

Seagull Optimization Algorithm with Share Creation with an Image Encryption Scheme for Secure Vehicular Ad Hoc Networks

Ravichandran Mohan

Department of Computer Science and Engineering, Annamalai University, India
rkmmails@gmail.com (corresponding author)

Ganesan Prabakaran

Department of Computer Science and Engineering, Annamalai University, India
aucse@yahoo.com

Thirugnanasambandham Priyadarshikadevi

Department of Computer Science and Engineering, Mailam Engineering College, India
hodcse@mailamengg.com

Received: 20 December 2023 | Revised: 5 January 2024 | Accepted: 10 January 2024

Licensed under a CC-BY 4.0 license | Copyright (c) by the authors | DOI: <https://doi.org/10.48084/etasr.6786>

ABSTRACT

A Vehicular Ad hoc Network (VANET) allows transmission, amid moving or stationary vehicles via wireless technology. Amongst several problems, safe transmission is the most important one in smart VANETs in 5G networks. Smart vehicles require integration with advanced road systems encompassing smart payment and traffic control systems. Numerous security mechanisms are used in VANETs to ensure safe communication. One such mechanism is cryptographic digital signatures based on encryption. This study introduces the new seagull optimization algorithm involving share creation with an image encryption scheme (SGOA-SCIES) for secure VANET transmissions. The goal of the SGOA-SCIES technique is to create a considerable number of shares and encrypt them to accomplish security. In the SGOA-SCIES technique, a Multiple Share Creation (MSC) scheme is employed to generate numerous share sets. For the share encryption process, the SGOA-SCIES technique engages the Fractional-Order Chaotic System (FOCS) approach to encrypt the generated shares. The optimal keys of the FOCS method can be chosen by the SGOA usage, which ameliorates the security level. The performance evaluation of the SGOA-SCIES method is examined on benchmark data. The simulations demonstrate the enhanced SGOA-SCIES methodology outcome and compare it with the ones of other existing systems and under the implementation of various measures.

Keywords-security; vehicular ad-hoc network; encryption; key generation; share creation

I. INTRODUCTION

VANETs are considered a developing concept that allows dependable, infotainment-rich, and safe driving networking [1]. However, service providers, automobile manufacturers, and governments are still hesitant to employ VANETs due to certain difficulties generated during their usage, namely user options, requirements for infrastructure, cost, security and safety problems [2]. In the past, the automotive industry concentrated on in-car technology for upgrading entertainment and navigation systems. However, currently the research community engaged special focus of their studies on VANETs due to the increased computation, processing, and computational capacity of the higher-end vehicles [3]. These capacities allowed the evolution of V2I (vehicle-to-infrastructure) and V2V (vehicle-to-vehicle) transmission [4].

These transmission models may provide customers with protection and infotainment applications instead of only offering them particular applications, like a challenged endpoint, which could for instance be a friend's home or a restaurant in another city [5].

Various safety challenges are considered for providing information security defence in vehicular networks, among which, access control and data privacy are highly significant [6]. Data confidentiality confirms that the former cannot be revealed or leaked to unauthorized vehicles or nodes. For providing data integrity and confidentiality in VANET communication, encryption is employed to enable only authenticated users to acquire the transmitted information [7]. Conventional symmetrical data encryption could be a result, yet it requires communication expenses for establishing

authentication keys among data recipients and senders that prominently decrease the time consumed for accessing the resources. An alternate intuitive solution is to encrypt every piece of information with the receiver vehicle's public key and indicate the data prior to their transmission [8]. Given that data are generally transferred to numerous vehicles, there are several data ciphertexts by these standard encryption methods that fail to achieve real-time conditions of data distribution in vehicular applications [9]. This problem can be tremendously severe on the environments of security application's accurate timing limits. Besides that, access control maintenance is a massively unresolved issue, especially, in cases where there is no centralized access control for disseminating the encrypted data in extremely dynamic surroundings [10].

II. RELATED WORKS

Authors in [11] developed the fully homomorphic encryption with the optimum key generation secure group communication (FHEOKG-SGC) system. Initially, this method presents an FHE-based encoding system and later the keys in the FHE technique are effectively selected via SCA. Simultaneously, the plum tree model can be exploited for detecting routes. In [12], a dual-channel encryption technique is designed. Firstly, a chaotic map controls the preliminary value of 5D conservative chaotic systems. Then, a chaotic sequence is exploited as convolution kernels of CNN for generating plaintext correlated chaotic pointers. An image fusion technique, which fuses and splits images into two parts, is proposed. Authors in [13] designed the EPO-based Routing Protocol (EPORP) for an outbreak detection in Sybil. The Sybil attack is discovered through the rumour riding method. The Split XOR (SXOR) operator is implemented for optimizing VANET safety. The optimum keys are carefully selected through the EPO technique. Authors in [14] developed an image encryption technique by joining chaotic maps and Josephus problems. The entire encryption procedure implements the traditional permutation–diffusion model. During permutation, the double-chaotic cycle technique is devised by upgrading the chaotic shift transformation technique. During diffusion, the Josephus problem description is prolonged through chaotic maps to retain the Josephus sequence diversity. In [15], a 7D hyperchaotic map produces the secret key for image encryption. A minimax DE model provides the ideal parameter for the hyperchaotic maps. The parameter fitness is assessed by the entropy and correlation coefficient. Then, the secret key is generated by the hyperchaotic maps. This key performs the diffusion process on the input image and produces an encrypted image. Authors in [16] put forward adaptive safety-aware lottery-EDF schedulers for constrained resources packet switching of Ethernet network with the GAIA multi-agent method. This scheme employs periodic, non-shared cryptographic key generation operations of varying sizes based on textual features in digital images stored on the server.

Authors in [17] introduced a chaotic cryptographic-based privacy safeguarding method to increase privacy in MANET-IoT. The key-generating operation in chaotic mapping can be enhanced by producing the optimum key pair via the recently established SA-SFO method. The key nominated from the

chaotic maps can be impacted by choosing the optimum parameter via SA-SFO. Authors in [18] propose BDIE-AOFOLS, a blockchain-based image encryption method utilizing an arithmetical optimization algorithm with a fractional-order Lorenz system, optimizing key generation for the highest PSNR values. In [19], an energy-efficient ROACM protocol is introduced for ad hoc wireless networks, incorporating path discovery, metric-based selection, and optimal bandwidth allocation via a seagull optimization algorithm. The summary covers various encryption methods, including fully homomorphic encryption, dual-channel encryption, adaptive lottery-EDF schedulers, blockchain-based image encryption, and the mentioned ROACM protocol.

III. THE PROPOSED MODEL

In the presented study, the SGOA-SCIES method is suggested for the share encryption in VANETs, in an attempt to produce numerous shares and encrypt them for enhanced security. It comprises three operation stages: MSC, FOCS-based share encryption, and SGOA-based key generation. Figure 1 shows the workflow of the SGOA-SCIES system.

