Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 28 (2025), No. 4-B, pp. 1425–1436
DOI : 10.47974/JDMSC-2288

A hybrid cryptographic and steganography approach for secure IoT data transmission

Ali H. Abdulkhaleq*
Department of Information Technology
Technical College of Management
Al-Furat Al-Awsat Technical University
Najaf
Iraq

Kareem K. Ibrahim †
Ahmed S. Abdulreda §
Department of Computer Education
Najaf Education Directorate
Ministry of Education
Najaf
Iraq

Abstract

Data transmission security has become a critical challenge in the age of the Internet of Things (IoT) because of the increasing threats. To enhance data security in IoT-based environments, this study introduces a hybrid cryptographic and steganographic approach. Unlike cryptography, where data is encrypted to prevent unauthorized access, steganography hides data inside innocuous media. In addition to encrypting sensitive information, the proposed method hides it from potential attackers by combining these technologies. In order to achieve superior security and scalability, a Variable Least Significant Bit (VLSB) Substitution scheme is employed along with advanced cryptographic techniques. Comparing hybrid methods to traditional methods, experimental results demonstrate that the hybrid approach significantly reduces the number of altered pixels during data embedding. Smart IoT environments benefit from this dual-layer strategy by preserving data integrity and confidentiality, making them more resilient and secure.

Subject Classification: *93E10, 94A13.*

Keywords: *IoT security, Hybrid cryptography, Steganography, Data transmission, Variable LSB substitution (VLSB), Smart city infrastructure.*

* *E-mail:* **ahmedfakhir.mo@gmail.com (Corresponding Author)**
† *E-mail:* **karimk.aljabri@student.uokufa.edu.iq**
§ *E-mail:* **ahmeds.albudairi@student.uokufa.edu.iq**

1. Introduction

IoT has increased the need for data transmission security. As IoT devices proliferate, so do cyber threats, making it imperative to develop robust methods of protecting data integrity and confidentiality. An innovative solution involves combining cryptographic techniques with steganography- a hybrid approach that combines the strengths of both to create a stronger defence mechanism. With cryptography, data remains unintelligible to anyone without the decryption key, ensuring information remains safe from unauthorized access. The art of steganography, on the other hand, conceals the existence of the data itself by hiding it within seemingly innocuous carriers. As a result, attackers are unable to detect or decipher sensitive information when these two technologies are combined. It is a general term that refers to situations in which people, devices with wireless recognition, sensors, embedded sensor-based small devices, and everyday objects are connected to a network and can be computed. A two-level data privacy enhancement is achieved by using the methodology above, preventing data privacy loss during IoT data transmission. To ensure data transmission in smart environments is secure, we recommend adopting an integrated strategy combining cryptography and steganography [1]. Cryptography cannot, therefore, conceal encrypted data from prying eyes or attackers. The use of cryptography in conjunction with steganography in IoT can enhance the safety and security of data transmission since the data is completely concealed within a host image. In the proposed security approach, steganography would conceal transmitted information from attackers in the IoT environment, thus improving security [2].

Security of confidential data has become increasingly important in today's era, and steganography has proven to be an effective method for obtaining secure data. [3]. A steganographic technique involves embedding processes to hide secret data in messages, audio, images, and videos [4]. In order to prevent malicious attacks on secret data, it is used [5]. The internet is becoming more and more popular for exchanging data. Data security, therefore, plays a crucial role in Internet data communication. By combining steganography and cryptography, secure information can be provided [6]. Cryptography is used in combination with steganography to enhance data security [7]. In terms of information security, both methods are important [8].

A steganography method usually conceals a secret bit for every pixel in the cover image. The steganography process has introduced different adaptive embedding processes to deal with these issues. Steganography has been modified to address these issues by introducing different adaptive embedding processes. Cover images with adaptive embedding contain a variable number of bits per pixel. Steganography security was therefore improved through these adaptive techniques. Also, the edge pixels are not greatly affected by changes during embedding. Encrypting and hiding information is possible by using cryptography and steganography.

