Analog Guard®

Encryption Implemented as a Physical-Layer Mixed-Signal Environment

Foundational IP White Paper

Core thesis

Analog Guard® frames secure communication as a dynamically evolving physical signal environment rather than as a purely mathematical data-layer operation.

Prepared for	Technical, investor, aerospace/cybersecurity, secure communications, and spectrum-operations audiences
Prepared by	Analog Guard, Inc.
Source document	Analog Guard Foundational IP Article V4
Date	December 2025

Document Profile

Item	Description
Subject	Physical-layer mixed-signal encryption using dynamically evolving analog signal behavior.
Technology focus	Analog Guard® architecture, including dynamic carriers, PLTNM, resonant analog behavior, parallel signal paths, and matched analog reconstruction.
Primary problem addressed	Conventional encrypted communications may hide message contents while leaving carrier behavior, timing, spectral structure, and transmission patterns observable.
Architectural premise	Protection may be distributed through the physical behavior of the communication signal itself rather than being limited to software algorithms and static digital keys.
Reader orientation	This document is a white-paper presentation of the attached article; it is not a patent claim chart, product datasheet, or security certification report.

Executive Summary

Modern cybersecurity is primarily organized around mathematical protection of digital information. Encryption algorithms, keys, protocols, and authentication mechanisms remain essential, but they generally operate after information has been separated from the physical signal environment that carries it.

Analog Guard® proposes a different architectural model [2-4]. The communication signal itself participates in the protection mechanism through continuously evolving waveform behavior and multidimensional analog modulation processes. This white paper explains the foundational IP concept in which security is implemented as a dynamically evolving signal environment. The protected object is not merely the data payload. It is the evolving waveform environment in which carrier behavior, temporal relationships, and analog-state conditions influence whether information can be recovered.

The practical implication is a shift from purely key-centric encryption toward reconstruction-dependent security. Successful recovery depends not only on access to the appropriate keying relationship, but also on reproduction of the correct analog conditions, timing behavior, carrier dynamics, phase relationships, and signal-processing environment.

Stated simply, Analog Guard® seeks to make the signal carrying information part of the protection system itself, extending protection beyond the message and into the physical-layer environment through which the message travels.

Key Takeaways

- Analog Guard® treats the waveform and carrier environment as active parts of the encryption architecture.
- The architecture is designed to reduce stable reference points used by interception, classification, and model-assisted signal analysis systems.
- Parallel paths may preserve independent analog-encrypted channels until after decryption and binary reconstruction.
- PLTNM and related analog processes introduce timing, phase, resonance, and waveform-shaping behavior into the protection environment.
- Matched analog conditions support recovery; mismatched analog conditions can produce distortion, noise, and reconstruction failure.
- The approach complements, rather than replaces, conventional cryptographic and secure-communications techniques.

Contents

1. Introduction and Core Thesis

Modern cybersecurity was built on a relatively simple assumption: information can be protected mathematically [1]. For decades, encryption systems have relied on algorithms that transform readable data into computationally difficult problems using digital keys and software-based cryptographic operations. Whether protecting financial systems, military communications, cloud infrastructure, or consumer devices, the dominant philosophy has remained largely unchanged: security exists primarily in mathematics.

Analog Guard® proposes a fundamentally different approach to secure communications.

The technology described in U.S. Patent Nos. 12,126,720 and 12,615,149 suggests that information security can also emerge from the controlled complexity of physical signal behavior itself [10,11]. Instead of relying exclusively on computational algorithms, the architecture embeds protection into continuously changing analog waveforms, dynamic carrier environments, resonant behavior, phase relationships, temporal distortion, and multidimensional analog modulation processes.

In practical terms, Analog Guard® treats the communication signal itself as part of the encryption mechanism.