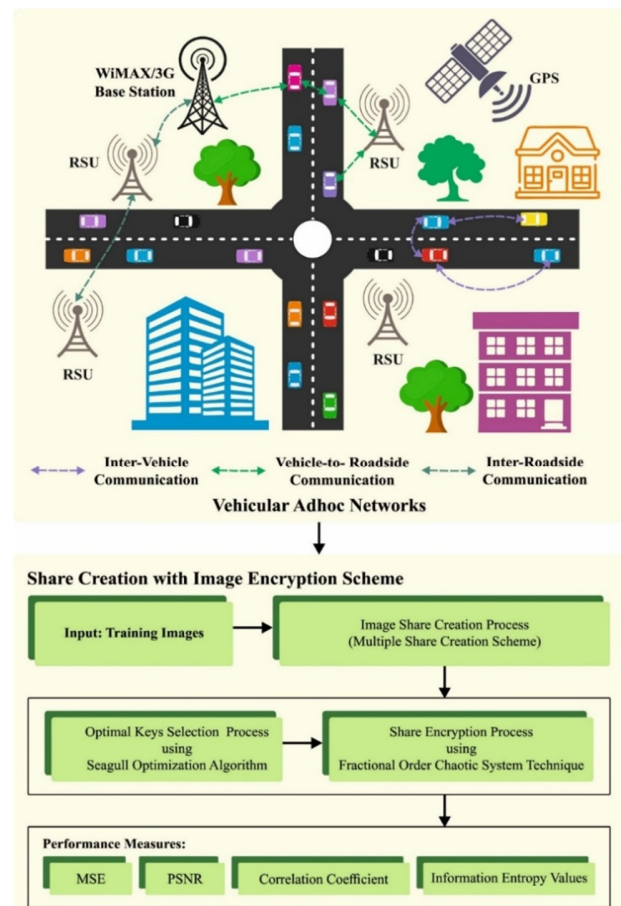


Fig. 1. Workflow of the SGOA-SCIES method.

A. Share Creation Procedure

Here, the MSC is enforced for producing a share collection. The RGB values are respectively determined in the matrix form

(R_m, G_m, B_m) and the extraction of actual image pixel value is conducted [20]. The matrix size is the same as the input image $(P * Q)$ and are described as:

$$\text{Pixel} = \sum R + G + B \quad (1)$$

Pixel depicts the overall amount of $R_m, G_m,$ and B_m values.

B. Share Creation

Each pixel that exists in the input images can be expressed by n transformed means, called shares. Each share includes sub-pixels of the RGB images. Based on the pixel value, the $R, G,$ and B shares exist in the RGB images and are characterized as $R_s, G_s,$ and B_s as follows:

$$R_s = \int_1^k \lim_{k \rightarrow 1 \text{ ton}} R_{ab} \quad (2)$$

$$G_s = \int_1^k \lim_{k \rightarrow 1 \text{ ton}} G_{ab} \quad (3)$$

$$B_s = \int_1^k \lim_{k \rightarrow 1 \text{ ton}} B_{ab} \quad (4)$$

where a and b show the matrix location, $R_s, G_s,$ and B_s symbolize the share of RGB and $R_{ab}, G_{ab},$ and B_{ab} indicate the image pixel component. The pixel value of RGB is taken from the original images and retained as an individual matrix. Then, the share is created based on the splitting of images into different parts. The objective of SMSC is to encrypt the images into an amount of insignificant shared imaging. The shares do not define any valuable data if the share is collectively incorporated.

The elementary matrices should be derived before share creation, based on the amount of shares to be generated that are predefined by the user. The matrix is obtained if the outputs of RGB in the pixels are partitioned by S . In general, the block size is found to be 4×4 or 8×8 . Also, an arbitrary key is provided by the input imaging block size. The amount of share is described as 2^S if $S \geq 2$. Later, the shares are derived by carrying out the XOR operation of the basic matrix on different combinations. In such cases, the share and matrix counts are 4 and 2. By splitting the RGB values of the pixel by 2, the matrix is derived. For instance, assume the block is of size 2×2 , the RGB value is defined. Then, the key matrix K_M is arbitrarily produced. The basic matrix is formulated by the aforementioned process and is characterized by B_{M1} and B_{M2} correspondingly. Before share creation, the succeeding process is conducted with the XR_1 and XR_2 matrices.

$$XR_1 = 128 - B_{M1} \quad (5)$$

$$XR_2 = B_{M2} \quad (6)$$

The red band share is formed by XORing both matrices:

$$Rs1 = XR_1 \oplus K_M \quad (7)$$

$$Rs2 = XR_2 \oplus XR_1 \quad (8)$$

$$Rs3 = XR_2 \oplus Rs1 \quad (9)$$

$$Rs4 = Rs1 \oplus R \quad (10)$$

$$\begin{cases} s_1 = (x_t(300) \times 100 - \text{floor}(x_t(300) \times 100)) \times 10^6 \text{ mod } m \\ s_2 = (x_t(500) \times 100 - \text{floor}(x_t(500) \times 100)) \times 10^6 \text{ mod } m \end{cases} \quad (17)$$

The abovementioned process is reiterated for the remaining green and blue bands to produce various shares.

C. Share Reconstruction

Various shares are merged to form the actual images in the share reconstruction process.

$$R = Rs1 \oplus Rs2 \oplus Rs3 \oplus Rs4 \oplus K_M \quad (11)$$

$$G = Gs1 \oplus Gs2 \oplus Gs3 \oplus Gs4 \oplus K_M \quad (12)$$

$$B = Bs1 \oplus Bs2 \oplus Bs3 \oplus Bs4 \oplus K_M \quad (13)$$

Encryption and decryption by applying the FOCS technique are employed on every colour band when the share is reconstructed. Before the encryption and decryption processes, the colour band images are split into various blocks. The blocks are divided into the 4×4 dimension. Various shares are produced and the encryption technique is exploited. Then the FOCS-based encryption technique is exploited on the shares.

D. Share Encryption using the FOCS Technique

FOCS approach is used to encrypt the shares. A color image encryption model is introduced using FOCS by combining 3 chaotic models (Fractional Lorenz System (FLS), Tent Map (TM), and Arnold Map (AM)) [21]. At first, the color plain image was divided into $R, B,$ and G layers. Then, 3 layers are scrambled with AM, where the key and R and G layers are the initial value of the former, and other 2 are scrambling. The gray values of RGB are moulded and employed as an initial value of FLS. Then, add-mode diffusing is implemented. Lastly, the encrypted images are obtained. The pixel matrix size is $M \times M \times 3$, the plain images are signified as $A,$ and the encryption process can be defined as follows:

Step 1: Enter P plain images and K keys, and assume the size of A is $M \times M \times 3$. Read the primary values and parameters of AM in K and exploit AM to scramble the plain images. Select the last 2 pixels of R layers, attain the gray values as AM parameter while scrambling the G layer, and employ the function which is same as scrambling B layer to get image P_1 .

$$P_1 = \begin{Bmatrix} R \\ G \\ B \end{Bmatrix} = \begin{Bmatrix} r(1), r(2), r(3), \dots, r(m) \\ g(1), g(2), g(3), \dots, g(m) \\ b(1), b(2), b(3), \dots, b(m) \end{Bmatrix} \quad (14)$$

$$m = \text{MIN} \quad (15)$$

Step 2: Read the initial values of TM $X(0)$ from key K . The TM is repeated 800 times. The first 300 conversion conditions are rejected and takes of the state values are represented as K_r .

$$K_\zeta = [x_t(200), x_t(300), x_t(400), x_t(500)] \quad (16)$$

Step3: Use (17) to make the K_ζ into s_1 and s_2 coordinates to place the pixels in P_1 . The FLS is repeated MIV and $2MN$ times, with smaller model perturbation repeated every 3000 times. This repetition occurs to attain the dimension of $3 \times MIV$ and $3 \times 2MIV$ of the new pseudo-random sequence S_1 and S_2 that are transformed (18) to password K_1 and K_2 .

$$K_o = \begin{bmatrix} K_{o1} \\ K_{o2} \end{bmatrix} = \begin{bmatrix} R_{s1}, G_s, B_{s1} \\ R_{s2}, G_{s2}, B_{s2} \end{bmatrix} \quad (18)$$

$$\begin{cases} K_1(j) = (\text{floor}(S_1(j) \times 2^{16}) \text{mod} 256) + 1 \\ K_2(j) = (\text{floor}(S_2(j) \times 2^{16}) \text{mod} 256) + 1 \end{cases} \quad (19)$$

Step4: The password K_1 to transfer the information between the layers of images is used. It is calculated as:

$$\begin{cases} r'(i) = r(i) \oplus k_1(1,i) \oplus b(i) \\ g'(i) = g(i) \oplus k_1(2,i) \oplus r(i), i = 1,2, \dots, MIN \\ b'(i) = b(i) \oplus k_1(3,i) \oplus g'(i) \end{cases} \quad (20)$$

where $r'(i)$, $g'(i)$, and $b'(i)$ show the pixel value after diffusing. Then the pixel, which addresses to the plain data of each layer, is diffused into other 2 layers. This enhances the ability to resist the selected-plain attack.