2. Related Work

Scientists must conduct numerous investigations to guarantee the required level of security as a result of this problem. It is possible to solve this problem by combining encryption with hidden techniques. In many studies, it has been recommended that encryption and hidden techniques be combined in one system. These approaches have been defended in previous surveys on the subject. Author [9] provides a comprehensive overview of approaches to integrating cryptography and steganography systems. A combined steganography and cryptographic technique was demonstrated and compared [10].

Additionally, it illustrates how to obscure highly confidential messages to avoid being intercepted. In a colour image, the author [11] proposes encoding critical data at all levels of the RGB colour space using a new method based on how humans perceive colours. For image steganography, [12] proposes a new LSB technique. Two layers of security were applied by the author [13] in order to hide critical data from personal computers.

There is a proposed LSB-based algorithm for image steganography [14]. For data concealment, a common bit pattern is used. The LSBs of pixels are adjusted according to the pattern and message bits. The potential of this method is limited. The vector quantization tables embed hidden secret messages, increasing hidden capacity and stego size as a result [15]. It is possible to encrypt and decrypt a private file using the random LSB implantation technique by distributing secret message bits randomly among image bits [16]. During transmission, secret messages could be protected by combining encrypting and steganography techniques [17]. An additional paper describes a method for embedding secret data at multiple levels using visual cryptography and steganography [18]. Image pixels were minimized by half-toning during the processing step. Through the use of visual cryptography, shares are hidden within various cover images using LSB-based steganography. With the combination of image steganography and cryptography, data can be secured in a variety of ways. Our approach is discussed in this section by carefully examining several methods.

A cryptographic, compression, and steganography method was proposed by the author [19] to protect sensitive text data. Researchers found that combining the methods outperformed using only LSB steganography. It is recommended to combine RSA-Huffman, Run-length encoding, and DWT for high-quality stego-images [20]. According to the experiments, the proposed module was more reliable and storage-capable than other options. As a network of interconnected devices, the Internet of Things (IoT) facilitates seamless data transfer[21]. As a result of IoT devices' limited processing and storage resources, ensuring data security remains a significant challenge. IoT data protection has been improved through hybrid approaches that combine cryptography and steganography techniques[22].

3. Proposed Methodology

3.1. *Image Encryption*

By decomposing a hidden image into eight binary bit planes using the VLSB method, the hidden image can be encrypted [23]. Based on this VLSB method, non-negative decimal numbers D can be represented as $(b_{m-1}, \dots b_1, b_0)$.

$$D = \sum_{j=0}^{m-1} b_j . 2^j = b_0 . 2^0 + b_1 . 2^1 + \cdots b_{m-1} . 2^{m-1} \quad (1)$$

In grayscale images, pixels are numbered from 0 to 255. The diffusion stage is followed by confusion, while the confusion stage is followed by diffusion. In this stage, we generate two binary key streams using. $K_1(y_0, \delta_1)$ and then enter the diffusion and confusion stages.

Piecewise linear chaotic maps (PWLCM) are used to generate the key streams. Here are the definitions of the PWLCM [24]:

$$y_{j+1} = F(y_j, \delta) = \begin{cases} y_j/\delta & y_j \in [0, \delta) \\ (y_j - \delta)/(0.5 - \delta) & y_j \in [\delta, 0.5) \\ F(1 - y_j, \delta & \gamma_j \in (0.5,1) \end{cases} \quad (2)$$

A PWLCM's initial condition is represented by $y_j \in (0, 1)$ and the control parameter is represented by $\delta \in (0, 0.5)$. It is recommended that y_0 and δ_1 be set to their default values when encrypting a Hidden Image with a size of $M \times N$. Using the PWLCM map, the chaotic sequence or keystream $Y = \{y_1, y_2, \dots y_{MN}\}$. is obtained by iteration $M \times N$ times. In order to convert $y(j)$ into $y_1(j)$, the following expressions are used:

$$Y_1 = mod(floor(Y \times 10^{14}), 256) \quad (3)$$

Y is then decomposed into 8-bit planes using VLSB. Following this, it is necessary to group these bit planes into two groups to get binary sequences. k_1 and k_2. As the bits are arranged from left to right in higher bit planes, they form these groups.

