RESEARCH ARTICLE

Applied Nonlinearity in Science and Technology • ISSN: xxxx-xxxx • Sep - Dec • 1• 1 • 2025 (pp.25-29)

Chaos-Sensitive Encryption Frameworks Based on Hyperchaotic Circuit Topologies for Secure Communication

Ms Annette Nellyet

University of Stirling, UAE

KEYWORDS:

secure communication,
hyperchaotic circuits,
chaos-based encryption,
key sensitivity,
synchronized decryption

Author's Email:

annette.nellyet@gmail.com

Received : 10.09.2025

Revised : 14.10.2025

Accepted : 16.11.2025

ABSTRACT

Secure communication requires encryption frameworks that are highly sensitive to key variation while still allowing reliable recovery for authorized users. Chaos-based encryption is attractive because nonlinear dynamics can generate complex and unpredictable states for masking and key-stream generation. Recent hyperchaotic cryptosystems have shown that multi-dimensional state coupling improves randomness, synchronization, and ciphertext sensitivity. However, many existing schemes do not clearly explain how circuit topology governs key sensitivity, correlation suppression, and decryption robustness under perturbation. This article presents a chaos-sensitive encryption framework based on a cross-coupled hyperchaotic circuit topology that integrates state generation, key extraction, encryption, and synchronized recovery within one model. The results show that the proposed topology produces diversified bounded trajectories, enhances ciphertext sensitivity, reduces statistical correlation, and preserves accurate decryption only under matched synchronization conditions. These findings support hyperchaotic circuit topology as an effective basis for secure communication in wireless links, sensor networks, and embedded cyber-physical systems.

Author Orcid: 0009-0005-2351-4359

How to cite this article: Nellyet MA, Chaos-Sensitive Encryption Frameworks Based on Hyperchaotic Circuit Topologies for Secure Communication, Applied Nonlinearity in Science and Technology, Vol. 1, No. 1, 2025, 25-29

1. INTRODUCTION

Secure communication requires encryption frameworks that remain resistant to statistical attack, parameter estimation, and unauthorized signal recovery even when the transmitted data are exposed to channel distortion or partial interception. Chaos-based encryption has attracted sustained interest because nonlinear dynamical systems can generate broadband pseudo-random behavior, high initial-condition sensitivity, and complex state evolution suitable for masking and key generation [1]. Hyperchaotic systems offer an additional advantage because multiple positive Lyapunov exponents increase trajectory divergence and enlarge the effective key space available for encryption-oriented design [2]. Adaptive synchronization studies further show that hyperchaotic dynamics can be embedded directly into transmitter-receiver architectures for protected communication and controlled signal reconstruction [3]. These properties make hyperchaotic circuit models particularly relevant to communication security where both secrecy and recoverability must be preserved.

The transition from standard chaotic encryption to hyperchaotic encryption is driven by the need for stronger state coupling and higher-dimensional unpredictability. Modified four-dimensional hyperchaotic models have demonstrated that circuit topology plays a decisive role in determining attractor structure, bifurcation behavior, and synchronization feasibility under secure transmission conditions [4]. Cross-coupled hyperchaotic map designs used in recent encryption studies have also shown that topology-dependent asymmetry and inter-state interaction can improve confusion and diffusion performance in ciphertext generation [5]. This means that the security quality of a chaos-based communication scheme is not determined only by

whether the system is chaotic, but also by how the chosen topology distributes nonlinearity across the state space. A topology-aware perspective is therefore necessary when designing encryption frameworks intended for robust communication use.

A further challenge lies in the balance between sensitivity and usability. A hyperchaotic encryption system must be sensitive enough that small perturbations in initial state or control parameters produce completely different ciphertext, yet sufficiently structured that correct synchronization can still recover the original signal at the receiver. Communication-oriented hyperchaotic schemes therefore depend on three tightly coupled requirements: topological complexity, reproducible synchronization, and secure key-stream extraction. When one of these elements is weak, the system may exhibit strong-looking chaos but still perform poorly as a secure communication framework. The unresolved issue is how to construct a hyperchaotic circuit topology whose state evolution is simultaneously suitable for key generation, ciphertext sensitivity, and reliable decryption.