E. Optimal Key Generation by Utilizing SGOA

At the final stage, the SGOA is applied to produce an optimal set of keys for the FOCS approach. The SGOA is based on the inspiration of the movement pattern and on the attacking prey strategies of the seagulls [22]. To define the location of a new search agent (\vec{F}_s), collision avoidance between search agents in SOA is achieved using the second parameter N .

$$\vec{F}_s = N_x \vec{D}_s(t) \quad (21)$$

In (7), \vec{D}_s , denotes the current seagull location and the existing iteration. The collision avoidance parameter N is modelled as follows:

$$N = E_c - \left(t * \left(\frac{E_c}{Max.Iter} \right) \right) \quad (22)$$

For this, the value of 2 is selected to control the changes in the variable that linearly dropped from E_c to 0. The search agent makes an effort to move close to the position of the ideal individual using (23):

$$\vec{M}_s = A_x (\vec{P}_{bs}(t) - \vec{D}_s(t)) \quad (23)$$

The parameter A is randomized to attain the equilibrium tendency between the exploitation and exploration phases, and is computed by:

$$A = 2 * N^2 * rand() \quad (24)$$

The subsequent changes were made to each location of the search agents:

$$\vec{R}_s = [\vec{F}_s + \vec{M}_s] \quad (25)$$

During their migration, seagulls often change their attacking angle and speed. These behaviors in 3D are defined through the following equations:

$$S' = r * \cos(j) \quad (26)$$

$$T' = r * \sin(j) \quad (27)$$

$$U' = r * j \quad (28)$$

where r refers to the radius of seagulls' spiral movement and the random number selected within $[0, 2]$. The SGOA







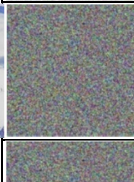
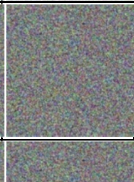
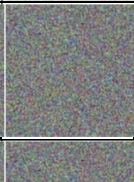
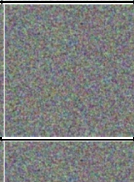


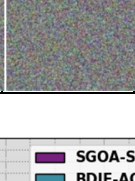

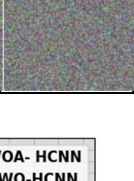
technique is applied in initializing the public and secret keys included in the encryption process. The fitness function of SGO for the FOLS method is given by:

$$Fitness\ function = \max \{PSNR\} \quad (29)$$

IV. RESULTS AND DISCUSSION

This segment inspects the outputs of the SGOA-SCIES approach on 5 test images. Table I portrays a sample visualization of multiple shares generated by the SGOA-SCIES technique on the applied test imaging. The findings suggest that the shares do not convey any significant information pertaining to the original image. The suggested model is simulated by employing Python 3.6.5 tool on PC i5-8600k, 250GB SSD, GeForce 1050Ti 4GB, 16GB RAM, and 1TB HDD. The parameter settings are provided as: learning rate: 0.01, activation: ReLU, epoch count: 50, dropout: 0.5, and batch size: 5. In Figure 2, the outputs indicate that the SGOA-SCIES technique obtains the least MSE values on all images. On IMG-1, the SGOA-SCIES technique obtains decreased MSE of 0.051, while the BDIE-AOFOLS, SSO-HCNN, WOA-HCNN, and GWO-HCNN models obtain improved MSE of 0.0590, 0.0636, 0.1850, and 0.2875, respectively.

TABLE I. VISUALIZATION OF THE MSC SCHEME

Original Image	1 - Share	2 - Share	3 - Share	4 - Share
				
				
				

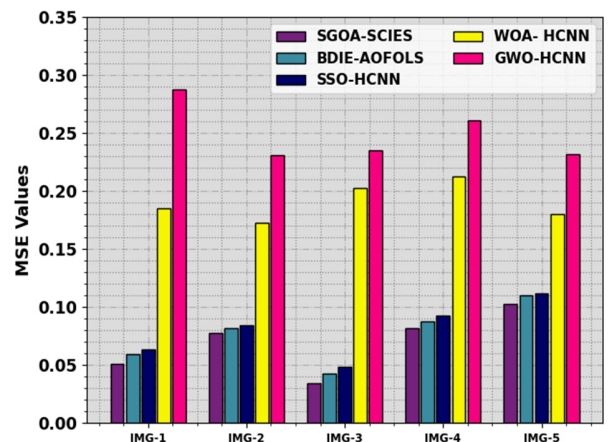


Fig. 2. MSE outcome of SGOA-SCIES under distinct test images.

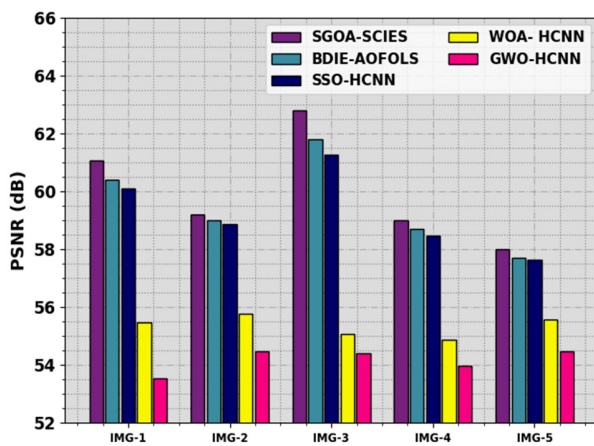


Fig. 3. PSNR outcome of SGOA-SCIES under distinct test images.

A detailed comparative analysis of the proposed with recent models [23] model is made. In Figure 3, the outcome exhibits that the SGOA-SCIES method reaches greater PSNR values. On IMG-1 the SGOA-SCIES method attain increased PSNR of 61.055dB while BDIE-AOFOLS, SSO-HCNN, WOA-HCNN, and GWO-HCNN approaches attain lesser PSNR of 60.42dB, 60.10dB, 55.46dB, and 53.54dB, respectively. Similarly, on IMG-5, the SGOA-SCIES approaches attain increased PSNR of 58.002dB while BDIE-AOFOLS, SSO-HCNN, WOA-HCNN, and GWO-HCNN approaches attain reduced PSNR of 57.72dB, 57.65dB, 55.58dB, and 54.48dB, respectively. These outputs ensured the enhanced security accomplishment of the SGOA-SCIES approach over the other techniques.

V. CONCLUSION

In this study, a new SGOA-SCIES method is demonstrated for the encryption of the shares in the VANET, aiming to create multiple shares and encrypt them to achieve security. It consists of three operation stages, which are MSC, FOCS-based share encryption, and SGOA-based key generation. In the presented SGOA-SCIES technique, the MSC scheme can be employed to generate multiple sets of shares. For the share encryption process, the SGOA-SCIES algorithm exploits the FOCS method to encrypt the generated shares. The optimal keys of the FOCS technique can be chosen by the use of SGOA which enhances the security level. The performance evaluation of the SGOA-SCIES method is examined on benchmark data. The stimulation outputs depicted the enhanced accomplishment of the SGOA-SCIES approach over other recent methodologies under various measures. The SGOA-SCIES technique may encounter challenges related to scalability and adaptability in dynamic network conditions. Future work for SGOA-SCIES should prioritize improving scalability, tackling dynamic network challenges, and optimizing for broader VANET communication applicability.