3.2. *Diffusion Stage*

The diffusion stage involves the following steps:

1. The elements of P_2 should be added as follows:
$$S_1 = \sum_{j=1}^{4MN} P_2(j) \quad (4)$$
2. Obtain P_{11} by performing cyclic shift operations on P_1. A right shift of S_1 bits is applied to the elements in P_1 of the matrix.
3. P_{11} the first element is encrypted with P_{11}previous element, and P_2 the first element is encrypted with k_1 the first element, as shown below.
$$Q_1(j) = P_{11}(j) \oplus P_{11}(j-1) \oplus P_2(j) \oplus k_1(j) \quad (5)$$
4. The elements Q_1 are listed below. Add them all:
$$S_2 = \sum_{j=1}^{4MN} Q_2(j) \quad (6)$$

5. Calculate P_2 by performing a cyclic shift operation on P_2. A right shift of S_2 bits is applied to the elements in the matrix P_2.
6. P_{22} the first element is encrypted with P_{22}previous element, and P_1 the first element is encrypted with k_2 the first element, as shown below:

$$Q_2(j) = P_{22}(j) \oplus P_{22}(j-1) \oplus Q_1(j) \oplus k_2(j) \tag{7}$$

3.3. *Confusion Stage*

When we are in the stage of confusion, we perform the following steps:

1. As shown below, add all the elements in Q_1 and Q_2

$$S_3 = \sum_{j=1}^{4MN} Q_1(j) + Q_2(j) \tag{8}$$

2. Use $K_2(z_0, \delta_2)$. to generate keystreams Z_1 and Z_2. As a first step, the value a_0 is generated with the following expression

$$a_0 = mod(z_0 + \frac{S_3}{4MN,1)} \tag{9}$$

The generates a random sequence $A = \{a_1, a_2, \ldots a_{2MN}\}$ using $PWLCM\ 2 \times 4MN$.

This results in a two-part sequence:

$$A_1 = \{a_1, a_2, \ldots a_{4MN}\} \tag{10}$$

$$A_2 = \{a_{MN+1}, a_{MN+2}, \ldots a_{4MN} \tag{11}$$

This expression is then used to convert these sequences A_1 and A_2 into integer sequences Z_1 and Z_1.

$$Z_1 = mod(floor(A_1 \times 10^{14}), 4MN) + 1 \tag{12}$$

$$Z_2 = mod(floor(A_2 \times 10^{14}), 4MN) + 1 \tag{13}$$

3. As shown below, swap the elements of Q_1 and Q_2 to obtain the encrypted row vector R_1

$$temp = Q_1(j) \tag{14}$$

$$Q_1(j) = Q_2(Z_1(j) \tag{15}$$

$$Q_2\big(Z_1(j)\big) = temp \tag{16}$$

4. Using Q1 and Q2, swap the elements in Q2 to obtain the encrypted row vector R2:

$$temp = Q_2(j) \tag{17}$$

$$Q_2(j) = Q_1(Z_2(j) \tag{18}$$

$$Q_1\big(Z_2(j)\big) = temp \tag{19}$$

5. A cypher image is obtained by transforming the row vectors R_1 and R_2 into $M \times N$ the image.

3.4. *Salp Swarm Optimization Algorithm (SSOA) Based Adaptive Embedding*

Image cover pixels range from 0 to 255. A steganography embedding function establishes different parameter values for smooth and edge regions to embed the secret image data. An objective function derived from SSOA [25] is

used to obtain smooth and edge pixels for the embedding process (l1−norm) [26]. Objective functions represent edges as maximum values. The secret bit values are encoded in the cover image via steganography embedding. It will be different in this process if you have edges or smooth areas. After obtaining the stego-image, we can proceed to the next step.

3.4.1. Edge/Smooth Block Localization

In this paper, an SSOA algorithm is proposed for localizing edges and smooth pixels in the cover image by optimizing the objective function (Manhattan Distance operator (l2−norm)). SSOA mimics the natural swarming behaviour of salps by using population-based optimization. Individuals begin the SSOA by being randomly initialized. Leaders and followers make up the swarm of Salps.

