TP-IoAV: A tri-party cloud data protection scheme for Internet of Autonomous Vehicle coupled with chaotic biometric cryptography

Zhenlong Man, Ze Yu, Jiahui Yu, Xiangfu Meng

***Abstract*—As driverless technology advances, an immense amount of data will be generated, shared, and used between vehicles, users, and the cloud. This includes road conditions, GPS data, biometric data, which raises significant privacy concerns. This paper presents a secure authentication protocol and privacy protection framework based on chaotic biological cryptography for data sharing and storage in the Internet of Autonomous Vehicles(IoAV) framework. A biometric key generator is designed using single-modal multi-fingerprint feature-level reconstruction, allowing users to generate personalized private key pools. This protects biometric data in the cloud while ensuring revocability. By incorporating a nonlinear control function into the traditional three-dimensional Rucklidge chaotic system, a 4D-Yoz hyperchaotic system is created, ensuring secure key distribution and adherence to the "one time pad" principle. To verify the effectiveness of the chaos creature password and ensure the security of cloud-stored images, proposes an image encryption-storage algorithm based on the "L_∞" metric and the semi-tensor product of the matrix, introducing the chaotic biological key. Experimental simulations and performance analysis show that this algorithm effectively secures image data in the Internet of Vehicles.**

***Index Terms*—Internet of Autonomous Vehicle(IoAV), Security, Multi-party Key Agreement, Chaotic System**

I. Introduction

THE Internet of Vehicles (IoV) represents a pivotal component of prospective intelligent traffic safety systems, exhibiting a notable surge in advancement over recent years. The conventional architectural framework of this system encompasses three fundamental elements: users, vehicles, and the cloud network [1]. This facilitates vehicles's capacity to communicate with devices in real time, facilitate global decision optimization through information sharing, and ultimately achieve the objective of remote vehicle control.

As research into big data and artificial intelligence progresses, the sharing of data has become increasingly widespread, leading to innovations in technologies such as driverless cars, smart bus systems, and smart parking. However, intelligent transportation systems require the processing of a considerable amount of user data and traffic information during operation, which has led to a heightened awareness of the importance of data security in the context of promotion and application. For instance, traffic cameras are employed to capture vehicle speed and traffic patterns, thereby optimizing traffic management. Conversely, onboard cameras are responsible for functions such as obstacle detection and intelligent distance monitoring [2]–[4]. Zavvos et al [5]. identified four main privacy risks in vehicular networks: personal information privacy, multi-party privacy, trust, and consent. In the process of vehicle networking communication, the generation and sharing of large amounts of data accompanies the entire life cycle of system operation, involving voluntary and involuntary privacy leaks of users. The urgent necessity to study and solve the problem of how to safely and efficiently process shared data and ensure the transmission and storage of shared data under the IoAV network is paramount. The most recent investigation by Edris et al. into the security of the IoV reveals a potential guideline for protecting IoV security: namely, that the real identity and location information of users should not be accessed illegally by unwanted users [6]. From a technical standpoint, the IoV is characterised as a decentralised network in which vehicles function as both routers and hosts. It is imperative to ensure that malicious nodes do not cause illegal intrusions and attacks. Furthermore, it is not possible to assume that the network environment, communication channels, or even the vehicles (nodes) involved in the communication process are trustworthy. The only user who can be trusted is a third party with absolute security. However, it is important to note that the key pool stored by this third party is also susceptible to theft and tampering. In order to maximise the security level of the IoV, it is essential to comprehensively consider the security of data at all stages, from collection to sharing to use, and this process should be independent of any user (even the sender).

It is evident that the development and application of autonomous driving technology has enabled vehicles to communicate with roadside units and cloud networks, thereby facilitating automatic route planning, intelligent obstacle avoidance and driving assistance. However, this development is concomitant with increased security risks, which can be classified as either active manipulation by threat actors or passive leakage of privacy. To illustrate the former, the literature cites instances of attacks by hacker groups on Tesla's Autopilot software, resulting in erroneous turn planning and significant societal distrust in autonomous driving technology [7], [8]. This, in turn, has precipitated substantial economic losses and a crisis of confidence. The latter is a more prevalent and recurrent phenomenon. The development of artificial intelligence tech-

This work was supported in part by Basic Research Project of Liaoning Provincial Department of Education (JYTQN2023208) and in part by Liaoning Province Guiding City Science and Technology Development Special Project - Liaoning Provincial Natural Science Foundation Joint Plan (20240344). Zhenlong Man and Ze Yu made equal contributions (Corresponding author: Zhenlong Man (email:manzhenlong@lntu.edu.cn)

nology has led to increasingly sophisticated connected car systems, though these are not immune to security threats. The in-depth application of AI technology in autonomous driving connected cars has been shown to lead to increased data access and large-scale data transmission, which can potentially expose even more significant privacy leaks and data security issues [9]. As Hamideh et al. investigated, the security risks in autonomous driving connected cars have a lot of room for discussion [10].

In the context of identity authentication, the utilisation of biometric authentication for both identification and key generation in the IoV has gained significant traction. This represents a parallel research trajectory, concomitant with the identification of the vehicle's unique identifier. In comparison with conventional knowledge-based (e.g. PIN codes and passwords) and asset-based (e.g. smart cards) key management methods [11], [12], biometric authentication solutions have garnered significant attention due to their non-replicability and uniqueness [13]. However, the highly sensitive nature of biometric information poses a significant risk of irreparable harm and loss of personal identity information online if misappropriated or modified. As early as 2010, researchers such as Manvjeet Kaur [14] identified security threats in the storage of biometric data in databases, including data leakage and privacy violations. They proposed the use of auxiliary data to assist in authentication, with the aim of reducing the risk of the original data being stolen or altered. The EU General Data Protection Regulation (GDPR) classifies biometric data as sensitive data. Unfortunately, the protection of biometric templates themselves is still insufficient for large databases and cloud data centres. Li et al. recently reviewed the latest research and protocols on privacy-preserving biometrics [15]. More worryingly, with the development of artificial intelligence and pattern recognition technology, biometrics has become a powerful tool for individuals and businesses to interact with large databases or distributed systems, but its security has not been fully addressed. In terms of connected cars, Hanay et al. have recently proposed a secure communication scheme based on biometrics and hash key derivation functions [16], and we highly appreciate their work. However, we must point out that in practical applications, the security of the entire process of collecting, transmitting and storing biometric templates still needs to be fully considered. Through a cleverly designed encryption scheme, the protection of biometric templates can improve the robustness of the system while protecting the data. The research by Xie et al. proposes a conditional privacy-preserving IoV authentication protocol that ensures communication security through a three-factor confidentiality strategy. Our research builds on the above and provides a customised secure three-party communication solution for the IoV by designing secure biometric template collection, key generation (pseudo-hashing) and periodic key pools.

In conclusion, the implementation of biometric authentication in lieu of conventional authentication techniques and the utilisation of a chaotic system to generate a repository of personal keys for data encryption demonstrate considerable promise for application within the domain of the IoAV. However, it is imperative to guarantee the security of the biometric data itself.

However, existing IoV security approaches face several critical limitations that hinder their practical deployment in autonomous vehicle environments. Traditional biometric authentication systems suffer from inherent vulnerabilities including template irreversibility, susceptibility to spoofing attacks, and limited scalability for multi-party communications. Current encryption schemes typically focus on single-aspect protection, addressing either data confidentiality or authentication integrity, but rarely providing comprehensive security coverage for the complex tri-party interactions required in IoAV systems. Furthermore, many existing chaotic cryptographic methods operate with limited key spaces and predictable parameter ranges, making them vulnerable to advanced cryptanalytic attacks in long-term deployment scenarios. The lack of integrated frameworks that simultaneously address biometric template protection, multi-party key agreement, and real-time encryption requirements represents a significant gap in current IoAV security research.

To address the comprehensive security challenges in IoAV environments, this paper proposes an integrated three-party security framework that combines chaotic biometric cryptography with advanced encryption techniques. **The specific contributions are as follows:**

- **Tri-party communication agreement:** We propose a secure communication protocol for IoAV that enables protected data exchange between cloud servers, users, and vehicle terminals. The protocol utilizes ciphertext storage of biometric data, effectively mitigating privacy and security vulnerabilities during authentication and transmission processes.
- **Restrictive Entropy Bio-Code Generator (Re-BCG):** We develop a biometric key generator based on constrained entropy that employs multi-fingerprint features to address limitations of traditional biometric templates. The generator dynamically updates the key pool based on user authentication behavior, enabling a "one time pad" distribution that enhances system security and flexibility.
- **Integrated cryptographic framework for IoAV:** A comprehensive security solution is introduced, featuring an improved 4D-Yoz hyperchaotic system with enhanced randomness and ergodicity properties. This approach employs the L_∞ metric (Chebyshev distance) for scrambling and the semi-tensor product for diffusion, providing superior chaotic characteristics and significantly enhanced resilience against attacks on data in vehicular networks.

The remainder of this paper is organized as follows: Section II reviews related work in IoV security. Section III presents our TP-IoAV framework and system architecture. Section IV details the Re-BCG implementation. Section V describes the 4D-Yoz hyperchaotic system and image encryption algorithm. Section VI analyzes security adversaries. Section VII presents experimental results. Section VIII concludes with contributions and future directions.

II. Related Work

A. Authentication and Privacy in IoV

In transparent networks, data interception, tampering, forgery and false information injection are possible [12]. Therefore, robust authentication, key assurance and data encryption techniques are crucial for secure communication in traditional IoV systems. Libing Wu et al [17]. developed a privacy-preserving authentication protocol for IoV, which enhances security but increases overhead. The scheme also uses group signature technology, dividing regions into groups managed by designated personnel, allowing any vehicle to sign messages for its group members. However, this approach does not fully address detailed authentication and key uniqueness. Xia Feng et al. introduced blockchain technology and proposed a privacy-preserving blockchain-based authentication protocol with global-updated commitment [18], which ensures anonymity and unlinkability while having low computational costs. Hu Xiong et al. proposed a fine-grained mutual recognition protocol that provides forward and backward security [19].