REFERENCES

- [1] K. Nova, U. A. S. S. Jacob, G. Banu, M. S. P. Balaji, and S. S. "Floyd-Warshalls algorithm and modified advanced encryption standard for secured communication in VANET," *Measurement: Sensors*, vol. 27, Jun. 2023, Art. no. 100796, <https://doi.org/10.1016/j.measen.2023.100796>.
- [2] A. Munshi, "Randomly-based Stepwise Multi-Level Distributed Medical Image Steganography," *Engineering, Technology & Applied Science Research*, vol. 13, no. 3, pp. 10922–10930, Jun. 2023, <https://doi.org/10.48084/etasr.5935>.
- [3] K. Vinoth Kumar and D. Balaganesh, "An optimal lightweight cryptography with metaheuristic algorithm for privacy preserving data transmission mechanism and mechanical design in vehicular ad hoc network," *Materials Today: Proceedings*, vol. 66, pp. 789–796, Jan. 2022, <https://doi.org/10.1016/j.matpr.2022.04.304>.
- [4] A. N. Mazher and J. Waleed, "Implementation of modified GSO based magic cube keys generation in cryptography," *Eastern-European Journal of Enterprise Technologies*, vol. 1, no. 9 (109), pp. 43–49, Feb. 2021, <https://doi.org/10.15587/1729-4061.2021.225508>.
- [5] C. Lakshmi, K. Thenmozhi, J. B. B. Rayappan, and R. Amirtharajan, "Hopfield attractor-trusted neural network: an attack-resistant image encryption," *Neural Computing and Applications*, vol. 32, no. 15, pp. 11477–11489, Aug. 2020, <https://doi.org/10.1007/s00521-019-04637-4>.
- [6] S. Alkhlwi, "Huffman Encoding with White Tailed Eagle Algorithm-based Image Steganography Technique," *Engineering, Technology & Applied Science Research*, vol. 13, no. 2, pp. 10453–10459, Apr. 2023, <https://doi.org/10.48084/etasr.5501>.
- [7] J. Qi, T. Gao, X. Deng, and C. Zhao, "A pseudonym-based certificateless privacy-preserving authentication scheme for VANETs," *Vehicular Communications*, vol. 38, Dec. 2022, Art. no. 100535, <https://doi.org/10.1016/j.vehcom.2022.100535>.
- [8] M. A. Mahdi, T. C. Wan, A. Mahdi, M. a. G. Hazber, and B. A. Mohammed, "A Multipath Cluster-Based Routing Protocol For Mobile Ad Hoc Networks," *Engineering, Technology & Applied Science Research*, vol. 11, no. 5, pp. 7635–7640, Oct. 2021, <https://doi.org/10.48084/etasr.4259>.
- [9] K. A. Kumari, A. Sharma, C. Chakraborty, and M. Ananyaa, "Preserving Health Care Data Security and Privacy Using Carmichael's Theorem-Based Homomorphic Encryption and Modified Enhanced Homomorphic Encryption Schemes in Edge Computing Systems," *Big Data*, vol. 10, no. 1, pp. 1–17, Feb. 2022, <https://doi.org/10.1089/big.2021.0012>.
- [10] D. Sharma, S. K. Gupta, A. Rashid, S. Gupta, M. Rashid, and A. Srivastava, "A novel approach for securing data against intrusion attacks in unmanned aerial vehicles integrated heterogeneous network using functional encryption technique," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 7, 2021, Art. no. e4114, <https://doi.org/10.1002/ett.4114>.
- [11] A. Albakri, R. Alshahrani, F. Alharbi, and S. B. Ahamed, "Fully Homomorphic Encryption with Optimal Key Generation Secure Group Communication in Internet of Things Environment," *Applied Sciences*, vol. 13, no. 10, Jan. 2023, Art. no. 6055, <https://doi.org/10.3390/app13106055>.
- [12] Z. Man, J. Li, X. Di, Y. Sheng, and Z. Liu, "Double image encryption algorithm based on neural network and chaos," *Chaos, Solitons & Fractals*, vol. 152, Nov. 2021, Art. no. 111318, <https://doi.org/10.1016/j.chaos.2021.111318>.
- [13] N. C. Velayudhan, A. Anitha, and M. Madanan, "Sybil Attack with RSU Detection and Location Privacy in Urban VANETs: An Efficient EPORP Technique," *Wireless Personal Communications*, vol. 122, no. 4, pp. 3573–3601, Feb. 2022, <https://doi.org/10.1007/s11277-021-09102-x>.
- [14] R. Wang, G.-Q. Deng, and X.-F. Duan, "An image encryption scheme based on double chaotic cyclic shift and Josephus problem," *Journal of Information Security and Applications*, vol. 58, May 2021, Art. no. 102699, <https://doi.org/10.1016/j.jisa.2020.102699>.
- [15] M. Kaur, D. Singh, and V. Kumar, "Color image encryption using minimax differential evolution-based 7D hyper-chaotic map," *Applied Physics B*, vol. 126, no. 9, Aug. 2020, Art. no. 147, <https://doi.org/10.1007/s00340-020-07480-x>.
- [16] J. F. Abukhait and M. S. Saleh, "An Adaptive Confidentiality Security Service Enhancement Protocol Using Image-Based Key Generator for Multi-Agent Ethernet Packet Switched Networks," *International Journal of Electrical and Electronic Engineering & Telecommunications*, vol. 12, no. 2, pp. 112–123, 2023, <https://doi.org/10.18178/ijeetc.12.2.112-123>.

- [17] S. Pamarthi and R. Narmadha, "Adaptive Key Management-Based Cryptographic Algorithm for Privacy Preservation in Wireless Mobile Adhoc Networks for IoT Applications," *Wireless Personal Communications*, vol. 124, no. 1, pp. 349–376, May 2022, <https://doi.org/10.1007/s11277-021-09360-9>.
- [18] M. A. Alohalı *et al.*, "Blockchain-Driven Image Encryption Process with Arithmetic Optimization Algorithm for Security in Emerging Virtual Environments," *Sustainability*, vol. 15, no. 6, Jan. 2023, Art. no. 5133, <https://doi.org/10.3390/su15065133>.
- [19] A. A. Bahattab, "Designing ROACM routing protocol along with bandwidth allocation using seagull optimization for ad hoc wireless network," *Telecommunication Systems*, vol. 81, no. 3, pp. 357–372, Nov. 2022, <https://doi.org/10.1007/s11235-022-00941-y>.
- [20] R. Punithavathi, A. Ramalingam, C. Kurangi, A. S. K. Reddy, and J. Uthayakumar, "Secure content based image retrieval system using deep learning with multi share creation scheme in cloud environment," *Multimedia Tools and Applications*, vol. 80, no. 17, pp. 26889–26910, Jul. 2021, <https://doi.org/10.1007/s11042-021-10998-7>.
- [21] J. Chen, C. Li, and X. Yang, "Chaos Synchronization of the Distributed-Order Lorenz System via Active Control and Applications in Chaotic Masking," *International Journal of Bifurcation and Chaos*, vol. 28, no. 10, Sep. 2018, Art. no. 1850121, <https://doi.org/10.1142/S0218127418501213>.
- [22] E. S. Ghith and F. A. A. Tolba, "Tuning PID Controllers Based on Hybrid Arithmetic Optimization Algorithm and Artificial Gorilla Troop Optimization for Micro-Robotics Systems," *IEEE Access*, vol. 11, pp. 27138–27154, 2023, <https://doi.org/10.1109/ACCESS.2023.3258187>.
- [23] M. M. Khayyat, M. M. Khayyat, S. Abdel-Khalek, and R. F. Mansour, "Blockchain enabled optimal Hopfield Chaotic Neural network based secure encryption technique for industrial internet of things environment," *Alexandria Engineering Journal*, vol. 61, no. 12, pp. 11377–11389, Dec. 2022, <https://doi.org/10.1016/j.aej.2022.05.002>.