The edge/smooth block is localized by distributing m Salps randomly on an image of size $M \times N$. A 2-D representation of the swarm of m salps can be seen in (20). This swarm is looking for the optimal threshold (i.e., food source) in the search space named T. For edge detection to be optimal, we must determine each agent's fitness following population initialization, as in (20). In this case, the l1−norm is calculated by each salp in the SSOA. Manhattan Distances are calculated from the centre pixel r to all 8 neighbours in the pixel at (i, j) of cover image C to detect salps.

$$S_i = \begin{bmatrix} S_1^1 & S_2^1 & \cdots & S_n^1 \\ S_1^2 & S_2^2 & \cdots & S_n^2 \\ \cdots & \vdots & \vdots & \vdots \\ S_1^m & S_2^m & \cdots & S_n^m \end{bmatrix} \tag{20}$$

Edge pixels are determined by calculating the discrete derivatives of adjacent pixels. When the objective function reaches its maximum value, there is a greater chance that edges will occur.

$$\begin{aligned} f = &\left|C_{(i-1),(j-1)} - r\right| + \left|C_{(i-1,j)} - r\right| + \left|C_{i-1,j+1} - r\right| + \left|C_{(i,j-1)} - r\right| \\ &+ \left|C_{i(,j+1)} - r\right| + \left|C_{(i,j+1)} - r\right| + \left|C_{(i+1,j+1)} - r\right| \\ &+ \left|\, C_{(i+1,j)} - r\right| + \left|\, C_{(i+1,j+1)} - r\right| \end{aligned} \tag{21}$$

With the operator$|\cdot|$, absolute values are obtained, while r represents the position (i, j) within the cover image C where the latest salp appears.

In the best search agent competition, salps are ranked based on their fitness. According to SSOA, the leader particle's location is computed as follows:

$$S_j^1 = \begin{cases} T_j + \varepsilon_1 \left(\left(B_U^j - B_L^j\right)\varepsilon_2 + B_L^j \right) & \varepsilon_3 \geq 0.5 \\ T_j - \varepsilon_1 \left(\left(B_U^j - B_L^j\right)\varepsilon_2 + B_L^j \right) & \varepsilon_3 < 0.5 \end{cases} \tag{22}$$

Position vectorsS_j^1 and T_j represent the leader and food source, respectively. B_U^j and B_L^j represent upper- and lower-bounds.

Random values between 0 and 1 are ε_2 and ε_3. The important parameter ε1 can be calculated using the expression below

$$\varepsilon_1 = 2e^{-\left(\frac{4n}{N_max}\right)^2} \tag{23}$$

An iteration value of n indicates the current number, while an iteration value of n and N_{max} indicates the maximum.

A follower's position is then updated by SSOA based on

$$S_j^1 = 0.5 \times \left(S_j^i + S_j^{i-1}\right) \tag{24}$$

i^{th} follower's position in i^{th} dimension is represented by S_j^1. SSOA initiates all salps at random. All salps are evaluated in order to select the salp with the best objective function. Equations (22) and (24) are used to update leader and follower position vectors. Meanwhile, we update the parameter ε_1 using (23). It is necessary to repeat these processes until a threshold is reached for edge detection.

Using $g = (g_1, g_2, \ldots g_k)$ as the grey value, the edges/smooth pixels in the cover image are divided into nonoverlapping k-pixel blocks.

In addition to determining whether a block is smooth or edge, edge pixels can be used to determine whether it is edge or smooth.

$$class = \begin{cases} edgeblock & if\ N_e > N_s \\ smoothblock & if\ N_e < N_s \end{cases} \tag{25}$$

A number of edge pixels are represented by N_e, while several smooth pixels are represented by N_s.