Miao Junfeng et al. propose a UAV-assisted vehicle networking authentication protocol that uses an elliptic curve algorithm to ensure security and is more resistant to known attacks [20]. The protocol focuses on identity authentication. In a recent publication, Jie Cui [21] and colleagues put forward a novel approach to safeguarding confidential data by integrating Physical Unclonable Functions (PUFs) into automotive sensors, while also considering security, computational costs, and environmental noise. However, some experts have highlighted a potential limitation of traditional PUFs: machine learning techniques could predict them, resulting in security risks including data leakage or loss [22]–[24]. In the context of considering security issues in vehicular communications and distributed systems, Ke Gu et al [25]. discuss the privacy challenges in the Internet of Things (IoT) communications, emphasizing the connection between identifiable information and vehicles. They develop a decentralized privacy-preserving scheme that uses fog computing to hide vehicle identities and a secret sharing scheme to achieve tracking. They also propose a fog server generation method based on a voting mechanism to meet IoT security requirements, demonstrating secure data collection in real and random number models.

The present algorithm is dedicated to the combination of the authentication function of biometrics with the security of pseudo-random numbers, with a view to constructing a trusted authentication scheme for multi-party communication whilst ensuring identity authentication. The protocol is designed to identify legitimate identities in untrusted networks and to strictly regulate these identities. The security of the protocol is ensured through the use of a large key space and the update behaviour itself.

B. Biometric Template Protection and Security

In contemporary academic circles, the secure storage of biological data has emerged as a prominent area of interest. Scholars such as Shantanu Rane [26] have conducted an in-depth examination of the foundational principles of biometric and identity authentication, identifying significant challenges in integrating these methods with conventional encryption techniques. Anirban Sengupta et al [27]. proposed a hardware security method that employs protein molecular biometric signatures and facial biometric encryption keys. This method utilizes a protein sequence comprising 20 different amino acids to develop an encryption scheme, combining these with facial biometric keys to enhance robustness. In the domain of fingerprint image encryption, Liu Huipeng et al. developed a novel encryption algorithm, utilising a combination of chaos theory and dynamic X models. Concurrently [28], Rajeskannan et al. proposed an alternative algorithm utilising a second-order hyperstable chaotic oscillator. However, these studies do not take into account the practical considerations necessary for ensuring the privacy of biological templates when encrypting fingerprint images [29].

Although the aforementioned scheme effectively secures biological information, it is designed for single-fingerprint images during key generation and does not fully address noise factors, revocability requirements, frequent user behavior, and transparent network environments in the IoV. To address these limitations, we have developed a bio-chaotic cryptosystem with constrained entropy for single-modal multi-fingerprint images. The efficacy of this scheme has been validated through experimentation.

C. Data Encryption in IoV

In the context of the IoT, the security of images is of paramount importance, given their pervasive use in a range of applications including identity confirmation, road condition monitoring, surveillance, and remote sensing. These applications typically involve the processing of significantly larger volumes of data than traditional forms [30]–[33]. A data breach could result in significant violations of privacy. Manjari Singh Rathore and colleagues [34] put forth a novel data protection methodology that combines encryption and steganography [34]. This approach utilizes a variety of symmetric encryption techniques within the three primary components of the vehicle communication process. The high sensitivity, pseudo-randomness, and convenience of chaotic systems render them optimal for image encryption. For example, X. Chai et al [35]. employed a chaotic image encryption scheme based on DNA sequence operations, achieving DNA-level scrambling and diffusion through a Coupled Map Lattice (CML). However, one-dimensional chaotic maps are constrained by limited periodic windows and narrow key spaces, which impede their capacity for key complexity. To address this limitation, J. Zhang et al [36]. proposed an image encryption scheme based on the cat map and the hyperchaotic Lorenz system, utilizing the Arnold cat map for scrambling and ensuring that key generation is related to the plaintext.

Recent developments in IoT and vehicular networks have further advanced image encryption methodologies. Singh et al. [37] introduced an image security model combining chaos and DNA cryptography specifically for Industrial IoT (IIoT) images, demonstrating enhanced resistance to statistical attacks through biological encoding mechanisms. Huang and Cai

TABLE I
SYMBOL SUMMARY

Symbol	Description
U_i	User end (mobile app, unified controller)
Bio_i	User's biometric feature set
Or_i	Digital key group depending on fingerprint input sequence
$h(\cdot)$	Designed unidirectional pseudo-hash function
$Bk(\cdot)$	Random biometric key generated using Re-BKG
$Y_{x\|y\|z\|w}$	Random numbers generated by chaotic system
UO_i	Digital key group in random state
YB_i	Biometric key in random state
$\mathcal{M}$	Biometric key matrix generated by Re-BKG
C_i	Intelligent vehicle terminal
CB	Cloud Server
DB	DataBase

[38] proposed a duple color image encryption system based on 3-D nonequilateral Arnold transform for IIoT applications, effectively addressing the vulnerabilities inherent in traditional 2D scrambling approaches. For intelligent transportation systems, Sun et al. [39] developed BI-IEA, a bit-level image encryption algorithm for cognitive services, achieving optimized correlation coefficients of adjacent pixels at 0.0022, -0.0018, and -0.0005 in horizontal, vertical, and diagonal directions respectively. Additionally, Muhammad et al. [40] presented a secure surveillance framework for IoT systems using probabilistic image encryption, reducing computational overhead while maintaining robust security properties.

The present paper extends the key space under the premise of limited entropy by fusing chaos and biometrics, and proposes an encryption algorithm that incorporates the semi-tensor product. The protection of images in the context of user car networking necessitates these advanced cryptographic approaches, particularly given the real-time processing requirements and resource constraints inherent in vehicular communication environments.

III. Y-INTERNET OF AUTONOMOUS VEHICLE

In this section, a secure communication model between users, vehicles, the cloud, and data centers is established to provide secure communication and session key sharing to ensure the security of user and vehicle data during the operation of the IoV and Autonomous Vehicles (AV). The specific architecture is shown in Figure 1. The specific plan is as follows: The autonomous vehicle collects road information through embedded intelligent sensing devices such as on-board sensors (e.g., cameras, radars), microcontrollers, etc., and uploads it to the cloud server. The cloud shares data with the vehicle through a DataBase (DB), machine learning model, distributed system, etc., and at the same time, a legitimate User (U_i) can send instructions to open cloud permissions and control the vehicle. Table I summarizes the symbols used and their meanings.

A. Y-IoAV system frame

In the Y-IoAV connected car system, data security is ensured through the implementation of TP-IoAV. First, the biometric features of the authenticated user are used to generate an original biometric template. The authentication behavior record is used to generate a key pool in lieu of storing the original biometric template. The regular authentication behavior and introduction of a chaotic system can ensure a sufficiently large key pool to prevent biometric attacks such as destruction, theft, injection, and cloning. Concurrently, cloud servers distributed in nearby data centers are responsible for supporting the mutual authentication process.

In addition, the disorder and randomness inherent to the chaotic system guarantee that legitimate users's remote operations are conducted in a "one time pad" state. Secure communication between remote control users and AVs is established. The user's authentication status can influence the DC's decision to transmit data. This guarantees the security of personal biometric, private, and high-value data during transmission between AVs, UP, cloud servers, and DCs.

- U_i: Users register and authenticate via biometrics, gaining authorization for cloud communication, vehicle remote control, and data acquisition. This functionality integrates with mobile applications and wearable devices. Keys update in real-time based on authentication behavior, while sensitive data handling is protected through key agreement protocols.
- C_i: Vehicles communicate with the cloud network through the On-Board Unit (OBU), accessing critical traffic information and machine learning outputs. The TKP-CV implementation restricts unauthorized operations and secures data transmission and storage through encryption.
- CB: Cloud servers integrated with the chaotic system access the original biometric key pool and generate random keys via the 4D-Yoz hyperchaotic system. Parameter adjustment expands the key pool, ensuring dynamic "one key pad" distribution for command operations.
- DB: Data centers collect and aggregate information from authenticated users and vehicles, including road condition images and remote sensing data. These images are stored in encrypted format to prevent unauthorized access and modification.

Secure communication is critical for the IoAV. Our approach uses a multi-layered security architecture where a biometric key agreement protocol protects each communication channel. Vehicles use cryptographic identifiers from the 4D-Yoz hyperchaotic system to authenticate to the cloud, and user commands are verified through the Re-BCG mechanism before execution. This prevents unauthorised access and protects against man-in-the-middle attacks during vehicle-to-cloud and user-to-vehicle communications. All sensitive data is encrypted using the proposed image security algorithms, ensuring protection even if intercepted. The dynamic key updating mechanism refreshes encryption keys based on authentication patterns, making previously captured communication data useless for attackers.

B. Tri-party communication agreement

It is now feasible for users to control data centers and smart cars through cloud servers; nevertheless, there is a risk of data leakage or tampering with during transmission. It is therefore possible to periodically update the biometric template by using