Seagull Optimization Algorithm with Share Creation with an Image Encryption Scheme for Secure Vehicular Ad Hoc Networks

Ravichandran Mohan

Department of Computer Science and Engineering, Annamalai University, India
rkmmails@gmail.com (corresponding author)

Ganesan Prabakaran

Department of Computer Science and Engineering, Annamalai University, India
aucse@yahoo.com

Thirugnanasambandham Priyadarshikadevi

Department of Computer Science and Engineering, Mailam Engineering College, India
hodcse@mailamengg.com

Received: 20 December 2023 | Revised: 5 January 2024 | Accepted: 10 January 2024

Licensed under a CC-BY 4.0 license | Copyright (c) by the authors | DOI: <https://doi.org/10.48084/etasr.6786>

ABSTRACT

A Vehicular Ad hoc Network (VANET) allows transmission, amid moving or stationary vehicles via wireless technology. Amongst several problems, safe transmission is the most important one in smart VANETs in 5G networks. Smart vehicles require integration with advanced road systems encompassing smart payment and traffic control systems. Numerous security mechanisms are used in VANETs to ensure safe communication. One such mechanism is cryptographic digital signatures based on encryption. This study introduces the new seagull optimization algorithm involving share creation with an image encryption scheme (SGOA-SCIES) for secure VANET transmissions. The goal of the SGOA-SCIES technique is to create a considerable number of shares and encrypt them to accomplish security. In the SGOA-SCIES technique, a Multiple Share Creation (MSC) scheme is employed to generate numerous share sets. For the share encryption process, the SGOA-SCIES technique engages the Fractional-Order Chaotic System (FOCS) approach to encrypt the generated shares. The optimal keys of the FOCS method can be chosen by the SGOA usage, which ameliorates the security level. The performance evaluation of the SGOA-SCIES method is examined on benchmark data. The simulations demonstrate the enhanced SGOA-SCIES methodology outcome and compare it with the ones of other existing systems and under the implementation of various measures.

Keywords-security; vehicular ad-hoc network; encryption; key generation; share creation

I. INTRODUCTION

VANETs are considered a developing concept that allows dependable, infotainment-rich, and safe driving networking [1]. However, service providers, automobile manufacturers, and governments are still hesitant to employ VANETs due to certain difficulties generated during their usage, namely user options, requirements for infrastructure, cost, security and safety problems [2]. In the past, the automotive industry concentrated on in-car technology for upgrading entertainment and navigation systems. However, currently the research community engaged special focus of their studies on VANETs due to the increased computation, processing, and computational capacity of the higher-end vehicles [3]. These capacities allowed the evolution of V2I (vehicle-to-infrastructure) and V2V (vehicle-to-vehicle) transmission [4].

These transmission models may provide customers with protection and infotainment applications instead of only offering them particular applications, like a challenged endpoint, which could for instance be a friend's home or a restaurant in another city [5].

Various safety challenges are considered for providing information security defence in vehicular networks, among which, access control and data privacy are highly significant [6]. Data confidentiality confirms that the former cannot be revealed or leaked to unauthorized vehicles or nodes. For providing data integrity and confidentiality in VANET communication, encryption is employed to enable only authenticated users to acquire the transmitted information [7]. Conventional symmetrical data encryption could be a result, yet it requires communication expenses for establishing

authentication keys among data recipients and senders that prominently decrease the time consumed for accessing the resources. An alternate intuitive solution is to encrypt every piece of information with the receiver vehicle's public key and indicate the data prior to their transmission [8]. Given that data are generally transferred to numerous vehicles, there are several data ciphertexts by these standard encryption methods that fail to achieve real-time conditions of data distribution in vehicular applications [9]. This problem can be tremendously severe on the environments of security application's accurate timing limits. Besides that, access control maintenance is a massively unresolved issue, especially, in cases where there is no centralized access control for disseminating the encrypted data in extremely dynamic surroundings [10].

II. RELATED WORKS

Authors in [11] developed the fully homomorphic encryption with the optimum key generation secure group communication (FHEOKG-SGC) system. Initially, this method presents an FHE-based encoding system and later the keys in the FHE technique are effectively selected via SCA. Simultaneously, the plum tree model can be exploited for detecting routes. In [12], a dual-channel encryption technique is designed. Firstly, a chaotic map controls the preliminary value of 5D conservative chaotic systems. Then, a chaotic sequence is exploited as convolution kernels of CNN for generating plaintext correlated chaotic pointers. An image fusion technique, which fuses and splits images into two parts, is proposed. Authors in [13] designed the EPO-based Routing Protocol (EPORP) for an outbreak detection in Sybil. The Sybil attack is discovered through the rumour riding method. The Split XOR (SXOR) operator is implemented for optimizing VANET safety. The optimum keys are carefully selected through the EPO technique. Authors in [14] developed an image encryption technique by joining chaotic maps and Josephus problems. The entire encryption procedure implements the traditional permutation-diffusion model. During permutation, the double-chaotic cycle technique is devised by upgrading the chaotic shift transformation technique. During diffusion, the Josephus problem description is prolonged through chaotic maps to retain the Josephus sequence diversity. In [15], a 7D hyperchaotic map produces the secret key for image encryption. A minimax DE model provides the ideal parameter for the hyperchaotic maps. The parameter fitness is assessed by the entropy and correlation coefficient. Then, the secret key is generated by the hyperchaotic maps. This key performs the diffusion process on the input image and produces an encrypted image. Authors in [16] put forward adaptive safety-aware lottery-EDF schedulers for constrained resources packet switching of Ethernet network with the GAIA multi-agent method. This scheme employs periodic, non-shared cryptographic key generation operations of varying sizes based on textual features in digital images stored on the server.

Authors in [17] introduced a chaotic cryptographic-based privacy safeguarding method to increase privacy in MANET-IoT. The key-generating operation in chaotic mapping can be enhanced by producing the optimum key pair via the recently established SA-SFO method. The key nominated from the

chaotic maps can be impacted by choosing the optimum parameter via SA-SFO. Authors in [18] propose BDIE-AOFOLS, a blockchain-based image encryption method utilizing an arithmetical optimization algorithm with a fractional-order Lorenz system, optimizing key generation for the highest PSNR values. In [19], an energy-efficient ROACM protocol is introduced for ad hoc wireless networks, incorporating path discovery, metric-based selection, and optimal bandwidth allocation via a seagull optimization algorithm. The summary covers various encryption methods, including fully homomorphic encryption, dual-channel encryption, adaptive lottery-EDF schedulers, blockchain-based image encryption, and the mentioned ROACM protocol.

III. THE PROPOSED MODEL

In the presented study, the SGOA-SCIES method is suggested for the share encryption in VANETs, in an attempt to produce numerous shares and encrypt them for enhanced security. It comprises three operation stages: MSC, FOCS-based share encryption, and SGOA-based key generation. Figure 1 shows the workflow of the SGOA-SCIES system.

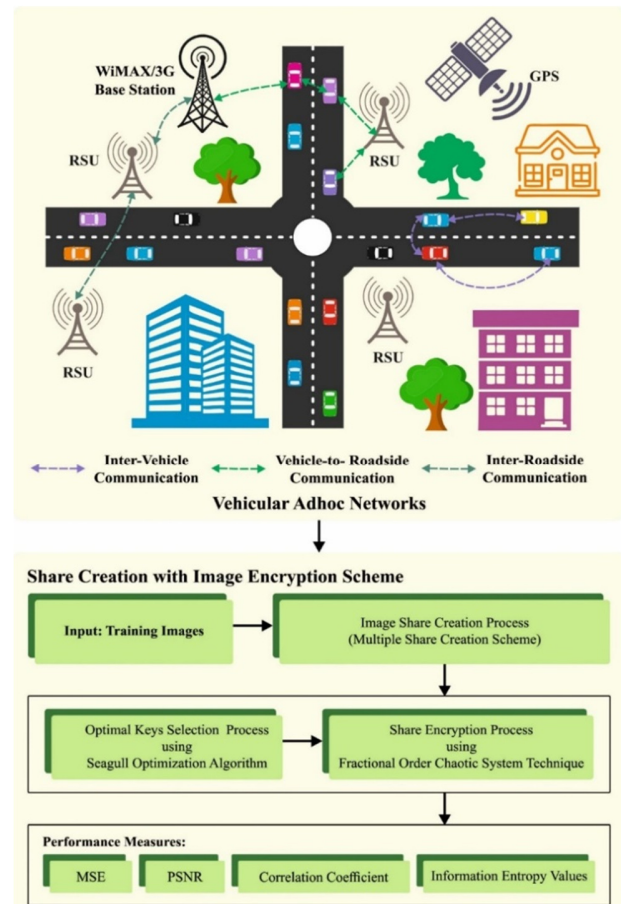


Fig. 1. Workflow of the SGOA-SCIES method.