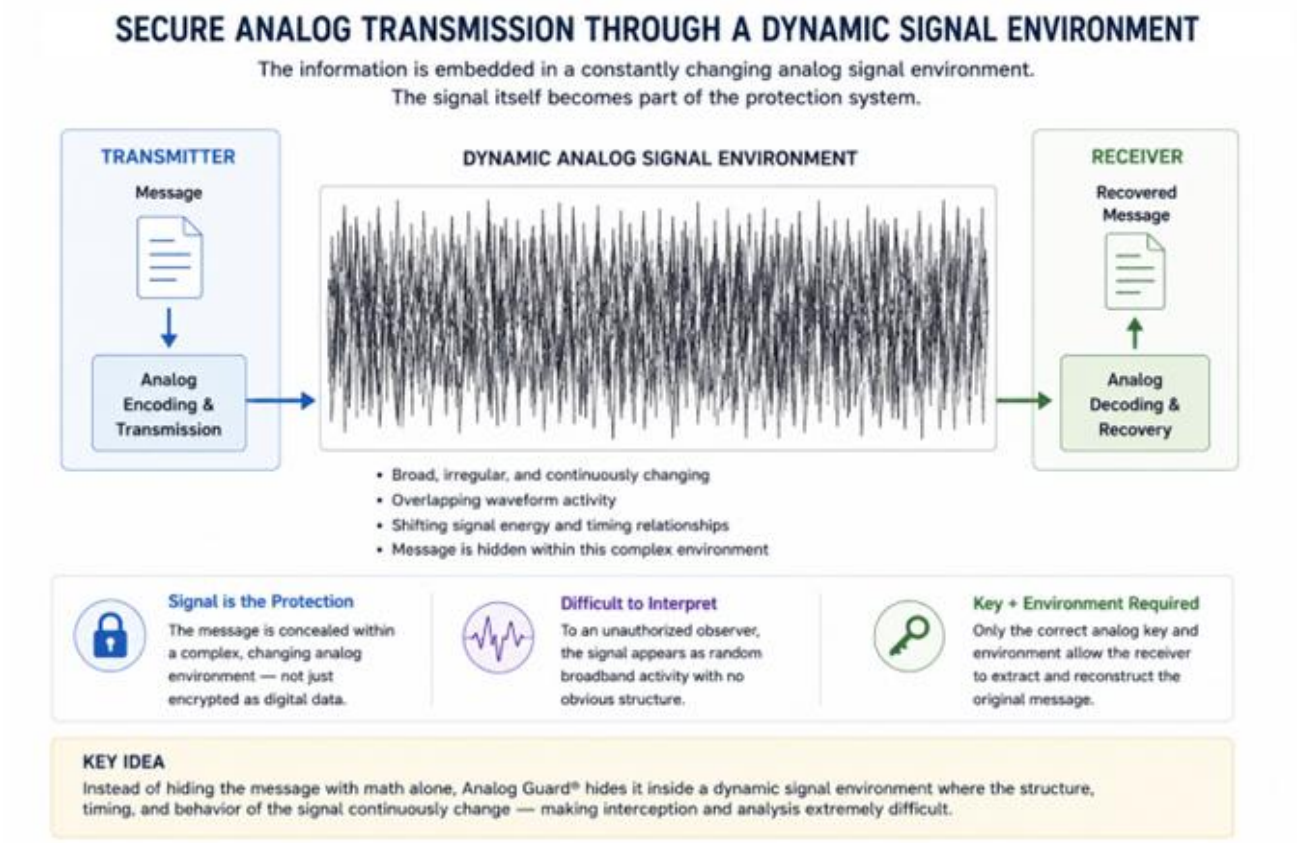

Figure 1. Transmission concealed within a continuously evolving analog signal environment.

This distinction is important because traditional communications systems separate the message from the transport mechanism carrying it. A digital encryption algorithm scrambles the information, but the carrier transporting the encrypted data often remains relatively stable and

observable. Frequencies may hop, modulation schemes may vary, and spread-spectrum techniques may be used, but the underlying transmission structure still tends to exhibit identifiable behavior.

Advanced signal-intelligence platforms classify emissions by analyzing carrier stability, timing periodicity, spectral signatures, synchronization structures, pulse intervals, modulation characteristics, and statistical repetition [5,6]. AI-assisted systems can accelerate this process by identifying subtle recurring behaviors across large signal datasets. Even when encrypted data cannot be directly decoded, the transmission itself may reveal operational information.

In many real-world environments, understanding that a communication is occurring can be nearly as valuable as understanding the contents of the communication itself. Transmission timing, activity levels, communication persistence, and signal identity can reveal operational patterns even when message payloads remain encrypted.