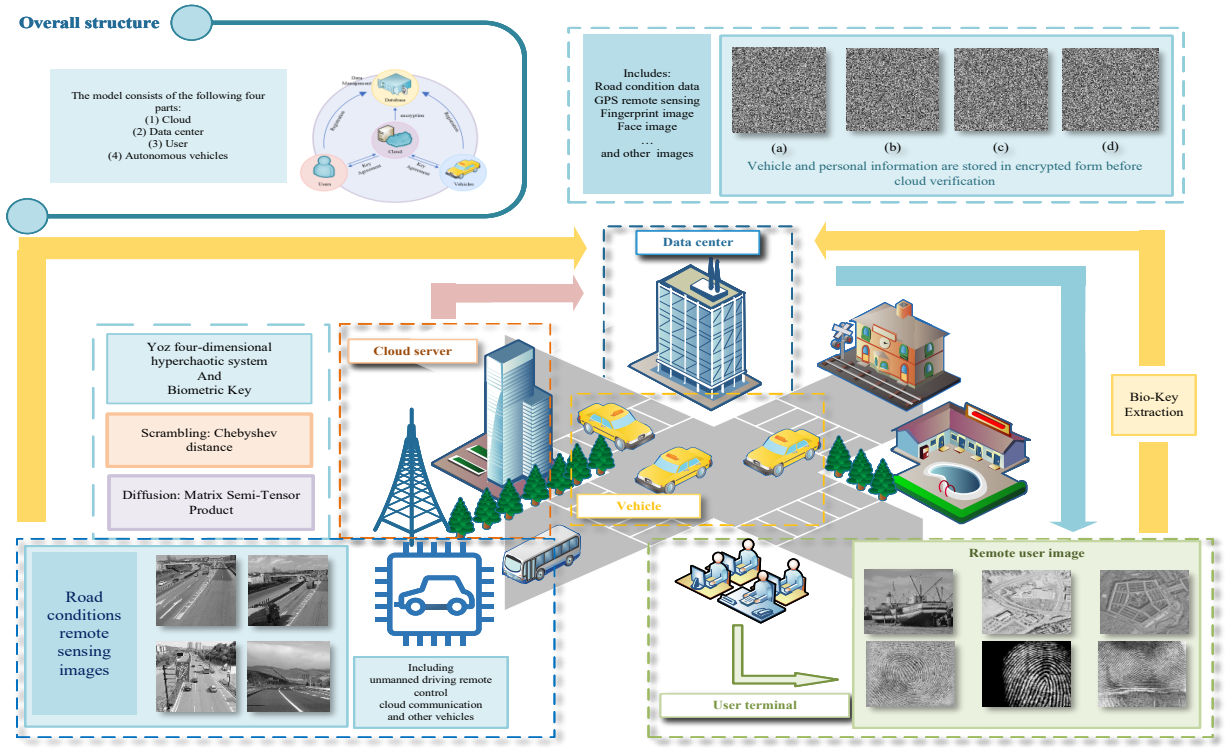

Fig. 1. System frame work of Y-IoAV showing data flow and encryption processes between cloud servers, data centers, user terminals, and autonomous vehicles.

the user's daily authentication behavior, while simultaneously introducing a chaotic system to ensure the revocability of the biometric template while achieving "one time pad" for authorized actions (such as retrieval and modification). In order to satisfy the aforementioned requirements, Three-Party Key Agreement Protocol for Internet of Autonomous Vehicles (TP-IoAV) has been devised for use in IoV and driverless cars, as illustrated in Figure 2. A secure user biometric key pool is created by a constrained entropy biometric key generator for communication with the cloud. The key pool is expanded in the cloud by a 4D-Yoz hyperchaotic system to provide key protection data and privacy. The user's private data is encrypted with a key and finally stored in the data center, allowing the three parties to securely exchange confidential messages.

For privacy data, traffic information, and vehicle capture images, encryption is performed using the image algorithm described in Section V to ensure data security in the database and to ensure that only legitimate users can access the privacy data in the database.

1) User registration and initialization of the key: In order to establish a secure communication channel between the cloud server and the user, it is necessary for the user to register their identity through the use of biometric authentication, whereby a binary pair Bio_i, Or_i is sent to the cloud server. It should be noted that the biometric images themselves are not stored within the database; this is in accordance with the regulations set out by the relevant data protection legislation. In lieu of storing the biometric images themselves, this information is utilized to generate biometric keys through the Re-BCG,

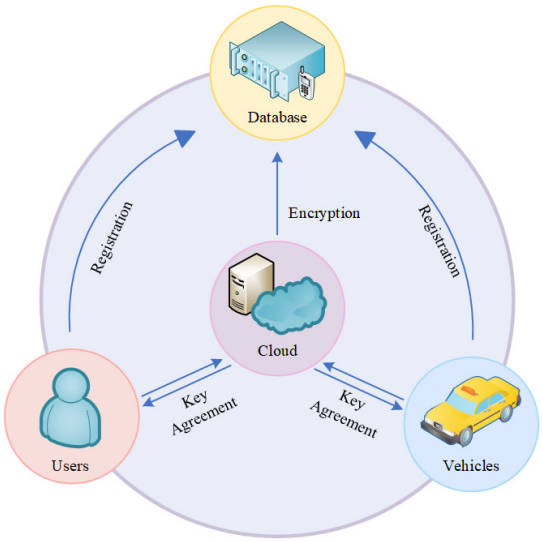

Fig. 2. Tri-party key agreement protocol illustrating secure communication mechanisms between users, cloud servers, and vehicles.

a bio-code generator that employs restrictive entropy. To guarantee the system's integrity and the privacy and security of authorized users, the key pool is refreshed daily through authentication, which includes a biometric key matrix and a digital biometric key. To prevent targeted attacks during transmission, Or_i are generated through a pseudo-one-way hash function, and a minor alteration in the initial value can result in significant differences.

The pseudo-hash function is designed as follows: for the

original input sequence $S = \{s_1, s_2, s_3, ..., s_{10}\}$, a $seedvalue$ based on the digits is calculated to initialize the pseudo-random number generator. The formula is $seed = \sum_i^{10} s_i \times 31^{10-i}$, and this cumulative calculation reflects the degree of contribution of each digit to the $seedvalue$. To control the seed size, take $seed = (seed) mod(2^{31} - 1)$, and based on this seed, generate a random index Or_i and rearrange the number sequence.

2) Cloud key pool construction: Once the key has been initialized, the system control parameters a, b, c, d, k, e, n, m and the initial state values x, y, z, w are configured in the cloud. To stabilize the system state and circumvent transient effects, the Runge-Kutta method is employed to iterate the 4D-Yoz hyperchaotic system 800 times. The initial $t = 2000$ data points are discarded to guarantee the quality and randomness of the generated random sequence $Yoz_x, Yoz_y, Yoz_z, Yoz_w$. Subsequently, the key is obtained by truncating the matrix $m \times n$ in accordance with the biological key.

$$\begin{cases} K_x = & \mod (\lfloor Y_{ox} \times 10^{15} \rfloor, N \times M) \\ K_y = & \mod (\lfloor Y_{oy} \times 10^{15} \rfloor, N \times M) \\ K_z = & \mod (\lfloor Y_{oz} \times 10^{15} \rfloor, N \times M) \\ K_w = & \mod (\lfloor Y_{ow} \times 10^{15} \rfloor, N \times M) \end{cases} \tag{1}$$

The user's command behavior and stored data will be encrypted with the generated key. The introduction of the 4D-Yoz hyperchaotic system effectively expands and strengthens the original digital biological key and key pool, thereby providing an additional layer of security.

IV. Restrictive entropy bio-code generator

This section will introduce the proposed Re-BCG, a constrained entropy biometric key generator, and its specific application in the agreement and IoAV.

Conventional fingerprint identification technology employs the use of fingerprint data for the purpose of identifying individuals, following the initial processing and storage of said data within a database. Presently, there exists a relatively mature technology for single-fingerprint authentication, including the use of fingerprint feature templates and fingerprint blurring extractors for the purpose of identity recognition. Despite the remarkable complexity of the human condition, the biological characteristics of the species are, in fact, quite limited. For example, the human body is equipped with ten fingers. Even in the absence of any loss or leakage of fingerprint information, there are only 10 opportunities to utilise different fingers to update authentication credentials, which is insufficient to meet the requirements of an identity authentication system that requires regular updates to authentication credentials. Furthermore, it is challenging to achieve the necessary level of data encryption complexity. Furthermore, biometric templates stored in both local and cloud-based systems are susceptible to attack. Any alteration or theft of these templates will result in the irreversible loss of personal identity on the Internet.

Simultaneously, to guarantee the typical functioning of the recognition system in the presence of noise, the biometric template is typically designed to exhibit high noise tolerance. However, the intrinsic characteristics of the fingerprint, namely "feature aggregation" present a challenge in characterizing the feature points and utilizing the aggregated feature vectors for recognition. This, in turn, impairs the specificity of the biometric feature. This paper employs cosine similarity for modeling and vector constraint, thereby reducing the number of low-quality feature points that must be utilized while maintaining noise tolerance. This approach circumvents the constraints on recognition and key generation that result from high information entropy.

To address these issues, this paper proposes the design of a constrained entropy biological cryptographic generator, designated Re-BCG. The specific implementation steps are outlined as follows:

1) Image preprocessing: Construct a multi-fingerprint tuple $F = f_1, f_2, f_3, ..., f_k$, and before the fingerprint image enters the tuple, go through the following processing steps:

a) : Sharpening, which increases the contrast of the edges of the image and accentuates the ridges.

b) : Frequency domain processing: Analyze and process frequency domain characteristics and remove noise.

c) : Texture segmentation, which analyzes the fingerprint image for texture and highlights important features.

d) : Gradient direction analysis to obtain the ridge line direction.

At the same time, in order to ensure the robustness of the generated key, morphological denoising is performed to construct a threshold t. For the ridge pixel set $numPixels(i)$ of the fingerprint, the part with a connected domain smaller than the threshold is removed, and at the same time, by obtaining the inverted color image, the part with a connected domain larger than the threshold is found, and the inverted color island is removed and the black hole is filled. At the same time, during the experiment, many pseudo-points were found, such as bridge points and burr points. The matrix is defined as follows:

$$\begin{aligned} Interval1 &= \begin{bmatrix} 0 & -1 & -1 \\ 1 & 1 & -1 \\ 0 & -1 & -1 \end{bmatrix} \\ Interval2 &= \begin{bmatrix} -1 & -1 & -1 \\ -1 & 1 & -1 \\ 0 & 1 & 0 \end{bmatrix} \\ &\vdots \\ Interval8 &= \begin{bmatrix} -1 & -1 & 1 \\ -1 & 1 & -1 \\ -1 & -1 & -1 \end{bmatrix} \end{aligned} \tag{2}$$

The positive and negative colors of the bridge connection points should be connected, and the burr points should be removed simultaneously. Subsequent to this, a stable binary image of the fingerprint is obtained, and the tolerance threshold t of the fingerprint is determined.