A. Share Creation Procedure

Here, the MSC is enforced for producing a share collection. The RGB values are respectively determined in the matrix form

(R_m, G_m, B_m) and the extraction of actual image pixel value is conducted [20]. The matrix size is the same as the input image $(P * Q)$ and are described as:

$$\text{Pixel} = \sum R + G + B \quad (1)$$

Pixel depicts the overall amount of $R_m, G_m,$ and B_m values.

B. Share Creation

Each pixel that exists in the input images can be expressed by n transformed means, called shares. Each share includes sub-pixels of the RGB images. Based on the pixel value, the $R, G,$ and B shares exist in the RGB images and are characterized as $R_s, G_s,$ and B_s as follows:

$$R_s = \int_1^k \lim_{k \rightarrow 1} \text{ton} R_{ab} \quad (2)$$

$$G_s = \int_1^k \lim_{k \rightarrow 1} \text{ton} G_{ab} \quad (3)$$

$$B_s = \int_1^k \lim_{k \rightarrow 1} \text{ton} B_{ab} \quad (4)$$

where a and b show the matrix location, $R_s, G_s,$ and B_s symbolize the share of RGB and $R_{ab}, G_{ab},$ and B_{ab} indicate the image pixel component. The pixel value of RGB is taken from the original images and retained as an individual matrix. Then, the share is created based on the splitting of images into different parts. The objective of SMSC is to encrypt the images into an amount of insignificant shared imaging. The shares do not define any valuable data if the share is collectively incorporated.

The elementary matrices should be derived before share creation, based on the amount of shares to be generated that are predefined by the user. The matrix is obtained if the outputs of RGB in the pixels are partitioned by S . In general, the block size is found to be 4×4 or 8×8 . Also, an arbitrary key is provided by the input imaging block size. The amount of share is described as 2^S if $S \geq 2$. Later, the shares are derived by carrying out the XOR operation of the basic matrix on different combinations. In such cases, the share and matrix counts are 4 and 2. By splitting the RGB values of the pixel by 2, the matrix is derived. For instance, assume the block is of size 2×2 , the RGB value is defined. Then, the key matrix K_M is arbitrarily produced. The basic matrix is formulated by the aforementioned process and is characterized by B_{M1} and B_{M2} correspondingly. Before share creation, the succeeding process is conducted with the XR_1 and XR_2 matrices.

$$XR_1 = 128 - B_{M1} \quad (5)$$

$$XR_2 = B_{M2} \quad (6)$$

The red band share is formed by XORing both matrices:

$$Rs1 = XR_1 \oplus K_M \quad (7)$$

$$Rs2 = XR_2 \oplus XR_1 \quad (8)$$

$$Rs3 = XR_2 \oplus Rs1 \quad (9)$$

$$Rs4 = Rs1 \oplus R \quad (10)$$

$$\begin{cases} s_1 = (x_t(300) \times 100 - \text{floor}(x_t(300) \times 100)) \times 10^6 \text{mod } m \\ s_2 = (x_t(500) \times 100 - \text{floor}(x_t(500) \times 100)) \times 10^6 \text{mod } m \end{cases} \quad (17)$$

The abovementioned process is reiterated for the remaining green and blue bands to produce various shares.

C. Share Reconstruction

Various shares are merged to form the actual images in the share reconstruction process.

$$R = Rs1 \oplus Rs2 \oplus Rs3 \oplus Rs4 \oplus K_M \quad (11)$$

$$G = Gs1 \oplus Gs2 \oplus Gs3 \oplus Gs4 \oplus K_M \quad (12)$$

$$B = Bs1 \oplus Bs2 \oplus Bs3 \oplus Bs4 \oplus K_M \quad (13)$$

Encryption and decryption by applying the FOCS technique are employed on every colour band when the share is reconstructed. Before the encryption and decryption processes, the colour band images are split into various blocks. The blocks are divided into the 4×4 dimension. Various shares are produced and the encryption technique is exploited. Then the FOCS-based encryption technique is exploited on the shares.

D. Share Encryption using the FOCS Technique

FOCS approach is used to encrypt the shares. A color image encryption model is introduced using FOCS by combining 3 chaotic models (Fractional Lorenz System (FLS), Tent Map (TM), and Arnold Map (AM)) [21]. At first, the color plain image was divided into $R, B,$ and G layers. Then, 3 layers are scrambled with AM, where the key and R and G layers are the initial value of the former, and other 2 are scrambling. The gray values of RGB are moulded and employed as an initial value of FLS. Then, add-mode diffusing is implemented. Lastly, the encrypted images are obtained. The pixel matrix size is $M \times M \times 3$, the plain images are signified as $A,$ and the encryption process can be defined as follows:

Step 1: Enter P plain images and K keys, and assume the size of A is $M \times M \times 3$. Read the primary values and parameters of AM in K and exploit AM to scramble the plain images. Select the last 2 pixels of R layers, attain the gray values as AM parameter while scrambling the G layer, and employ the function which is same as scrambling B layer to get image P_1 .

$$P_1 = \begin{Bmatrix} R \\ G \\ B \end{Bmatrix} = \begin{Bmatrix} r(1), r(2), r(3), \dots, r(m) \\ g(1), g(2), g(3), \dots, g(m) \\ b(1), b(2), b(3), \dots, b(m) \end{Bmatrix} \quad (14)$$

$$m = \text{MIN} \quad (15)$$

Step 2: Read the initial values of TM $X(0)$ from key K . The TM is repeated 800 times. The first 300 conversion conditions are rejected and takes of the state values are represented as K_r .

$$K_\zeta = [x_t(200), x_t(300), x_t(400), x_t(500)] \quad (16)$$

Step3: Use (17) to make the K_ζ into s_1 and s_2 coordinates to place the pixels in P_1 . The FLS is repeated MIV and $2MN$ times, with smaller model perturbation repeated every 3000 times. This repetition occurs to attain the dimension of $3 \times MIV$ and $3 \times 2MIV$ of the new pseudo-random sequence S_1 and S_2 that are transformed (18) to password K_1 and K_2 .

$$K_o = \begin{bmatrix} K_{o1} \\ K_{o2} \end{bmatrix} = \begin{bmatrix} R_{s1}, G_s, B_{s1} \\ R_{s2}, G_{s2}, B_{s2} \end{bmatrix} \quad (18)$$

$$\begin{cases} K_1(j) = (\text{floor}(S_1(j) \times 2^{16}) \bmod 256) + 1 \\ K_2(j) = (\text{floor}(S_2(j) \times 2^{16}) \bmod 256) + 1 \end{cases} \quad (19)$$

Step4: The password K_1 to transfer the information between the layers of images is used. It is calculated as:

$$\begin{cases} r'(i) = r(i) \oplus k_1(1,i) \oplus b(i) \\ g'(i) = g(i) \oplus k_1(2,i) \oplus r(i), i = 1,2, \dots, MIN \\ b'(i) = b(i) \oplus k_1(3,i) \oplus g'(i) \end{cases} \quad (20)$$

where $r'(i)$, $g'(i)$, and $b'(i)$ show the pixel value after diffusing. Then the pixel, which addresses to the plain data of each layer, is diffused into other 2 layers. This enhances the ability to resist the selected-plain attack.