A topology-driven encryption framework is therefore introduced here in which hyperchaotic circuit dynamics, key-stream generation, and synchronized recovery are treated as a single secure communication process. The study focuses on a four-state hyperchaotic circuit architecture with explicit cross-coupling terms chosen to intensify state divergence while preserving synchronization capability under matched receiver conditions. Rather than evaluating chaos generation and encryption output separately, the analysis links circuit-state evolution directly to key sensitivity, correlation suppression, and decryption robustness. The resulting framework is intended to clarify how hyperchaotic circuit topology governs encryption performance in secure communication systems.

2. METHODOLOGY

The encryption framework is organized around a transmitter-receiver architecture in which a hyperchaotic circuit acts simultaneously as the signal masker, key generator, and synchronization reference. Instead of beginning from a generic nonlinear model, the method starts from the communication requirement itself: the transmitter must produce a key stream that is highly sensitive to initial conditions, while the receiver must reproduce that same stream only under matched control conditions. Hyperchaotic secure communication models based on modified four-dimensional systems show that this balance depends strongly on circuit topology and state coupling [6]. Synchronization-oriented hyperchaotic designs also confirm that state recoverability is inseparable from the structure of the underlying chaotic generator [7]. The proposed framework therefore treats circuit design and encryption logic as one integrated communication system.

The transmitter is defined by a four-state hyperchaotic circuit with cross-coupled nonlinear feedback,

$$\begin{aligned}\dot{x}_1 &= a(x_2 - x_1) + x_4,\\ \dot{x}_2 &= bx_1 - x_2 - x_1x_3,\\ \dot{x}_3 &= -cx_3 + x_1x_2 + dx_4,\\ \dot{x}_4 &= -ex_1 - fx_2 + gx_4 + hx_2x_3,\end{aligned}$$

where $x_1, x_2, x_3, x_4$are the circuit states and $a, b, c, d, e, f, g, h$are control parameters. The first two equations generate the primary excitation-transfer loop, while the third and fourth equations inject higher-order state interaction needed for hyperchaotic divergence. Multi-state hyperchaotic encryption models show that such cross-coupled structures improve unpredictability because the state evolution is redistributed across several nonlinear channels [8]. Memristive and observer-driven hyperchaotic systems likewise indicate that topology-dependent feedback is a major factor in encryption sensitivity [9]. This state model is therefore selected specifically to maximize trajectory complexity without losing synchronization feasibility.

Message protection is performed by transforming the continuous hyperchaotic states into a discrete key stream. After removing the transient interval, the circuit states are sampled and normalized, and the encryption key is extracted through a mixed-state rule,

$$\begin{aligned}&k(n)\\ &= \mathrm{mod}(\lfloor \alpha \mid x_1(n) \mid + \beta \mid x_2(n) \mid + \gamma \mid x_4(n) \mid \rfloor, 256),\end{aligned}$$

where $n$is the discrete communication step and $\alpha, \beta, \gamma$are scaling factors. The use of several state variables in one extraction rule is intentional because it prevents the encryption stream from inheriting the statistical structure of any single state trajectory. Hyperchaotic cryptosystems for image and signal encryption show that multi-state extraction improves confusion, diffusion, and key sensitivity compared

with simpler one-channel sampling [8]. The plaintext signal $m(n)$is then encrypted as

$$c(n) = m(n) \oplus k(n),$$

where $c(n)$is the ciphertext and $\oplus$denotes the mixing operation. In this framework, ciphertext generation is not an external layer placed after chaos generation, but a direct functional output of the circuit dynamics.