3.4.2. Embedding Process

Steganography embedding functions are implemented in two different ways in the proposed method. A smooth block uses parameters ρl and $b_s = 1 + \sum_{j=1}^{k} \binom{k}{j}\binom{\rho l}{j} \times 2^j$ with low values. Edge blocks can also use high values of ρh and $be = 1 + \sum_{j=1}^{k} \binom{k}{j}\binom{\rho h}{j} \times 2^j$. Following is a detailed description of how each k-pixel block is embedded:

1. Create a steganography embedding function by multiplying $F(g) = ag^T$ mod b_1 by smooth block $b_1 = b_e$ and $\rho_1 = \rho_h$ edge bloc, respectively. Too, $A = (a_1, a_2, \ldots . a_k), a_j = \left(2_{\rho 1} + 1\right)^{j-1}$.
2. Using the secret image, compute $= mod(s, b_1)$ and $d = u - F(g) mod\ b_1$, where s represents the encrypted bit values. A block of k pixels is unchanged when d=0. Once $(s - u)/b_1$ is substituted for secret value s, the pixel values of the next k pixels are modified. The next step will be taken if $d > 0$.
3. $F(v) = d$ and $||v|| \leq \rho$ determines the vector v.

4. Calculate $g' = (g_1', g_2', \dots g_k')$ by means of $g' = g + v$ then $g' = (g_1', g_2', \dots g_k')$ is attuned to $g'' = (g_1'', g_2'', \dots g_k'')$Overflow/underflow problems for stego-pixel values:

$$g" = \begin{cases} g' - b_1 & g' > 255 \\ g' + b_1 & g' < 0 \\ g' & 0 \geq g' \leq 255 \end{cases} \quad (26)$$

5. Assess whether block $g'' = (g_1'', g_2'', \dots g_k'')$ belongs to a smooth block or an edge block using the optimal threshold value developed by the proposed edge localization algorithm.

4. Result and Discussion

A comparison of variables LSB substitution and simple LSB substitution is shown in Figure 1. There are generally fewer pixel changes when using Variable LSB Substitution than Simple LSB Substitution, both on average and in the case of a best-case scenario.

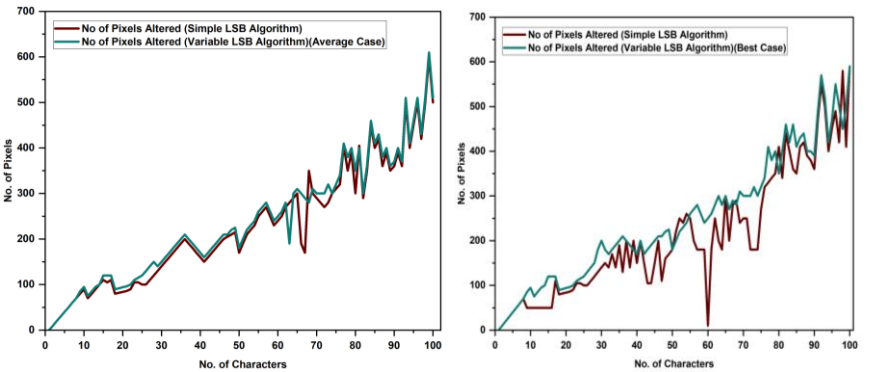

Figure 1

No. of Pixels versus no of characters in terms of (a) Avg. Case and (b) Best Case.

An example of pixel mapping for either Simple LSB substitution or Variable LSB substitution is shown in Figure 2. In .bmp images, the first 50 pixels contain all the necessary image metadata, so the Simple LSB Substitution scheme embeds data sequentially from pixel 50 onwards. It is relatively easy to attack this scheme due to its sequential approach. For enhanced security, Variable LSB Substitution targets cover image pixels randomly. In this method, random selection is performed based on hash-mapped pixel values, providing a much higher level of security than previous methods.

5. Conclusion

IoT-based smart city networks can benefit from hybrid cryptography and steganography for secure data transmission. Through both encryption and invisibility, the method enhances data security by combining cryptography and steganography. Experiments confirm that the Variable LSB Substitution scheme

outperforms traditional Simple LSB methods, showing fewer pixel alterations. Despite intercepting encrypted data, the concealed nature within the carrier media provides an additional barrier against unauthorized access, even when encrypted data is intercepted. Performance and image quality are further optimized by integrating advanced SSOA optimization. This study advances secure communication protocols for smart city infrastructures by addressing critical challenges related to data privacy, security, and scalability.