Analog Guard® is designed to reduce those stable reference points by moving protection into the broader signal environment. Characteristics of the waveform itself—including its temporal behavior, carrier dynamics, and evolving analog structure—become part of the protection architecture. Unlike conventional encryption systems, where the carrier simply transports encrypted bits, Analog Guard® integrates the carrier directly into the protection process. The waveform carrying the information becomes inseparable from the encryption architecture itself. An unauthorized observer is therefore confronted not merely with encrypted data, but with an unstable physical signal environment whose behavior changes during operation.

This changes the nature of attack. Instead of simply recovering a digital key or breaking an algorithm mathematically, an interceptor may also need to reconstruct the analog conditions governing the transmission in real time. That means reproducing not only the proper data relationships, but also the correct carrier dynamics, phase behavior, temporal structure, resonant conditions, and modulation interactions simultaneously.

2. Dynamic Carrier Environment

A central element of the Analog Guard® architecture is the concept of a dynamic carrier [10,11]. In conventional communication systems, carriers are generally stable and predictable. Their frequencies, phases, and modulation behavior follow controlled standards designed for reliable synchronization and efficient transmission.

Analog Guard® intentionally disrupts that stability. The carrier is no longer treated as a passive delivery mechanism; it becomes part of the protection mechanism.

In conventional communications systems, the carrier typically exists to transport information from one location to another. While modulation techniques may vary, the carrier itself is generally expected to remain sufficiently stable to support synchronization, demodulation, and signal classification. This predictability is beneficial for reliable communications but can also provide useful information to an observer.

Analog Guard® approaches the carrier differently. Rather than serving solely as a transport mechanism, the carrier becomes an active participant in the analog protection environment. ts

behavior may evolve as a function of analog keying relationships, waveform interactions, and other analog-state variables.

In effect, the carrier transitions from a transport mechanism into a participating element of the protection environment. The signal carrying the information is no longer independent of the protection process. Instead, the carrier and the protected information become increasingly coupled as the signal evolves.

As a result, the carrier no longer represents a fixed reference structure around which the protected information is organized. Instead, both the information and the carrier environment may evolve together, making the overall transmission more difficult to characterize using conventional signal-analysis techniques.

As illustrated in Figure 2, Analog Guard® transforms binary information into analog waveform behavior before encryption occurs.