2) Feature point acquisition: Construct a 3×3 matrix describing the features. For any fingerprint feature point, I, the set of points in the surrounding space is $I_1, I_2, I_3, ..., I_9$. Calculate the difference between any two adjacent pixels I_1 and I_2. When the distance between any two 3×3 spatial points

in an image is 6 units, the point is a cross point, and when the distance is 2 units, the point is an endpoint.

$$\forall I_i \in f, cn(a) = \sum_{i=1\ldots 9} |I(a_{imod8}) - I(a_{i-1})| \quad (3)$$

3) Feature modeling: In the case of a single fingerprint image, the center point K_p of the fingerprint is taken as the reference point. It is expected that different images will exhibit similar fingerprint center points. The Euclidean distance r between I_i and K_p is calculated, and the relative angle θ and cosine similarity $Simcos$ are used to construct the feature similarity value ϑ, as demonstrated in the following formula. The ten points with the highest ϑ are then extracted as the optimal points to be matched and grouped into a tuple. This process is repeated for any two input fingerprint images.

$$\vartheta = \sqrt{(r_i[\frac{(\theta\pi)}{180}]) \times Simcos_i} \quad (4)$$

4) Feature point merging: For any matching feature point $I_i = (x_i, y_i)$, the high-order matching points of any two fingerprint images form a feature point matrix, which records the rotation intersections. For any two fingerprint images, a group of similar points a_{xi}, b_{yi} within the tolerance threshold t is selected to form a key matrix. In the event that a key matrix of different sizes is required, the matrix can be constructed into an $N \times M$ size through reconstruction.

$$\delta = \begin{bmatrix} a_{x1} & a_{y1} \\ b_{x1} & b_{y2} \end{bmatrix} \times \begin{bmatrix} N_{xn} & N_{yn} \\ M_{xn} & M_{yn} \end{bmatrix} \times cos(\theta_{a,b}) \times cos(\theta_{N,M}) \quad (5)$$

5) Biological code generation: For disparate biological keys, a random key K is generated by obtaining the 4D-Yoz hyperchaotic system; thereafter, the matrix determinant is calculated to yield a random matrix. This random matrix is then employed to derive the random key.

$$\begin{cases} \delta'_x = \delta \times \mod(\lfloor Y_{ox} \times 10^{15} \rfloor, N \times \delta) \\ \delta'_y = \delta \times \mod(\lfloor Y_{oy} \times 10^{15} \rfloor, N \times \delta) \\ \delta'_z = \delta \times \mod(\lfloor Y_{oz} \times 10^{15} \rfloor, N \times \delta) \\ \delta'_w = \delta \times \mod(\lfloor Y_{ow} \times 10^{15} \rfloor, N \times \delta) \end{cases} \quad (6)$$

V. The Proposed Internet of Vehicles Image Encryption Algorithm

In response to the necessity for an expansion of the key pool in key agreement and the necessity for an investigation of user behavior under "one time pad" protection, the existing three-dimensional chaotic system was improved to a four-dimensional hyperchaotic system. Additionally, an image encryption storage algorithm based on L_∞ measurement and matrix semi-tensor product was designed, as described in the following section.

A. Chaos system

1) Rucklidge Chaos System: In recent years, numerous three-dimensional chaotic systems have been proposed, including the Chen system, the Lorenz system, and the Rosslor system [41], [42]. Some scholars have indicated that the introduction of nonlinear terms into the equation may result in the emergence of two or more coexisting chaotic attractors. Xuebing Zhang incorporated a cross-product nonlinear term into the Rucklidge system [43], leading to the establishment of a novel three-dimensional autonomous system, which is expressed as follows:

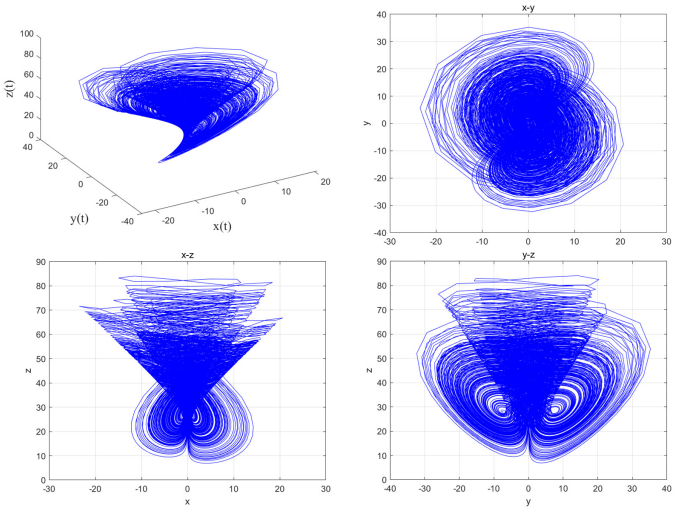

Fig. 3. Phase diagrams of the original Rucklidge chaotic system displaying chaotic trajectories across different planes.

$$\begin{cases} \dot{x} = -ax + by - yz \\ \dot{y} = x + xz \\ \dot{z} = -cz + y^2 \end{cases} \quad (7)$$

The system has been numerically simulated with parameters $a = 10, b = 28$, and $c = 2$, and it has been demonstrated that there are three real equilibrium points. In particular, the equilibrium point $S = (0, -7.4833, 28)$ exhibits excellent chaotic behavior. The dynamics of such a system can be visualized by means of a phase portrait, which reveals the complex trajectory of the system state over time. The resulting phase portrait is shown in Figure 3.

2) 4D-Yoz Hyperchaotic System: Based on the aforementioned chaotic system, this paper constructs a 4D-Yoz hyperchaotic system that demonstrates high dynamic complexity and a wide parameter control range. To achieve this, a nonlinear controller action model is established, a nonlinear controller is introduced, feedback paths and square terms are added, and a cosine function is included in the second and fourth terms. The system can be expressed as follows:

$$\begin{cases} \dot{x} = -ax + ay + sin(y) + ew \\ \dot{y} = -xz + sin(z) + dx + cy + nsin(2w) \\ \dot{z} = mxy^3 - bz \\ \dot{w} = (n+1)y + kx + ncos(z) \end{cases} \quad (8)$$

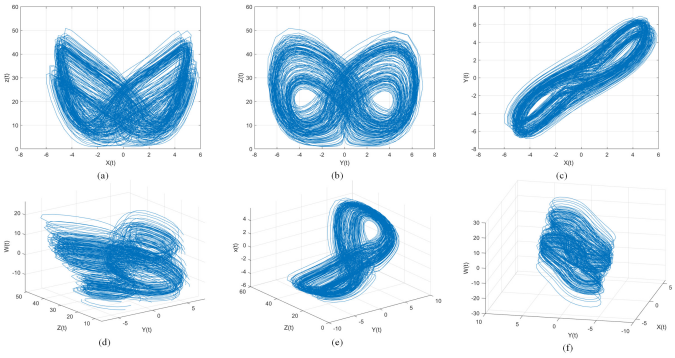

Fig. 4. Phase portraits of the improved 4D-Yoz hyperchaotic system demonstrating enhanced chaotic characteristics and complex trajectories.

When x = 1, y = 1, z = 2, and w = 4, the phase diagram of the 4D-Yoz hyperchaotic system is shown in Figure 4.

In ensuring the high chaotic performance of the proposed chaotic system, this paper employs an analysis of the Lyapunov exponents of the system. The Lyapunov exponent represents an effective methodology for the determination of chaotic behavior in a given system. The primary attributes of a nonlinear dynamical system can be quantified by the number of positive Lyapunov exponents. A system exhibiting a single positive Lyapunov exponent is deemed to be chaotic. A system exhibiting two or more positive Lyapunov exponents is deemed to be exhibiting hyperchaotic behavior. When the aforementioned parameters are set to a=37, b=8.5, c=18, d=2, k=5, e=2.5, n=4, and m=1, the corresponding Lyapunov exponents are L1=31.67, L2=9.94, L3=5.5, and L4=-40, indicating that the system exhibits hyperchaotic behavior. Furthermore, a comparison with the original chaotic system reveals that our system exhibits heightened chaotic characteristics.

The bifurcation diagram elucidates the alterations in the system's dynamic behavior when the parameters undergo changes, such as period doubling and chaotic windows. Figure 5 depicts the bifurcation diagram and lyapunov exponent of the proposed chaotic system in comparison with the original system. It is evident that the 4D-Yoz hyperchaotic system displays a more expansive chaotic period and superior chaotic performance.

B. Scrambling algorithm based on Chevshcherby metric and pixel rotation

This section presents the image encryption algorithm proposed in this paper. The pseudo-code is shown in Algorithm 1, which contains the image shuffling and diffusion processes. The subsequent subsections provide detailed descriptions and justifications for each step.

1) istance metrics: Let $X = \{x_1, x_2, ..., x_n\}$, $Y = \{y_1, y_2, ..., y_n\}$ and the distance between X and Y be calculated by different formulas. A common formula for the Euclidean distance in n-dimensional space is:

$$d(x,y) = \sqrt{\sum_{i=1}^{n} \times (x_i - y_i)^2} \tag{9}$$

Different distance metrics can reflect different relationships between data. For example, Euclidean distance reflects the

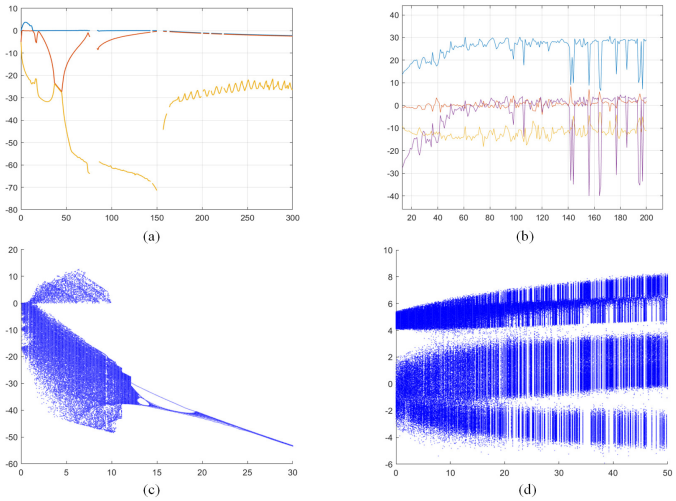

Fig. 5. Performance analysis comparison: (a) Lyapunov exponent of the chaotic system before improvement; (b) 4D-Yoz hyperchaotic system Lyapunov exponent analysis; (c) bifurcation structure of the chaotic system before improvement; (d) bifurcation structure of the 4D-Yoz hyperchaotic system.