E. Optimal Key Generation by Utilizing SGOA

At the final stage, the SGOA is applied to produce an optimal set of keys for the FOCS approach. The SGOA is based on the inspiration of the movement pattern and on the attacking prey strategies of the seagulls [22]. To define the location of a new search agent (\vec{F}_s), collision avoidance between search agents in SOA is achieved using the second parameter N .

$$\vec{F}_s = N_x \vec{D}_s(t) \quad (21)$$

In (7), \vec{D}_s , denotes the current seagull location and the existing iteration. The collision avoidance parameter N is modelled as follows:

$$N = E_c - \left(t * \left(\frac{E_c}{Max.Iter} \right) \right) \quad (22)$$

For this, the value of 2 is selected to control the changes in the variable that linearly dropped from E_c to 0. The search agent makes an effort to move close to the position of the ideal individual using (23):

$$\vec{M}_s = A_x (\vec{P}_{bs}(t) - \vec{D}_s(t)) \quad (23)$$

The parameter A is randomized to attain the equilibrium tendency between the exploitation and exploration phases, and is computed by:

$$A = 2 * N^2 * rand() \quad (24)$$

The subsequent changes were made to each location of the search agents:

$$\vec{R}_s = [\vec{F}_s + \vec{M}_s] \quad (25)$$

During their migration, seagulls often change their attacking angle and speed. These behaviors in 3D are defined through the following equations:

$$S' = r * \cos(j) \quad (26)$$

$$T' = r * \sin(j) \quad (27)$$

$$U' = r * j \quad (28)$$

where r refers to the radius of seagulls' spiral movement and the random number selected within $[0, 2]$. The SGOA


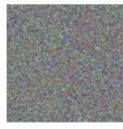
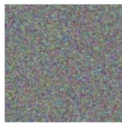
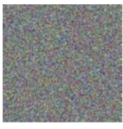
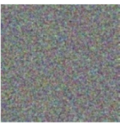

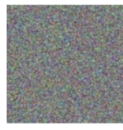
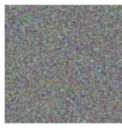
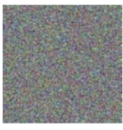
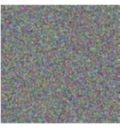



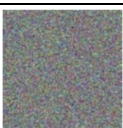
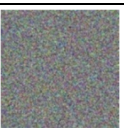
technique is applied in initializing the public and secret keys included in the encryption process. The fitness function of SGO for the FOLS method is given by:

$$Fitness\ function = \max \{PSNR\} \quad (29)$$

IV. RESULTS AND DISCUSSION

This segment inspects the outputs of the SGOA-SCIES approach on 5 test images. Table I portrays a sample visualization of multiple shares generated by the SGOA-SCIES technique on the applied test imaging. The findings suggest that the shares do not convey any significant information pertaining to the original image. The suggested model is simulated by employing Python 3.6.5 tool on PC i5-8600k, 250GB SSD, GeForce 1050Ti 4GB, 16GB RAM, and 1TB HDD. The parameter settings are provided as: learning rate: 0.01, activation: ReLU, epoch count: 50, dropout: 0.5, and batch size: 5. In Figure 2, the outputs indicate that the SGOA-SCIES technique obtains the least MSE values on all images. On IMG-1, the SGOA-SCIES technique obtains decreased MSE of 0.051, while the BDIE-AOFOLS, SSO-HCNN, WOA-HCNN, and GWO-HCNN models obtain improved MSE of 0.0590, 0.0636, 0.1850, and 0.2875, respectively.

TABLE I. VISUALIZATION OF THE MSC SCHEME

Original Image	1 - Share	2 - Share	3 - Share	4 - Share
				
				
				

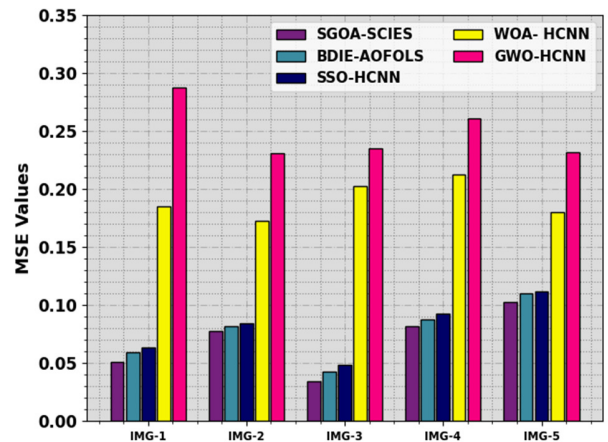


Fig. 2. MSE outcome of SGOA-SCIES under distinct test images.

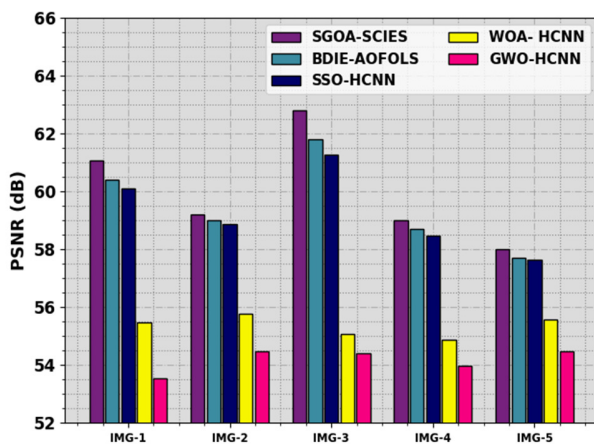


Fig. 3. PSNR outcome of SGOA-SCIES under distinct test images.

A detailed comparative analysis of the proposed with recent models [23] model is made. In Figure 3, the outcome exhibits that the SGOA-SCIES method reaches greater PSNR values. On IMG-1 the SGOA-SCIES method attain increased PSNR of 61.055dB while BDIE-AOFOLS, SSO-HCNN, WOA-HCNN, and GWO-HCNN approaches attain lesser PSNR of 60.42dB, 60.10dB, 55.46dB, and 53.54dB, respectively. Similarly, on IMG-5, the SGOA-SCIES approaches attain increased PSNR of 58.002dB while BDIE-AOFOLS, SSO-HCNN, WOA-HCNN, and GWO-HCNN approaches attain reduced PSNR of 57.72dB, 57.65dB, 55.58dB, and 54.48dB, respectively. These outputs ensured the enhanced security accomplishment of the SGOA-SCIES approach over the other techniques.

V. CONCLUSION

In this study, a new SGOA-SCIES method is demonstrated for the encryption of the shares in the VANET, aiming to create multiple shares and encrypt them to achieve security. It consists of three operation stages, which are MSC, FOCS-based share encryption, and SGOA-based key generation. In the presented SGOA-SCIES technique, the MSC scheme can be employed to generate multiple sets of shares. For the share encryption process, the SGOA-SCIES algorithm exploits the FOCS method to encrypt the generated shares. The optimal keys of the FOCS technique can be chosen by the use of SGOA which enhances the security level. The performance evaluation of the SGOA-SCIES method is examined on benchmark data. The stimulation outputs depicted the enhanced accomplishment of the SGOA-SCIES approach over other recent methodologies under various measures. The SGOA-SCIES technique may encounter challenges related to scalability and adaptability in dynamic network conditions. Future work for SGOA-SCIES should prioritize improving scalability, tackling dynamic network challenges, and optimizing for broader VANET communication applicability.