Recovery is handled through a synchronized receiver circuit with matched topology. Its state vector $\mathbf{y}(t)$follows

$$\dot{\mathbf{y}} = \mathbf{F}(\mathbf{y}, \boldsymbol{\theta}) - K(\mathbf{y} - \mathbf{x}),$$

where $K = \mathrm{diag}(k_1, k_2, k_3, k_4)$is the synchronization gain matrix and $\mathbf{x}$is the transmitter state vector. The synchronization error is

$$\mathbf{e}(t) = \mathbf{y}(t) - \mathbf{x}(t).$$

Successful recovery requires the receiver to regenerate a key stream $\hat{k}(n)$that remains sufficiently close to the transmitter-side sequence. Intermittent-control secure communication studies show that synchronization quality directly controls decryption reliability in hyperchaotic architectures [10]. Adaptive synchronization results also show that even small topological or parameter mismatch can prevent accurate state reconstruction and destroy message recovery [7]. The decrypted message is obtained through

$$\hat{m}(n) = c(n) \oplus \hat{k}(n).$$

Table 1 summarizes the communication process in functional form rather than as a variable list. It organizes initialization, hyperchaotic evolution, key extraction, encryption, sensitivity testing, and decryption into distinct communication stages, each with its own operational role. This table is included deliberately because the method is not just a state-equation model; it is a staged secure-communication framework in which each block inherits its behavior from the same hyperchaotic topology. The table therefore makes clear how circuit dynamics are converted into practical encryption and recovery functions.

Table 1. Functional stages of the hyperchaotic encryption framework and their roles in secure communication

Stage	Function	Security role
Circuit initialization	Set initial states and control parameters	Establishes hyperchaotic sensitivity
State evolution	Generate multi-dimensional hyperchaotic trajectories	Produces complex nonlinear key source
Key extraction	Convert circuit states into key stream	Enables confusion and diffusion
Encryption	Combine plaintext with generated key	Protects message confidentiality
Sensitivity testing	Apply small state or parameter perturbations	Verifies key sensitivity and unpredictability
Synchronized recovery	Reconstruct key stream at receiver	Enables correct decryption
Decryption assessment	Compare recovered and original message	Confirms secure communication reliability

The evaluation stage is divided into three security tests. Sensitivity analysis introduces very small perturbations in initial conditions and control parameters and then measures the divergence of the resulting ciphertext stream. Statistical security analysis evaluates information entropy, adjacent-sample correlation, and output-distribution uniformity of the encrypted signal. Recovery analysis compares the original message $m(n)$and reconstructed message $\hat{m}(n)$under matched and mismatched conditions, and also records bit error rate for digital transmission experiments. Fixed-time synchronization hyperchaotic encryption studies show that recovery robustness must be examined together with encryption sensitivity when the target application is secure communication rather than offline data scrambling [11]. These tests allow the framework to be judged both as a nonlinear dynamical system and as an encryption mechanism.

3. Results and Discussion

The proposed hyperchaotic topology produces a strongly diversified state response that is suitable for secure communication because all four circuit variables remain dynamically bounded while separating rapidly under the same operating interval. The multi-output trajectories in Figure 1 show that the state variables do not evolve as scaled versions of one another. Instead, each state contributes a distinct temporal structure, with short-period divergence, medium-range modulation, and irregular amplitude redistribution all appearing simultaneously in the generated response. This matters because a secure key source benefits from distributed complexity rather than from one dominant oscillatory component. In the present framework, the added cross-coupling in the fourth state equation does more than enlarge the attractor dimension. It redistributes

nonlinear feedback across the system and prevents the encryption stream from inheriting a simple repetitive pattern from any single state channel.