Algorithm 1 Image Encryption Algorithm for IoAV

Require: Original image I, biometric key matrix M, 4D-Yoz sequences Yo_x, Yo_y, Yo_z, Yo_w
Ensure: Encrypted image I_e

Step 1: Scrambling phase using L_∞ metric
Find GCD G of image width and height
Initialize scanning element matrix of size $G \times G$
for each $G \times G$ block in image **do**
  for each pixel at position (i, j) in block **do**
    Calculate Chebyshev distance using Eq. (11)
    Set polar coordinates: $\rho = \sqrt{x^2 + y^2}$, $\theta = \arctan(y/x)$
    Calculate K value using Eq. (13)
  end for
  Sort pixels by K values in descending order
  Rearrange pixels clockwise if G is even, counterclockwise if odd
  Calculate block expansion based on mean pixel values
  Repeat scrambling process on expanded blocks
end for
Step 2: Diffusion phase using Semi-Tensor Product
Divide scrambled image into 2^5 blocks $\{P_1, P_2, ..., P_{32}\}$
for each block P_i **do**
  Calculate mean gray value $Gray$ for block
  Set rotation angle Θ using Eq. (19)
  Reconstruct matrix $M \times \Theta$ based on rotation angle
  Apply semi-tensor product: $P_i \times$ [random matrix]
end for
Combine processed blocks to form encrypted image I_e
return I_e

situation where the individual component measures of a sample vector are standardized, while normalized Euclidean distance quantifies the differences between different attributes in the same interval by assigning different weights to different attributes of different components. Improve the application effect.

$$d(x,y)' = \sqrt{\sum_{i=1}^{n} (y_i - x_i)^2 / s_i} \tag{10}$$

In order to achieve improved disambiguation, the L_∞ measure, or Chebyshev distance, is employed. This metric is derived from the uniform norm and represents a type of hyperconvex metric (injective matric space). In the case of grid matrices, the Chebyshev distance between two points is defined as the absolute difference between their respective coordinate data.

2) isordering process: The relative position of pixels is determined by measuring the distance between pixels. During the recursion process, a polar coordinate system is established, with the origin at the corner points of the meta-matrix. The pixel blocks are indexed by the associated randomly sized metamatrix and rearranged based on parity differences according to the polar radian and the L_∞ metric for the required K value. Due to the random correlation of the metamatrix expansion, the polar coordinate modeling and L_∞ metric rearrangement in the recursive process are also highly random and complex, which can effectively destroy the correlation between pixels. The specific steps are shown below:

a) : The initial stage of the procedure entails identifying the greatest common divisor (G) of the image's width and height. This is followed by the initialization of the scanning element matrix with $G \times G$. This step serves to define the underlying units and the range of subsequent operations.

b) : The Chebyshev distance between each pixel in the block and the coordinate position of (G, G) is calculated for all pixels in the range of $G \times G$, starting from the position of pixel $(1, 1)$. Based on the polar coordinate system, further transformations and calculations are performed to construct the K-value calculation formula.

$$Q_{A,B} = \max |X_{1i} - X_{2i}| = \lim_{P \to N} \left(\sum_{i=1}^{N} |X_{1i} - X_{2i}|^P \right)^{\frac{1}{P}} \tag{11}$$

Where polar coordinates are modeled based on the point (G, G) pixel as the center, defined as:

$$\begin{cases} x = \rho \cos(\theta) \\ y = \rho \sin(\theta) \end{cases} \tag{12}$$

where $\rho = \sqrt{x^2 + y^2}, \quad \theta = \arctan\left(\frac{y}{x}\right)$

$$K = \frac{Q_{A,B} \times \arccos(\cos(\theta_x) + \cos(\theta_y)) \times \pi}{180} \tag{13}$$

c) : In the case of the pixels within the scan element matrix, the pixels are rearranged in descending order based on the magnitude of K. In the event that G is even, the pixels are rearranged in a clockwise manner. Conversely, when G is odd, the pixels are arranged in a counterclockwise fashion.

d) : Following the completion of the aforementioned rearrangement, a random block expansion is calculated based on the pixel mean values of the swept pixel blocks, as delineated by the scanning element matrix, with the objective of adjusting the size of the aforementioned matrix. Thereafter, steps b) to d) are repeated for the adjusted matrix, with the aim of further disordering the image.

The process may be repeated as many times as necessary. Experimental evidence indicates that when the number of iterations is set to a value between two and four times the original value, the algorithm is able to achieve a more optimal level of disarray and enhance the security of the image.

C. Diffusion Algorithm for Matrix Semi-Tensor Products Coupled to Biological Keys

To protect the image data stored in the cloud, an effective disambiguation algorithm is designed to generate the original semi-tensor product random matrix by Re-BCG with the 4D-Yoz hyperchaotic system. The matrix is then divided into 2^5 blocks, thereby dividing the set of images. The chunks $\{P_1, P_2, ..., P_{32}\}$ are subjected to semi-tensor product calculations, which are then followed by the rotation of the semi-tensor product random matrix in accordance with the average pixel gray level value across the different chunks. This process is repeated until all chunks have been processed sequentially.

1) matrix semi-tensor product: In 2021, Cheng et al [44]. introduced the matrix Semi-Tensor Product (STP), initially designed for high-dimensional arrays. Due to its robust arithmetic capability, STP is capable of solving multilinear and nonlinear mathematical problems and has since been adopted as a general matrix multiplication method. This approach circumvents the dimensional constraints of conventional matrix multiplication, enabling operations on arbitrary matrices while maintaining their intrinsic characteristics, thereby enhancing adaptability and flexibility. Chai et al [45]. observed that if the matrix and multiplication processes are reversible, they can be integrated into a unified process, which is applicable to image encryption. Simulation outcomes substantiate the efficacy of this methodology. The STP theory of the matrix can be delineated as follows:

a) : Let $A = a_{ij} \in M_{m \times n}$, $B = (b_{ij} \in M_{s \times t})$. The tensor product of A and B can be expressed as:

$$A \otimes B = \begin{bmatrix} a_{11}B & a_{12}B & \cdots & a_{1n}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1}B & a_{m2}B & \cdots & a_{mn}B \end{bmatrix} \tag{14}$$

where, $\otimes$ denotes the sign of the tensor product.

Assumption 1: If t is a factor of s and $s = t \times n$, then the n-dimensional row vector has:

$$\langle X, Y \rangle_{L_i} = \sum_{k=1}^{t} X^k Y_k \in \mathbb{R}^n \tag{15}$$

This is referred to as the left matrix semi-tensor product of X and Y, where X is represented by the vector $[x_1, x_2, \ldots, x_s]$.

Assumption 2: If s is a factor of t, $t = s \times n$, then this dimensional row vector has:

$$\langle X, Y \rangle_{L_i} = \left(\langle Y^T, X^T \rangle_L \right)^T \in \mathbb{R}^n \tag{16}$$

b) : Suppose $M \in M_{m \times n}$, $N \in M_{p \times q}$. If n is a factor of p or p is a factor of n, then $C = M \ltimes N$ is the left matrix semi-tensor product of M and N. If C consists of $M \times N$ blocks, $C = \langle C^{ij} \rangle$ and $C^{ij} = \langle M^i, N_j \rangle_L$, where $i = 1, 2, \ldots, j = 1, 2, \ldots, q$.

Define:

$$A \ltimes B = A(B \otimes I_n) \tag{17}$$

c) : If $A \in M_{m\times np}$, $B \in M_{p\times q}$, then define:

$$A \ltimes B = (A \otimes I_p)B \tag{18}$$

Here, I_n and I_p are the identity matrices of order n and p respectively.

The mathematical foundations underlying Assumptions 1 and 2 are derived from the theoretical framework of left matrix semi-tensor products as established by Zou et al. [44]. These assumptions are essential for ensuring dimensional compatibility during the diffusion operation, where the matrix multiplication requires specific size relationships between operands. The constraint that t divides s (or vice versa) guarantees that the semi-tensor product operations remain well-defined throughout the encryption process.

The selection of $2^5 = 32$ image blocks in our diffusion algorithm is strategically chosen to optimize the semi-tensor product calculations while maintaining computational efficiency. This block size configuration aligns with established practices in chaos-based image encryption systems and ensures optimal utilization of the 4D-Yoz hyperchaotic sequence properties.

2) The Process Of Diffusion: The following text describes the matrix semi-tensor product algorithm that has been devised for use in image diffusion. The text then goes on to set out the steps that need to be taken to implement the algorithm, together with the corresponding mathematical expressions.

a) : For an image of size $m\times n$, the image is divided into 2^5 blocks to form the image chunk set $\{P_1, P_2, \ldots, P_{32}\}$. The semi-tensor product operation, i.e., $P_1 \ltimes \mathcal{M}$, is then performed for each block P_1.

b) : For each image chunk, the gray mean value (denoted as Gray) is calculated for each pixel, and the rotation angle (denoted as Θ) is determined.

$$\Theta = (\lfloor \text{Gray} \mod 4 \rfloor \times 90) \times \frac{\pi}{180} \tag{19}$$

c) : For each chunk, reconstruct the random matrix $M \times \Theta$ according to its rotation angle Θ.

d) : The semi-tensor product of random matrices is computed for the set of chunks as follows:

$$P_i \times \begin{bmatrix} a_{11}B & a_{12}B & \cdots & a_{1n}B \\ \vdots & \vdots & \ddots & \vdots \\ n_{81}B & n_{82}B & \cdots & n_{88}B \end{bmatrix} \tag{20}$$

In the aforementioned matrix, the variable B represents a block that has been adjusted based on the rotation angle, denoted by the variable Θ. The variables a_{ij} and n_{ij} have been generated based on the encryption key.

D. Decryption Algorithm

The article employs a standard symmetric algorithm design, whereby the decryption process is the inverse of the encryption process. The specific pseudo-code is shown in Algorithm 2.

The decryption procedure consists of two primary phases that reverse the encryption operations in sequential order.