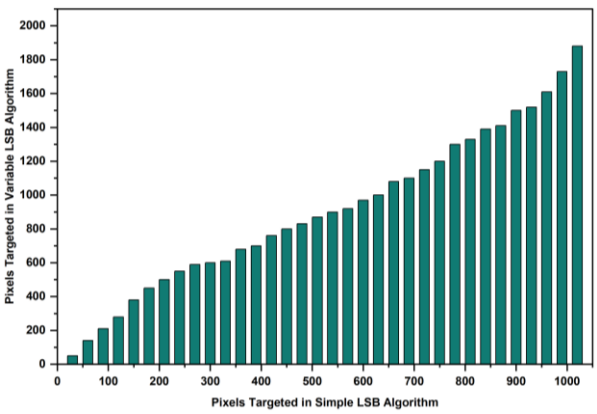

Figure 2
Pixels targeted in variable LSB versus simple LSB algorithm.

References

[1] S. Pramanik, "An adaptive image steganography approach depending on integer wavelet transform and genetic algorithm," *Multimed Tools Appl,* vol. 82, no. 22, pp. 34287–34319 (Sep. 2023), doi: 10.1007/s11042-023-14505-y.

[2] S. K. Bandyopadhyay, V. Goyal, S. Dutta, S. Pramanik, and H. H. R. Sherazi, "Unseen to Seen by Digital Steganography: Modern-Day Data-Hiding Techniques," in Advances in Information Security, Privacy, and Ethics, S. Pramanik, M. M. Ghonge, R. V. Ravi, and K. Cengiz, Eds., IGI Global, pp. 1–28 (2021). doi: 10.4018/978-1-7998-7160-6.ch001.

[3] M. E. Saleh, A. A. Aly, and F. A. Omara, "Data security using cryptography and steganography techniques," *International Journal of Advanced Computer Science and Applications*, vol. 7, no. 6, 2016, Accessed:

Feb. 23 (2025). [Online]. Available: https://pdfs.semanticscholar.org/2f3f/cc1d74787ee194316225333e354d566aa309.pdf

[4] P. Rani, S. Verma, S. P. Yadav, B. K. Rai, M. S. Naruka, and D. Kumar, "Simulation of the lightweight blockchain technique based on privacy and security for healthcare data for the cloud system," *International Journal of E-Health and Medical Communications* (IJEHMC), vol. 13, no. 4, pp. 1–15 (2022).

[5] P. Singh, "A comparative study of audio steganography techniques," *International Research Journal of Engineering and Technology* (IRJET), vol. 3, no. 4, pp. 580–585 (2016).

[6] N. Rashmi and K. Jyothi, "An improved method for reversible data hiding steganography combined with cryptography," in 2018 2nd International Conference on Inventive Systems and Control (ICISC), Coimbatore: IEEE, pp. 81–84 (Jan. 2018). doi: 10.1109/ICISC.2018.8398946.

[7] S. Bukhari, M. S. Arif, M. R. Anjum, and S. Dilbar, "Enhancing security of images by Steganography and Cryptography techniques," in 2016 Sixth International Conference on Innovative Computing Technology (INTECH), Dublin, Ireland: IEEE, pp. 531–534 (Aug. 2016). doi: 10.1109/INTECH.2016.7845050.

[8] M. Khari, A. K. Garg, A. H. Gandomi, R. Gupta, R. Patan, and B. Balusamy, "Securing Data in Internet of Things (IoT) Using Cryptography and Steganography Techniques," *IEEE Trans. Syst. Man Cybern, Syst.*, vol. 50, no. 1, pp. 73–80 (Jan. 2020), doi: 10.1109/TSMC.2019.2903785.

[9] Md. Khalid, K. Arora, and N. Pal, "A Crypto-Steganography: A Survey," *ijacsa*, vol. 5, no. 7 (2014), doi: 10.14569/IJACSA.2014.050722.

[10] H. Sharma, K. K. Sharma, and S. Chauhan, "Steganography techniques using cryptography-a review paper," *International Journal of Recent Research Aspects*, pp. 106–108 (2015).

[11] Q. Xie, J. Xie, and Y. Xiao, "A High Capacity Information Hiding Algorithm in Color Image," in 2010 2nd International Conference on E-business and Information System Security, Wuhan, China: IEEE, pp. 1–4 (May 2010). doi: 10.1109/EBISS.2010.5473583.