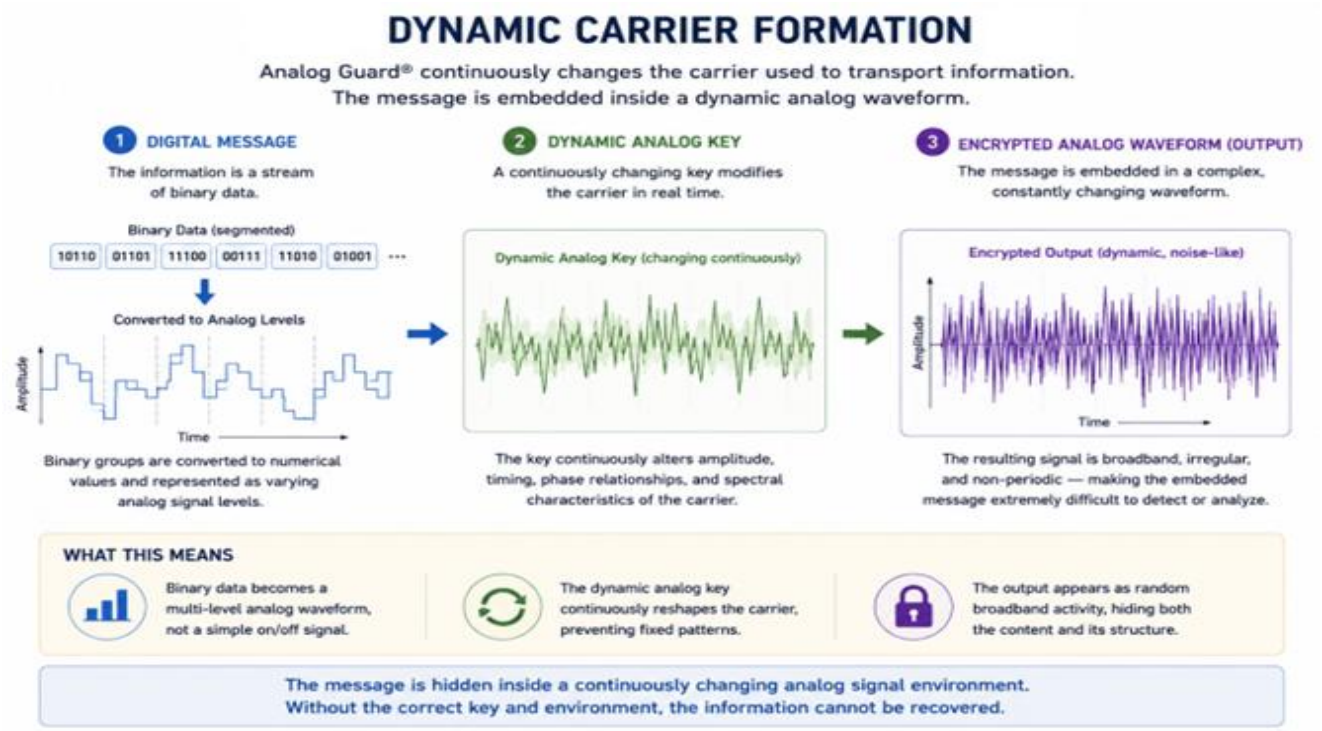

Figure 2. Binary information converted into analog waveform behavior before dynamic carrier-based encryption.

3. Analog Encoding and Carrier Participation

Before the carrier can participate in the protection process, the digital information must first be represented in a form that can interact with the analog environment. This occurs through the analog-encoding stage.

Rather than treating the message as a simple digital bitstream, the system converts grouped binary values into varying analog amplitude levels, creating a complex non-periodic waveform. The analog key then continuously modifies the carrier environment in real time, altering signal relationships as transmission occurs.

This conversion step is significant because it changes the nature of the information being protected. Instead of existing solely as a sequence of discrete digital symbols, the information becomes represented by continuously varying signal characteristics. Amplitude levels, timing relationships, phase behavior, and waveform geometry can now participate in the protection process. The information is therefore no longer isolated from the physical signal carrying it; it becomes intertwined with that signal's behavior.

This interdependence creates opportunities for protection mechanisms that do not exist in purely digital systems. Once information is represented as continuously varying waveform behavior, modifications to the signal environment can influence recoverability in ways that extend beyond conventional bit-level encryption.

This is a major departure from conventional encryption systems. In traditional digital encryption architectures, the encrypted data exists independently of the carrier transporting it. In Analog Guard®, the carrier itself becomes part of the protection mechanism [10,11]. The signal environment continuously changes while carrying the information.

This represents a departure from the traditional separation between information and transport. In the Analog Guard® architecture, the information and the signal environment carrying that information become increasingly interdependent.

The result is a transmission whose waveform structure and observable signal characteristics evolve continuously during operation. To an unauthorized observer, the transmission may resemble broadband analog noise rather than recognizable communications traffic [5,6].

This is important because interception and classification systems depend heavily on stable patterns. Fixed timing intervals, recognizable spectral distributions, and repetitive modulation behavior all provide clues that enable classification and analysis. Analog Guard® is designed to reduce those clues before they can be exploited.

4. Independent Parallel Signal Paths

As the architecture evolves, the system expands into multiple parallel signal paths operating simultaneously. Importantly, these parallel paths are not mixed together prior to decryption. Instead, each path functions as an independent encrypted transmission channel carrying its own analog-encrypted signal stream.

This distinction is central to understanding the parallel Analog Guard® implementation. In some secure communications systems, multiple signal streams may be combined into a composite waveform before transmission. Analog Guard® does not operate this way in its parallel implementation. Each signal path remains physically separate throughout transmission and recovery.

Figure 3 illustrates this concept by showing the original binary message divided into smaller data segments, with different portions of the binary information assigned to separate signal channels. Each channel independently converts its assigned binary segment into an analog-encoded waveform before encryption and transmission.

The analog waveforms are intended to be irregular, multi-level, non-periodic, and continuously varying rather than sinusoidal or repetitive. Each signal path may be visually and operationally distinct, reflecting differences in timing, phase behavior, modulation characteristics, or analog encoding conditions.

The important point is that the parallel analog signals themselves are never recombined during transmission. Each path remains independent while traveling through its own dynamically changing analog signal environment. The encrypted waveforms therefore remain isolated from one another until the recovery stage.