Algorithm 2 Image Decryption Algorithm for IoAV

Require: Encrypted image I_e, biometric key matrix M, 4D-Yoz sequences Yo_x, Yo_y, Yo_z, Yo_w
Ensure: Decrypted image I
Step 1: Inverse diffusion phase
Divide encrypted image into 2^5 blocks $\{P_1, P_2, ..., P_{32}\}$
for each block P_i **do**
  Calculate mean gray value and set rotation angle Θ using Eq. (19)
  Reconstruct matrix $M \times \Theta$ and apply inverse semi-tensor product
end for
Combine all blocks to form scrambled image I_s
Step 2: Inverse scrambling phase
Find GCD G of image dimensions and initialize scanning matrix
for each $G \times G$ block in scrambled image **do**
  Calculate block expansion based on pixel mean values
  Compute Chebyshev distances and K values using Eqs. (11)(13)
  Sort pixels by K values in descending order
  if G is even **then**
    Rearrange pixels counterclockwise (reverse of encryption)
  else
    Rearrange pixels clockwise (reverse of encryption)
  end if
  Process inverse block expansion transformation
end for
return Decrypted image I

1) Inverse Diffusion Phase: For each encrypted image block P_i, the rotation angle is reconstructed using Equation (19), and the inverse semi-tensor product operation is applied:

$$P_i^{-1} = P_i \ltimes [M \times \Theta]^{-1} \tag{21}$$

where $[M \times \Theta]^{-1}$ represents the inverse of the rotated biometric key matrix.

2) Inverse Scrambling Phase: The scrambling reversal process reconstructs the polar coordinate system and recalculates the K values using Equation (13). The inverse pixel rearrangement follows:

$$P_{inverse}(i,j) = P_{scrambled}(K_{sorted}^{-1}[i,j]) \tag{22}$$

where K_{sorted}^{-1} represents the inverse permutation of the sorted K values. The inverse block expansion operation is given by:

$$G_{new} = \frac{G_{original}}{expansion\_factor} \tag{23}$$

This symmetric design ensures complete restoration of the original image while maintaining cryptographic integrity.

VI. Security Adversaries in TP-IoAV

In this paper, to verify the security of the TP-IoAV protocol, a hierarchical threat model is constructed according to the Kerckhoffs principle [46] of modern cryptography, which assumes that the details of the algorithm and the structure of the system are completely transparent to the attacker, and that security is ensured only by the confidentiality of the key. The threat model employs a cumulative authority structure, whereby a high-level attacker automatically gains all the capabilities of a low-level attacker.

- **External Threat Attacker:** Attackers operating exclusively through public communication channels. They conduct passive eavesdropping, analyze encrypted traffic statistics, attempt cryptanalysis against the 4D-Yoz hyperchaotic system through differential, correlation, or brute-force methods, execute man-in-the-middle attacks to manipulate vehicle-user-cloud communications, and perform replay attacks to circumvent the 'one-time-one-key' mechanism.
- **Internal Threat Attacker:** Entities with legitimate partial system access. Beyond external attacker capabilities, they can breach cloud servers to access encrypted data and key management functions, attempt unauthorized access to biometric key pools to compromise the Re-BCG mechanism, and control vehicle terminals to extract sensitive road condition imagery and GPS data. Their legitimate access credentials render conventional security controls less effective.
- **Advanced Persistent Threat (APT):** Sophisticated attackers with comprehensive capabilities and substantial resources. They execute multi-stage infiltrations with privilege escalation, apply machine learning to predict or forge biometric templates, and reconstruct chaotic system parameters through ciphertext analysis. These long-term, targeted operations aim to compromise the L_∞ metric and matrix semi-tensor product encryption algorithms or undermine the tri-party communication protocol integrity.

Our threat model is constructed following Kerckhoffs's principle [46], a fundamental tenet of modern cryptographic analysis that assumes complete transparency of the cryptographic algorithm and system architecture to potential adversaries. Under this principle, security relies exclusively on the secrecy of cryptographic keys rather than the obscurity of the algorithm design. This assumption provides the most rigorous security evaluation framework, as it considers worst-case scenarios where attackers possess full knowledge of the TP-IoAV protocol structure, the 4D-Yoz hyperchaotic system parameters, and the Re-BCG implementation details. By adopting Kerckhoffs's principle, we ensure that our security analysis represents realistic threat conditions and that the proposed scheme can withstand attacks even when the system design is publicly known.

VII. Experimental simulation and performance analysis

Four route images, a surveillance image, a vehicle image, and different fingerprint images were selected as the test images, designated as 01, 02, 03, and 04, respectively. The plaintext remote sensing grayscale image presented in Figure 6 represents the corresponding ciphertext image obtained through the application of our encryption scheme. The decrypted image, in turn, represents the corresponding decrypted image. As illustrated in the figure, the encrypted images are all noise-like images devoid of any visual information leakage, while the decrypted images are identical to the specific corresponding plaintext images, thereby demonstrating the efficacy of our proposed image cryptosystem.

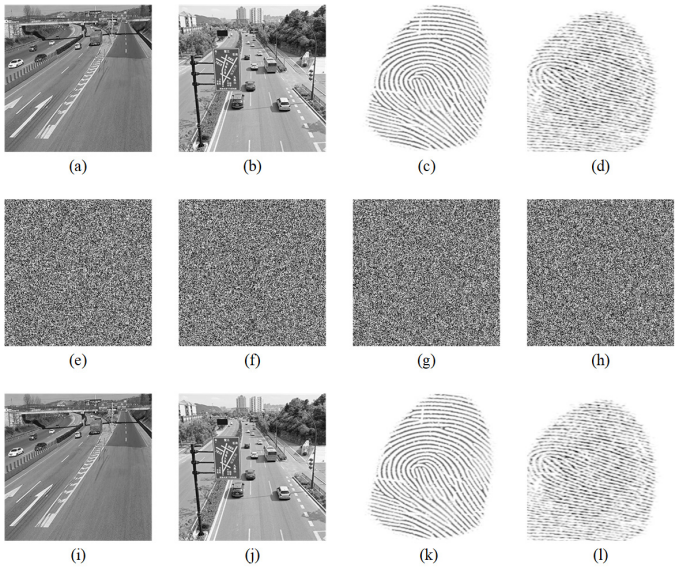

Fig. 6. Encryption results: (a-b) Original road images; (c-d) Original fingerprints; (e-h) Encrypted images; (i-l) Decrypted images.

A. Key Space Analysis

The key space is defined as the geometry of all keys that can be generated by an encryption algorithm. In order to resist various brute-force attacks, it is recommended that the key space of a high-security cryptosystem be no less than 2^{100}. In the encryption algorithm under consideration, the key is composed of the key matrix generated by Ce-BKG and the initial value and parameters of the 4D-Yoz hyperchaotic system. In the event that the computer's calculation accuracy is set to 10^{-16}, the key space of this method is 2^{576}, which is considerably larger than the required value. As demonstrated in Table II, this algorithm significantly expands the key space, ensuring sufficient capacity to withstand brute-force attacks.

TABLE II
KEY SPACE ANALYSIS

Scheme	**Our**	[47]	[48]	[49]
Key Space	2^{576}	2^{104}	2^{408}	2^{425}

B. Histogram analysis

A histogram is a graphical representation that illustrates the distribution of gray values in an image, indicating the relative frequencies of each value. The presence of a uniform histogram in an encrypted image indicates that the image in question is capable of effectively concealing the statistical properties of the plain-image, thereby enhancing the security of the encryption process. Figure 7 illustrates a comparison of the histograms of the plain-images and its cipher-images. The cipher-image displays a uniform histogram distribution in comparison to the plain-images, thereby demonstrating that the encryption operation effectively disrupts the statistical features of the plain-image. Consequently, the algorithm proposed in this design can effectively prevent attackers from obtaining valuable information by analyzing the statistical data of the

Cipher-image, thus resisting various attack methods based on statistical analysis.

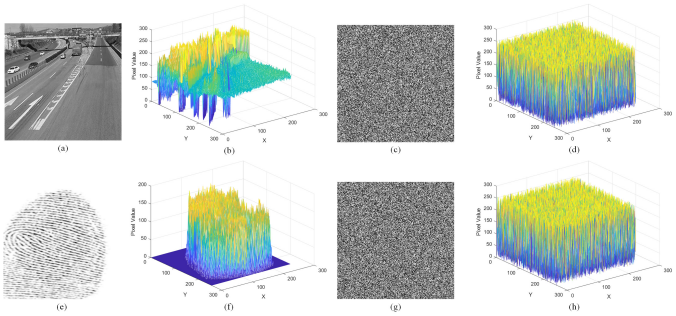

Fig. 7. Histogram analysis: (a,e) original images; (b,f) 3D histograms of originals; (c,g) encrypted images; (d,h) 3D histograms of encrypted images showing uniform distribution.

C. Pixel Correlation Analysis

The image encryption algorithm is designed to break the relationship between pixels. However, in general, adjacent pixels tend to have a strong correlation. To illustrate this phenomenon, 8000 pixel points were selected at random from the 01, 02, and 03 plain-images and their horizontal, vertical, and diagonal pixel correlation diagrams were drawn, as shown in Figure 8. The resulting images demonstrate that the pixels in the plain-images have a strong linear relationship.

To eliminate the potential for randomness, we calculated the mean of 1000 random values by randomly selecting 8000 pixels each time from the plain-image. The resulting data are presented in Table III. The pixel correlation of the plaint-image in the three directions is nearly 1, while the pixel correlation coefficients of the cipher-image are all within 0.05, which substantiates the efficacy of the image encryption algorithm.

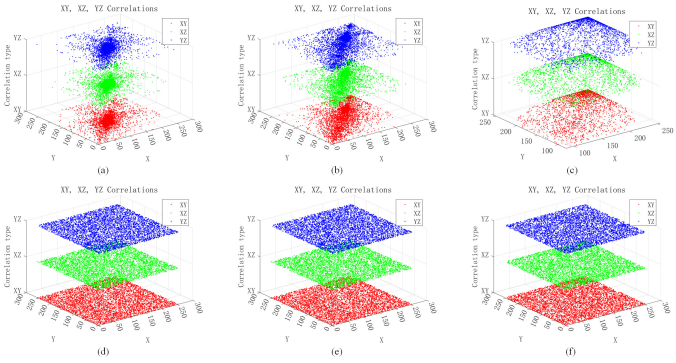

Fig. 8. Pixel correlation: (a-c) original image correlations; (d-f) encrypted image correlations showing effective decorrelation.