[12] S. Gupta, G. Gujral, and N. Aggarwal, "Enhanced least significant bit algorithm for image steganography," *IJCEM International Journal of Computational Engineering & Management,* vol. 15, no. 4, pp. 40–42 (2012).

[13] N. A. Al-Otaibi and A. A. Gutub, "2-leyer security system for hiding sensitive text data on personal computers," *Lecture Notes on Information Theory*, vol. 2, no. 2, pp. 151–157 (2014).

[14] S. Channalli and A. Jadhav, "Steganography An Art of Hiding Data," (2009), doi: 10.48550/ARXIV.0912.2319.

[15] P. Rani and M. H. Falaah, "Real-Time Congestion Control and Load Optimization in Cloud-MANETs Using Predictive Algorithms," *NJF Intelligent Engineering Journal*, vol. 1, no. 1, pp. 66–76 (2024).

[16] M. S. Sutaone and M. V. Khandare, "Image based steganography using LSB insertion technique," in 2008 IET International Conference on Wireless, Mobile and Multimedia Networks, IET, 2008, pp. 146–151. Accessed: Feb. 23 (2025). [Online]. Available: https://ieeexplore.ieee.org/abstract/document/4470096/

[17] B. Karthikeyan, A. C. Kosaraju, and Sudeep Gupta S, "Enhanced security in steganography using encryption and Quick Response code," in 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), Chennai, India: IEEE, pp. 2308–2312 (Mar. 2016). doi: 10.1109/WiSPNET.2016.7566554.

[18] S. S. Patil and S. Goud, "Enhanced Multi Level Secret Data Hiding," in An International Conference, 2016. Accessed: Feb. 23 (2025). [Online]. Available: https://www.academia.edu/download/45822001/1164.pdf

[19] J. C. T. Arroyo, "An Improved Image Steganography through Least Significant Bit Embedding Technique with Data Encryption and Compression Using Polybius Cipher and Huffman Coding Algorithm," IJATCSE, vol. 9, no. 3, pp. 3376–3383 (Jun. 2020), doi: 10.30534/ijatcse/2020/137932020.

[20] O. F. A. Wahab, A. A. M. Khalaf, A. I. Hussein, and H. F. A. Hamed, "Hiding Data Using Efficient Combination of RSA Cryptography,

and Compression Steganography Techniques," *IEEE Access,* vol. 9, pp. 31805–31815 (2021), doi: 10.1109/ACCESS.2021.3060317.

[21] B. Bhola et al., "Quality-enabled decentralized dynamic IoT platform with scalable resources integration," *IET Communications* (2022).

[22] P. Rani, P. N. Singh, S. Verma, N. Ali, P. K. Shukla, and M. Alhassan, "An implementation of modified blowfish technique with honey bee behavior optimization for load balancing in cloud system environment," *Wireless Communications and Mobile Computing*, vol. 2022, pp. 1–14 (2022).

[23] Y. Zhou, W. Cao, and C. P. Chen, "Image encryption using binary bitplane," *Signal processing*, vol. 100, pp. 197–207 (2014).

[24] M. Jain, R. C. Choudhary, and A. Kumar, "Secure medical image steganography with RSA cryptography using decision tree," in 2016 2nd international conference on contemporary computing and informatics (IC3I), IEEE, 2016, pp. 291–295. Accessed: Feb. 27 (2025). [Online]. Available: https://ieeexplore.ieee.org/abstract/document/7917977/

[25] S. Mirjalili, A. H. Gandomi, S. Z. Mirjalili, S. Saremi, H. Faris, and S. M. Mirjalili, "Salp Swarm Algorithm: A bio-inspired optimizer for engineering design problems," Advances in Engineering Software, vol. 114, pp. 163–191 (Dec. 2017), doi: 10.1016/j.advengsoft.2017.07.002.

[26] P. Rani and R. Sharma, "IMFOCA-IOV: Intelligent Moth Flame Optimization based Clustering Algorithm for Internet of Vehicle," in 2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT), *IEEE*, pp. 1–6 (2023).

Received February, 2025