REFERENCES

- [1] K. Nova, U. A. S. S. Jacob, G. Banu, M. S. P. Balaji, and S. S. "Floyd-Warshalls algorithm and modified advanced encryption standard for secured communication in VANET," *Measurement: Sensors*, vol. 27, Jun. 2023, Art. no. 100796, <https://doi.org/10.1016/j.measen.2023.100796>.
- [2] A. Munshi, "Randomly-based Stepwise Multi-Level Distributed Medical Image Steganography," *Engineering, Technology & Applied Science Research*, vol. 13, no. 3, pp. 10922–10930, Jun. 2023, <https://doi.org/10.48084/etasr.5935>.
- [3] K. Vinoth Kumar and D. Balaganesh, "An optimal lightweight cryptography with metaheuristic algorithm for privacy preserving data transmission mechanism and mechanical design in vehicular ad hoc network," *Materials Today: Proceedings*, vol. 66, pp. 789–796, Jan. 2022, <https://doi.org/10.1016/j.matpr.2022.04.304>.
- [4] A. N. Mazher and J. Waleed, "Implementation of modified GSO based magic cube keys generation in cryptography," *Eastern-European Journal of Enterprise Technologies*, vol. 1, no. 9 (109), pp. 43–49, Feb. 2021, <https://doi.org/10.15587/1729-4061.2021.225508>.
- [5] C. Lakshmi, K. Thenmozhi, J. B. B. Rayappan, and R. Amirtharajan, "Hopfield attractor-trusted neural network: an attack-resistant image encryption," *Neural Computing and Applications*, vol. 32, no. 15, pp. 11477–11489, Aug. 2020, <https://doi.org/10.1007/s00521-019-04637-4>.
- [6] S. Alkhlwi, "Huffman Encoding with White Tailed Eagle Algorithm-based Image Steganography Technique," *Engineering, Technology & Applied Science Research*, vol. 13, no. 2, pp. 10453–10459, Apr. 2023, <https://doi.org/10.48084/etasr.5501>.
- [7] J. Qi, T. Gao, X. Deng, and C. Zhao, "A pseudonym-based certificateless privacy-preserving authentication scheme for VANETs," *Vehicular Communications*, vol. 38, Dec. 2022, Art. no. 100535, <https://doi.org/10.1016/j.vehcom.2022.100535>.
- [8] M. A. Mahdi, T. C. Wan, A. Mahdi, M. a. G. Hazber, and B. A. Mohammed, "A Multipath Cluster-Based Routing Protocol For Mobile Ad Hoc Networks," *Engineering, Technology & Applied Science Research*, vol. 11, no. 5, pp. 7635–7640, Oct. 2021, <https://doi.org/10.48084/etasr.4259>.
- [9] K. A. Kumari, A. Sharma, C. Chakraborty, and M. Ananyaa, "Preserving Health Care Data Security and Privacy Using Carmichael's Theorem-Based Homomorphic Encryption and Modified Enhanced Homomorphic Encryption Schemes in Edge Computing Systems," *Big Data*, vol. 10, no. 1, pp. 1–17, Feb. 2022, <https://doi.org/10.1089/big.2021.0012>.
- [10] D. Sharma, S. K. Gupta, A. Rashid, S. Gupta, M. Rashid, and A. Srivastava, "A novel approach for securing data against intrusion attacks in unmanned aerial vehicles integrated heterogeneous network using functional encryption technique," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 7, 2021, Art. no. e4114, <https://doi.org/10.1002/ett.4114>.
- [11] A. Albakri, R. Alshahrani, F. Alharbi, and S. B. Ahamed, "Fully Homomorphic Encryption with Optimal Key Generation Secure Group Communication in Internet of Things Environment," *Applied Sciences*, vol. 13, no. 10, Jan. 2023, Art. no. 6055, <https://doi.org/10.3390/app13106055>.
- [12] Z. Man, J. Li, X. Di, Y. Sheng, and Z. Liu, "Double image encryption algorithm based on neural network and chaos," *Chaos, Solitons & Fractals*, vol. 152, Nov. 2021, Art. no. 111318, <https://doi.org/10.1016/j.chaos.2021.111318>.
- [13] N. C. Velayudhan, A. Anitha, and M. Madanan, "Sybil Attack with RSU Detection and Location Privacy in Urban VANETs: An Efficient EPORP Technique," *Wireless Personal Communications*, vol. 122, no. 4, pp. 3573–3601, Feb. 2022, <https://doi.org/10.1007/s11277-021-09102-x>.
- [14] R. Wang, G.-Q. Deng, and X.-F. Duan, "An image encryption scheme based on double chaotic cyclic shift and Josephus problem," *Journal of Information Security and Applications*, vol. 58, May 2021, Art. no. 102699, <https://doi.org/10.1016/j.jisa.2020.102699>.
- [15] M. Kaur, D. Singh, and V. Kumar, "Color image encryption using minimax differential evolution-based 7D hyper-chaotic map," *Applied Physics B*, vol. 126, no. 9, Aug. 2020, Art. no. 147, <https://doi.org/10.1007/s00340-020-07480-x>.
- [16] J. F. Abukhait and M. S. Saleh, "An Adaptive Confidentiality Security Service Enhancement Protocol Using Image-Based Key Generator for Multi-Agent Ethernet Packet Switched Networks," *International Journal of Electrical and Electronic Engineering & Telecommunications*, vol. 12, no. 2, pp. 112–123, 2023, <https://doi.org/10.18178/ijeetc.12.2.112-123>.

- [17] S. Pamarthi and R. Narmadha, "Adaptive Key Management-Based Cryptographic Algorithm for Privacy Preservation in Wireless Mobile Adhoc Networks for IoT Applications," *Wireless Personal Communications*, vol. 124, no. 1, pp. 349–376, May 2022, <https://doi.org/10.1007/s11277-021-09360-9>.
- [18] M. A. Alohalı *et al.*, "Blockchain-Driven Image Encryption Process with Arithmetic Optimization Algorithm for Security in Emerging Virtual Environments," *Sustainability*, vol. 15, no. 6, Jan. 2023, Art. no. 5133, <https://doi.org/10.3390/su15065133>.
- [19] A. A. Bahattab, "Designing ROACM routing protocol along with bandwidth allocation using seagull optimization for ad hoc wireless network," *Telecommunication Systems*, vol. 81, no. 3, pp. 357–372, Nov. 2022, <https://doi.org/10.1007/s11235-022-00941-y>.
- [20] R. Punithavathi, A. Ramalingam, C. Kurangi, A. S. K. Reddy, and J. Uthayakumar, "Secure content based image retrieval system using deep learning with multi share creation scheme in cloud environment," *Multimedia Tools and Applications*, vol. 80, no. 17, pp. 26889–26910, Jul. 2021, <https://doi.org/10.1007/s11042-021-10998-7>.
- [21] J. Chen, C. Li, and X. Yang, "Chaos Synchronization of the Distributed-Order Lorenz System via Active Control and Applications in Chaotic Masking," *International Journal of Bifurcation and Chaos*, vol. 28, no. 10, Sep. 2018, Art. no. 1850121, <https://doi.org/10.1142/S0218127418501213>.
- [22] E. S. Ghith and F. A. A. Tolba, "Tuning PID Controllers Based on Hybrid Arithmetic Optimization Algorithm and Artificial Gorilla Troop Optimization for Micro-Robotics Systems," *IEEE Access*, vol. 11, pp. 27138–27154, 2023, <https://doi.org/10.1109/ACCESS.2023.3258187>.
- [23] M. M. Khayyat, M. M. Khayyat, S. Abdel-Khalek, and R. F. Mansour, "Blockchain enabled optimal Hopfield Chaotic Neural network based secure encryption technique for industrial internet of things environment," *Alexandria Engineering Journal*, vol. 61, no. 12, pp. 11377–11389, Dec. 2022, <https://doi.org/10.1016/j.aej.2022.05.002>.