D. Information Entropy Analysis

Information entropy analysis is a statistical measure of uncertainty employed to assess the randomness of information in an image. Information entropy can be used to quantify the degree of dispersion of data in an image by measuring the distribution of gray values. Images with high information

TABLE III
PIXEL CORRELATION ANALYSIS

Image	Type	Horizontal	Vertical	Diagonal
Road monitoring	Plain-image	0.7584	0.8057	0.6020
	Cipher-image	0.0053	-0.0202	0.0077
Vehicle-borne	Plain-image	0.8615	0.8561	0.8041
	Cipher-image	-0.0202	-0.0036	0.0007
Fingerprint	Plain-image	0.7593	0.8812	0.7848
	Cipher-image	-0.0046	-0.0378	-0.0079

entropy exhibit a high degree of uncertainty and complexity, indicating a strong randomness in their content. Conversely, more ordered cipher-images typically display lower information entropy. The mathematical expression for information entropy can be defined as follows:

$$H(m) = -\sum_{i=0}^{2^{N-1}} p\left(m_i\right) \log_2 p\left(m_i\right) \tag{24}$$

In the aforementioned formula, N represents the gray level of the image, and $p(m_i)$ is the probability of m_i occurring. The logarithm is taken to the base 2, thus the information entropy is expressed in bits. For an ideal random image with 256 gray levels, the theoretical value of information entropy is 8.

The information entropy of various cipher-images was calculated. Table IV presents the outcomes of the algorithm and a comparison with alternative methodologies. It is evident that the information entropy of the cipher-image is nearly 8, which substantiates the assertion that the cipher-image generated by the algorithm exhibits heightened randomness.

TABLE IV
INFORMATION ENTROPY TEST

Image	Cipher-image
Road monitoring	7.9975
Vehicle-borne	7.9976
Fingerprint-1	7.9975
Fingerprint-2	7.9975
[50]	7.9969
[51]	7.9957

E. Peak Signal-to-Noise Ratio (PSNR) testing

The PSNR is a measure of the distortion of a cipher-image. The PSNR calculation formula is as follows: A lower PSNR value indicates a greater degree of distortion in the cipher-image under examination. When the PSNR is less than 15 dB, it is not possible for an unauthorized individual to obtain any valid information from the test image. The test results are shown in the Table V and the specific calculation formula is as follows:

$$\text{PSNR} = 10 \cdot \log_{10} \frac{MAX}{MSE} \tag{25}$$

F. Differential attack testing

The Number of Pixels Change Rate (NPCR) and the Unified Average Changing Intensity (UACI) can be employed to

TABLE V
PSNR TEST

Image	PSNR
Road monitoring	7.7485
Vehicle-borne	7.7441
Fingerprint-1	9.9157
Fingerprint-2	8.5376
[52]	14.0834
[53]	12.5318
[54]	14.0834

assess the resilience of cipher-images to differential attacks. The anticipated mean value of NPCR is 0.9961, while the anticipated mean value of UACI is 0.3346.

TABLE VI
DIFFERENTIAL ATTACK TEST

Image	NPCR(%)	UACI(%)
Road monitoring	99.5789	33.4635
Vehicle-borne	99.5895	32.3047
Fingerprint-1	99.6399	34.9161
Fingerprint-2	99.6338	33.6384
[55]	99.6521	28.0346
[56]	99.5865	28.0346

G. Security Analysis Against Adversary Models

The experimental results demonstrate the robustness of the TP-IoAV scheme against the proposed hierarchical threat model. Against external threat attackers, the system demonstrates formidable protection through its expansive key space (2^{576}), which effectively negates brute force attacks. Statistical security indicators - uniform histogram distribution, near-zero pixel correlation coefficients (Table III), information entropy values approaching 8 (7.9975-7.9976), and differential attack resistance with NPCR greater than 99.5% - confirm that attackers cannot derive meaningful information through statistical analysis or eavesdropping. In addition, the "one time pad" mechanism implemented via the 4D-Yoz hyperchaotic system renders replay attacks ineffective by ensuring unique authentication session keys.

For internal threat and APT actors, the TP-IoAV architecture implements multiple layers of defence. The Re-BCG mechanism avoids storing original biometric templates and instead generates dynamic key pools from authentication behaviour, while the separation between cloud servers and data centres enforces the principle of least privilege. PSNR values of less than 10 dB (Table V) ensure that encrypted data remains indecipherable even with partial system access. Against sophisticated APTs, the superior properties of the 4D-Yoz hyperchaotic system - demonstrated by multiple positive Lyapunov exponents - combined with multi-fingerprint feature-level reconstruction, create complex non-linear relationships that defy parameter prediction and machine learning-based template reconstruction. L_∞ metric scrambling and matrix semi-tensor product diffusion introduce mathematical complexity that would require prohibitive computational resources to break, confirming that the system provides comprehensive security for the IoAV while maintaining practical performance characteristics.

VIII. CONCLUSION

This paper presents a biometric cryptographic method, Re-BCG, which employs biometrics and chaotic systems, for use in a driverless car networking system. The proposed TP-IoAV is the proposed application for this method. In addition, an image encryption method based on the use of chaotic biometric keys and half-tensor products is also presented. Furthermore, the evaluation of the key's performance enhances the potential applications of the scheme. The optimized four-dimensional hyperchaotic system demonstrates superior chaotic performance compared to the traditional Rucklidge chaotic system, which is well-suited to meet the data protection requirements of driverless cars in the context of the growing volume of data. Furthermore, a three-party key agreement is devised to safeguard the data security associated with the information sharing between the vehicle, the user, and the cloud data center. In addition to utilising biometric recognition behaviour to generate the original key pool, the key pool will be deployed through the cloud to protect the "one time pad" protection for the user's session and confidential data exchange. A security analysis demonstrates that the chaotic biological key encryption scheme not only maintains good information entropy, but also passes the existing attack tests to meet high security requirements.

ACKNOWLEDGMENTS

This work was supported in part by Basic Research Project of Liaoning Provincial Department of Education (JYTQN2023208) and in part by Liaoning Province Guiding City Science and Technology Development Special Project - Liaoning Provincial Natural Science Foundation Joint Plan (20240344).

REFERENCES

[1] S. M. Karim, A. Habbal, S. A. Chaudhry, and A. Irshad, "Architecture, protocols, and security in iov: Taxonomy, analysis, challenges, and solutions," *Security and Communication Networks*, vol. 2022, no. 1, p. 1131479, 2022.

[2] H. Taslimasa, S. Dadkhah, E. C. P. Neto, P. Xiong, S. Ray, and A. A. Ghorbani, "Security issues in internet of vehicles (iov): A comprehensive survey," *Internet of Things*, vol. 22, p. 100809, 2023.

[3] E. Alalwany and I. Mahgoub, "Security and trust management in the internet of vehicles (iov): Challenges and machine learning solutions," *Sensors*, vol. 24, no. 2, p. 368, 2024.

[4] E. Khezri, H. Hassanzadeh, R. O. Yahya, and M. Mir, "Security challenges in internet of vehicles (iov) for its: A survey," *Tsinghua Science and Technology*, vol. 30, no. 4, pp. 1700–1723, 2025.

[5] E. Zavvos, E. H. Gerding, V. Yazdanpanah, C. Maple, S. Stein *et al.*, "Privacy and trust in the internet of vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 8, pp. 10 126–10 141, 2021.

[6] E. Khezri, H. Hassanzadeh, R. O. Yahya, and M. Mir, "Security challenges in internet of vehicles (iov) for its: A survey," *Tsinghua Science and Technology*, vol. 30, no. 4, pp. 1700–1723, 2025.

[7] S. R. Milford, B. S. Elger, and D. M. Shaw, "Believe me! why tesla's recent alleged malfunction further highlights the need for transparent dialogue," *Frontiers in Future Transportation*, vol. 4, p. 1137469, 2023.

[8] N. E. Boudette, "'it happened so fast': Inside a fatal tesla autopilot accident." *International New York Times*, pp. NA–NA, 2021.

[9] I. Ahmed, M. Ahmad, M. U. R. Siddiqi, A. Chehri, and G. Jeon, "Towards ai-powered edge intelligence for object detection in self-driving cars: Enhancing iov efficiency and safety," *IEEE Internet of Things Journal*, 2025.

[10] H. Taslimasa, S. Dadkhah, E. C. P. Neto, P. Xiong, S. Ray, and A. A. Ghorbani, "Security issues in internet of vehicles (iov): A comprehensive survey," *Internet of Things*, vol. 22, p. 100809, 2023.

[11] G. Manogaran, B. S. Rawal, V. Saravanan, P. MK, Q. Xin, and P. Shakeel, "Token-based authorization and authentication for secure internet of vehicles communication," *ACM Transactions on Internet Technology*, vol. 22, no. 4, pp. 1–20, 2023.

[12] S. Sharma and B. Kaushik, "A survey on internet of vehicles: Applications, security issues & solutions," *Vehicular Communications*, vol. 20, p. 100182, 2019.

[13] Q. Jiang, N. Zhang, J. Ni, J. Ma, X. Ma, and K.-K. R. Choo, "Unified biometric privacy preserving three-factor authentication and key agreement for cloud-assisted autonomous vehicles," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 9, pp. 9390–9401, 2020.

[14] M. Kaur, S. Sofat, and D. Saraswat, "Template and database security in biometrics systems: A challenging task," *International Journal of Computer Applications*, vol. 4, no. 5, pp. 1–5, 2010.

[15] L. Zeng, P. Shen, X. Zhu, X. Tian, and C. Chen, "A review of privacy-preserving biometric identification and authentication protocols," *Computers & Security*, p. 104309, 2025.

[16] H. Almomani, A. Alsarhan, M. AlJamal, M. Aljaidi, T. Alsarhan, B. Khassawneh, A. Alfaqih, G. Samara, and M. K. Singla, "Securing internet of vehicles iov communications: A biometric and hash-key derivation function hkdf-based approach," in *2024 25th International Arab Conference on Information Technology (ACIT)*. IEEE, 2024, pp. 1–7.