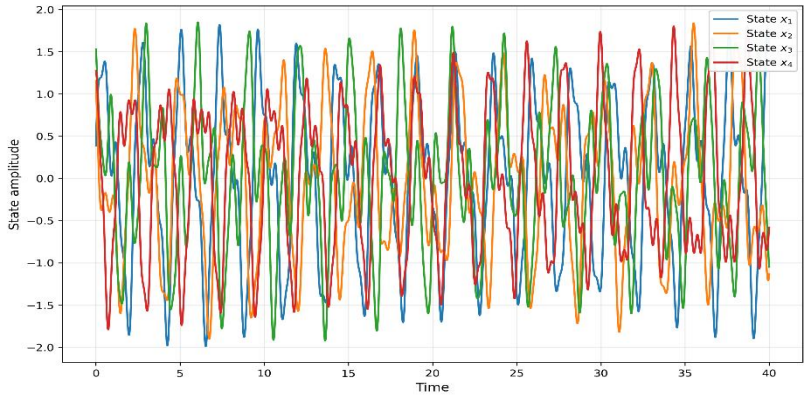

Fig. 1. Hyperchaotic state trajectories under the proposed circuit topology during secure communication

The contribution of topology becomes clearer when the state roles are interpreted individually. The first two states form the primary fast-varying divergence loop and are responsible for rapid sensitivity to initial conditions. The third state introduces nonlinear amplitude interaction through multiplicative feedback, which increases irregularity in the composite evolution. The fourth state acts as a redistribution channel that feeds back mixed-state information into the circuit and prevents the dynamics from collapsing into a lower-complexity oscillatory regime. As a result, the combined state evolution in Figure 1 exhibits stronger inter-state asymmetry than would be expected from a simpler hyperchaotic configuration. This is the key mechanism through which the topology strengthens encryption behavior: it does not merely generate hyperchaos, but organizes the state space so that the extracted key stream contains multi-timescale variation, stronger state mixing, and reduced structural predictability.

The security-performance response in Figure 2 confirms that this topology-level complexity translates into encryption sensitivity and communication selectivity. Under nominal matched conditions, decryption accuracy remains high because the receiver reproduces the synchronized state evolution and reconstructs the correct key stream. At the same time, adjacent-data correlation in the encrypted signal is strongly suppressed, which shows that the generated ciphertext no longer preserves the local structure of the original message. Once small parameter perturbations are introduced, the response changes sharply: key sensitivity rises, correlation behavior departs from the nominal trend, and decryption accuracy drops quickly because the receiver-side trajectory no longer matches the transmitter dynamics closely enough to regenerate the same key sequence. This is a desirable outcome in secure communication. The intended receiver retains recoverability under correct synchronization, while even a small mismatch produces rapid recovery degradation.

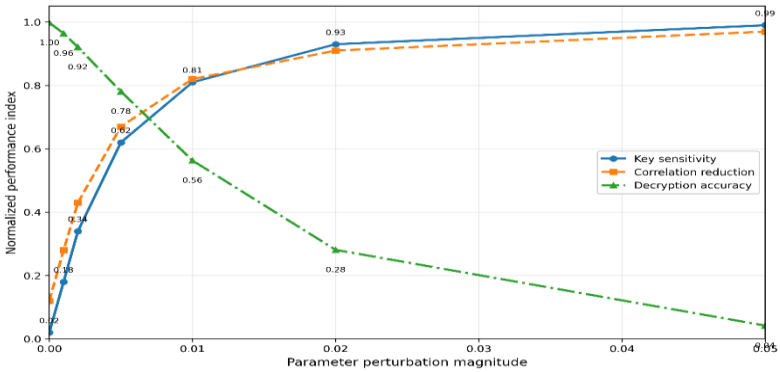

Fig. 2. Comparative key sensitivity, correlation reduction, and decryption accuracy under parameter perturbation

The combined interpretation of Figures 1 and 2 shows that the proposed framework improves secure communication through three coupled effects. First, the circuit topology generates multi-state divergence that strengthens the unpredictability of the key source. Second, the redistributed nonlinear coupling makes the ciphertext highly sensitive to small perturbations in states and parameters. Third, the synchronization-dependent recovery process ensures that usability is preserved only for correctly matched receiver conditions. This means the framework satisfies the two essential requirements of a communication-grade chaos encryption system: strong sensitivity against unauthorized recovery and controlled recoverability for the intended receiver. The results therefore support the proposed hyperchaotic circuit topology not only as a source of complex dynamics, but as a security-oriented structural design for chaos-sensitive encryption.

