.
[23] https://sipi.usc.edu/database/
[24] Uthayakumar, J., Vengattaraman, T. and Dhavachelvan, P., 2019. A new lossless neighborhood indexing sequence (NIS) algorithm for data compression in wireless sensor networks. *Ad Hoc Networks*, *83*, pp.149-157.