[17] L. Wu, Q. Sun, X. Wang, J. Wang, S. Yu, Y. Zou, B. Liu, and Z. Zhu, "An efficient privacy-preserving mutual authentication scheme for secure v2v communication in vehicular ad hoc network," *IEEE access*, vol. 7, pp. 55 050–55 063, 2019.

[18] X. Feng, K. Cui, L. Wang, Z. Liu, and J. Ma, "Pbag: A privacy-preserving blockchain-based authentication protocol with global-updated commitment in iovs," *IEEE Transactions on Intelligent Transportation Systems*, 2024.

[19] H. Xiong, T. Yao, Y. Zhao, L. Gong, and K.-H. Yeh, "A conditional privacy-preserving mutual authentication protocol with fine-grained forward and backward security in iov," *IEEE Transactions on Intelligent Transportation Systems*, 2024.

[20] J. Miao, Z. Wang, X. Ning, A. Shankar, C. Maple, and J. J. Rodrigues, "A uav-assisted authentication protocol for internet of vehicles," *IEEE Transactions on Intelligent Transportation Systems*, 2024.

[21] J. Cui, J. Yu, H. Zhong, L. Wei, and L. Liu, "Chaotic map-based authentication scheme using physical unclonable function for internet of autonomous vehicle," *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 3, pp. 3167–3181, 2022.

[22] P. Santikellur, A. Bhattacharyay, and R. S. Chakraborty, "Deep learning based model building attacks on arbiter puf compositions," *Cryptology ePrint Archive*, 2019.

[23] R. Yashiro, T. Machida, M. Iwamoto, and K. Sakiyama, "Deep-learning-based security evaluation on authentication systems using arbiter puf and its variants," in *Advances in Information and Computer Security: 11th International Workshop on Security, IWSEC 2016, Tokyo, Japan, September 12-14, 2016, Proceedings 11*. Springer, 2016, pp. 267–285.

[24] K. T. Mursi, B. Thapaliya, Y. Zhuang, A. O. Aseeri, and M. S. Alkatheiri, "A fast deep learning method for security vulnerability study of xor pufs," *Electronics*, vol. 9, no. 10, p. 1715, 2020.

[25] K. Gu, K. Wang, X. Li, and W. Jia, "Multi-fogs-based traceable privacy-preserving scheme for vehicular identity in internet of vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 8, pp. 12 544–12 561, 2021.

[26] S. Rane, Y. Wang, S. C. Draper, and P. Ishwar, "Secure biometrics: Concepts, authentication architectures, and challenges," *IEEE Signal Processing Magazine*, vol. 30, no. 5, pp. 51–64, 2013.

[27] A. Sengupta, R. Chaurasia, and A. Anshul, "Robust security of hardware accelerators using protein molecular biometric signature and facial biometric encryption key," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 31, no. 6, pp. 826–839, 2023.

[28] H. Liu, L. Teng, S. Unar, P. Liu, and X. Wang, "Fingerprint image encryption based on chaos and nonlinear dynamic "x" model diffusion," *Journal of Information Security and Applications*, vol. 82, p. 103723, 2024.

[29] R. Subramanian, S. Çiçek, A. Akgul, G. Adam, A. Karthikeyan, and K. Rajagopal, "Dynamical analysis of a quadratic megastable chaotic oscillator and its application in biometric fingerprint image encryption," *Complexity*, vol. 2024, no. 1, p. 2005801, 2024.

[30] F.-Y. Wang, "Parallel control and management for intelligent transportation systems: Concepts, architectures, and applications," *IEEE transactions on intelligent transportation systems*, vol. 11, no. 3, pp. 630–638, 2010.

[31] T. ETSI, "Intelligent transport systems (its); vehicular communications; basic set of applications," *Definitions. Technical Report 102 638, Tech. Rep.*, 2009.

[32] Y. Zhang, Y. Li, R. Wang, J. Lu, X. Ma, and M. Qiu, "Psac: Proactive sequence-aware content caching via deep learning at the network edge," *IEEE Transactions on Network Science and Engineering*, vol. 7, no. 4, pp. 2145–2154, 2020.

[33] H. Lu, Y. Zhang, Y. Li, C. Jiang, and H. Abbas, "User-oriented virtual mobile network resource management for vehicle communications," *IEEE transactions on intelligent transportation systems*, vol. 22, no. 6, pp. 3521–3532, 2020.

[34] M. S. Rathore, M. Poongodi, P. Saurabh, U. K. Lilhore, S. Bourouis, W. Alhakami, J. Osamor, and M. Hamdi, "A novel trust-based security and privacy model for internet of vehicles using encryption and steganography," *Computers and Electrical Engineering*, vol. 102, p. 108205, 2022.

[35] X. Chai, Y. Chen, and L. Broyde, "A novel chaos-based image encryption algorithm using dna sequence operations," *Optics and Lasers in engineering*, vol. 88, pp. 197–213, 2017.

[36] J. Zhang, "An image encryption scheme based on cat map and hyperchaotic lorenz system," in *2015 IEEE International Conference on Computational Intelligence & Communication Technology*. IEEE, 2015, pp. 78–82.

[37] A. K. Singh, K. Chatterjee, and A. Singh, "An image security model based on chaos and dna cryptography for iiot images," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 2, pp. 1957–1964, 2022.

[38] H. Huang and Z. Cai, "Duple color image encryption system based on 3-d nonequilateral arnold transform for iiot," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 7, pp. 8285–8294, 2022.

[39] Y. Sun, K. Yu, A. K. Bashir, and X. Liao, "Bl-iea: A bit-level image encryption algorithm for cognitive services in intelligent transportation systems," *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 1, pp. 1062–1074, 2021.

[40] K. Muhammad, R. Hamza, J. Ahmad, J. Lloret, H. Wang, and S. W. Baik, "Secure surveillance framework for iot systems using probabilistic image encryption," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3679–3689, 2018.

[41] M. Yassen, "Chaos control of chen chaotic dynamical system," *Chaos, Solitons & Fractals*, vol. 15, no. 2, pp. 271–283, 2003.

[42] Y. Li, G. Chen, and W. K.-S. Tang, "Controlling a unified chaotic system to hyperchaotic," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 52, no. 4, pp. 204–207, 2005.

[43] X. Zhang, H. Zhu, and H. Yao, "Analysis of a new three-dimensional chaotic system," *Nonlinear Dynamics*, vol. 67, pp. 335–343, 2012.

[44] C. Zou, X. Wang, and H. Li, "Image encryption algorithm with matrix semi-tensor product," *Nonlinear Dynamics*, vol. 105, no. 1, pp. 859–876, 2021.

[45] X. Chai, X. Zhi, Z. Gan, Y. Zhang, Y. Chen, and J. Fu, "Combining improved genetic algorithm and matrix semi-tensor product (stp) in color image encryption," *Signal Processing*, vol. 183, p. 108041, 2021.

[46] A. Kerckhoffs, *La cryptographie militaire*. BoD–Books on Demand, 2023.

[47] X. Lu and W. Song, "Improved trajectory data encryption method for internet of vehicles using gan-based chaotic logistic algorithm," *Alexandria Engineering Journal*, vol. 114, pp. 719–727, 2025.

[48] M. Gao, J. Li, X. Di, X. Li, and M. Zhang, "A blind signature scheme for iov based on 2d-scml image encryption and lattice cipher," *Expert Systems with Applications*, vol. 246, p. 123215, 2024.

[49] Y. Sun, K. Yu, A. K. Bashir, and X. Liao, "Bl-iea: A bit-level image encryption algorithm for cognitive services in intelligent transportation systems," *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 1, pp. 1062–1074, 2021.

[50] J. Wu, X. Liao, and B. Yang, "Image encryption using 2d hénon-sine map and dna approach," *Signal processing*, vol. 153, pp. 11–23, 2018.

[51] O. Mannai, R. Bechikh, H. Hermassi, R. Rhouma, and S. Belghith, "A new image encryption scheme based on a simple first-order time-delay system with appropriate nonlinearity," *Nonlinear Dynamics*, vol. 82, no. 1, pp. 107–117, 2015.

[52] H. Chang, E. Wang, and J. Liu, "Research on image encryption based on fractional seed chaos generator and fractal theory," *Fractal and Fractional*, vol. 7, no. 3, p. 221, 2023.

[53] W. Alexan, N. Alexan, and M. Gabr, "Multiple-layer image encryption utilizing fractional-order chen hyperchaotic map and cryptographically secure prngs," *Fractal and Fractional*, vol. 7, no. 4, p. 287, 2023.
[54] D. Jiang, L. Liu, L. Zhu, X. Wang, X. Rong, and H. Chai, "Adaptive embedding: A novel meaningful image encryption scheme based on parallel compressive sensing and slant transform," *Signal Processing*, vol. 188, p. 108220, 2021.
[55] X. Huang and G. Ye, "An image encryption algorithm based on hyper-chaos and dna sequence," *Multimedia tools and applications*, vol. 72, pp. 57–70, 2014.
[56] Y. Liu, X. Shen, J. Liu, and K. Peng, "Optical asymmetric jtc cryptosystem based on multiplication-division operation and rsa algorithm," *Optics & Laser Technology*, vol. 160, p. 109042, 2023.

IX. Biography Section

Zhenlong Man was born in 1992. Obtained a doctoral degree from Changchun University of Science and Technology in China in 2022. He currently an associate professor and master's supervisor in the Department of Computer Science and Technology at Liaoning Technical University. His research interests include multimedia data hiding, image encryption, digital watermarking, biometric recognition, and cryptography.

Ze Yu was born in 2004. He is an undergraduate student at the Department of Computer Science and Technology at Liaoning Technical University. He is currently furthering his studies at Liaoning Technical University in China. His research focuses include biocryptography, image encryption, and chaotic systems.

Jiahu Yu was born in 2004. She is an undergraduate student in the Department of Computer Science of Liaoning University of Technology, and is currently pursuing further studies in Liaoning University of Technology, with research interests in digital watermarking and image encryption.

Xiangfu Meng was born in 1981. He received the Ph.D. degree from Northeastern University, China, in 2010. He is currently a Full Professor and a Ph.D. Supervisor with Liaoning Technical University, China. His research interests include spatial data management, recommender systems, and web database query.