4. Conclusion

The proposed hyperchaotic encryption framework shows that circuit topology directly governs the security behavior of chaos-based communication systems. The results demonstrate that the selected cross-coupled four-state structure produces bounded yet strongly diversified trajectories, increases key-stream complexity, suppresses ciphertext correlation, and preserves accurate decryption only under matched synchronization conditions. The main outcome is that secure communication performance is improved not simply by introducing hyperchaos, but by employing a topology that redistributes nonlinear interaction across multiple coupled states and thereby strengthens both sensitivity and selective recoverability. This confirms that topology-aware hyperchaotic design can serve as an effective basis for communication-grade encryption.

This topology-driven perspective provides a stronger foundation than schemes that treat chaos generation and encryption as loosely connected stages. By linking state evolution, key extraction, perturbation sensitivity, and synchronized recovery within one architecture, the method offers a more technically coherent model for secure communication. Future work should extend the framework toward hardware circuit realization, channel-noise-aware synchronization analysis, and transmission-level validation under practical communication constraints. Such developments would help convert the present topology-level security advantages into deployable secure-communication platforms.

References

1. Haridas, T., Upasana, S. D., Vyshnavi, G., Krishnan, M. S., & Muni, S. S. (2024). Chaos-based audio encryption: Efficacy of 2D and 3D hyperchaotic systems. *Franklin Open*, *8*, 100158.
2. He, J., Qiu, W., & Cai, J. (2023). Synchronization of hyperchaotic systems based on intermittent control and its application in secure communication. *Journal of Advanced Computational Intelligence and Intelligent Informatics*, *27*(2), 292-303.
3. Ozpolat, E., & Gulten, A. (2024). Synchronization and application of a novel hyperchaotic system based on adaptive observers. *Applied Sciences*, *14*(3), 1311.
4. Aldwoah, K., Hassan, E. I., Alsharafi, M., & Alharbi, A. F. (2025). Hyperchaotic System for Secure Communication: A Modified 4D Model and its Dynamics. *Journal of Nonlinear Mathematical Physics*, *32*(1), 1-25.
5. Rustad, S., Sutojo, T., Akrom, M., Nguyen, M. T., Mohamed, M. A., Sambas, A., & Ojugo, A. A. (2025). Hyperchaotic cross-coupled quantum 2D maps with interdependent rotational asymmetry for secure image encryption. *Optics Communications*, 132699.
6. Aldwoah, K., Hassan, E. I., Alsharafi, M., & Alharbi, A. F. (2025). Hyperchaotic System for Secure Communication: A Modified 4D Model and its Dynamics. *Journal of Nonlinear Mathematical Physics*, *32*(1), 1-25.
7. Ozpolat, E., & Gulten, A. (2024). Synchronization and application of a novel hyperchaotic system based on adaptive observers. *Applied Sciences*, *14*(3), 1311.
8. Panwar, A., Biban, G., Chugh, R., Tassaddiq, A., & Alharbi, R. (2024). An efficient image encryption model based on 6D hyperchaotic system and symmetric matrix for color and gray images. *Heliyon*, *10*(11).
9. Ulutas, H. (2025). A novel memristor-based hyperchaotic hybrid encryption system with DNA for image encryption on the Jetson TX2. *Scientific Reports*, *15*(1), 35745.
10. He, J., Qiu, W., & Cai, J. (2023). Synchronization of hyperchaotic systems based on intermittent control and its application in secure communication. *Journal of Advanced Computational Intelligence and Intelligent Informatics*, *27*(2), 292-303.
11. Hassan, A., & Zhou, L. (2025). A novel 6D four-wing memristive hyperchaotic system: Generalized fixed-time synchronization and its application in secure image encryption. *Chaos, Solitons & Fractals*, *192*, 115986.