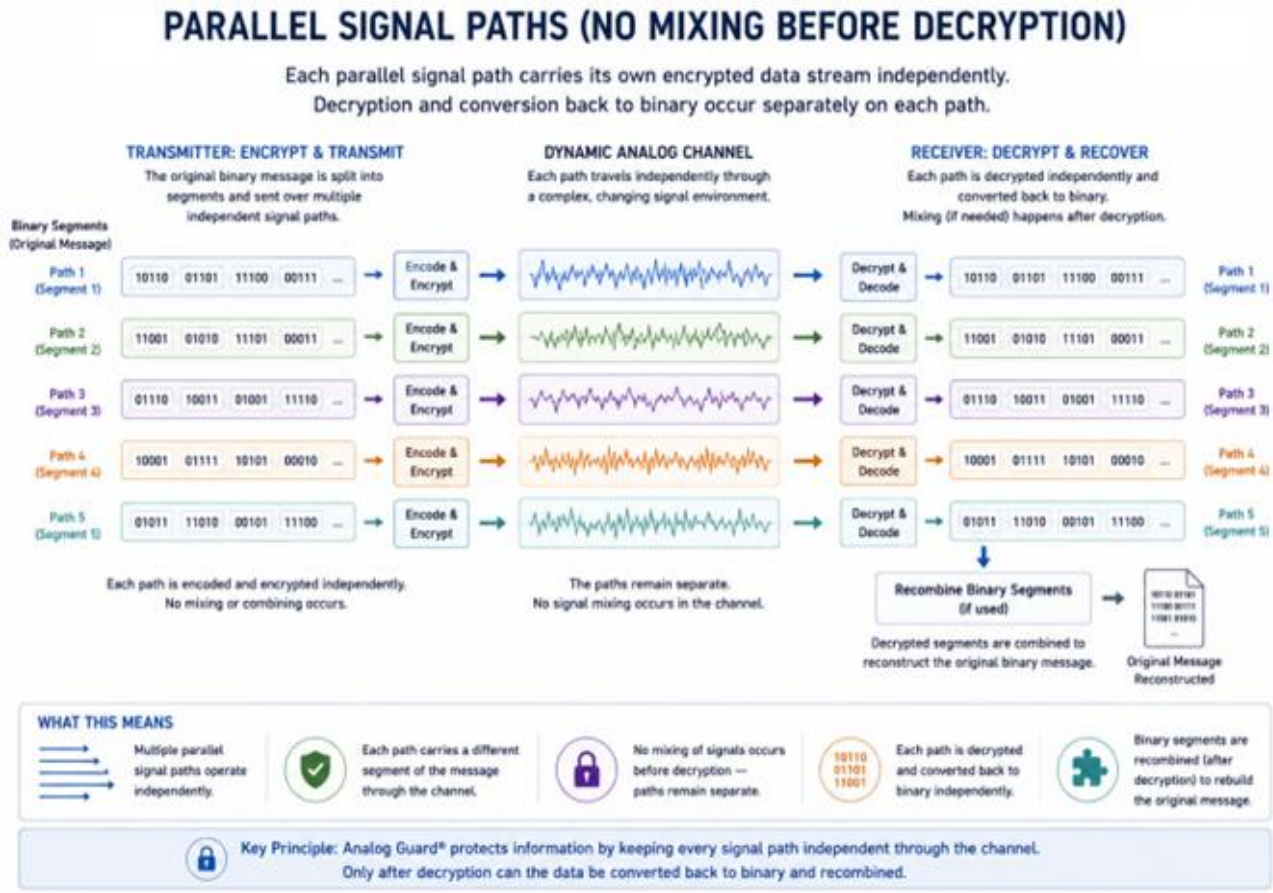

Figure 3. Independent parallel analog-encrypted signal paths maintained separately until recovery

At the receiver, each analog signal path undergoes independent decryption and recovery. The recovered analog information from each path is then converted back into its corresponding binary data segment. Only after successful decryption and binary reconstruction are the separate binary segments recombined to rebuild the original message or data file.

This architecture increases both reconstruction difficulty and architectural flexibility because interception would require recovering multiple independent encrypted analog channels simultaneously. An interceptor would not only need to recover the correct analog conditions for one signal path, but potentially several distinct encrypted paths operating independently at the same time.

Parallel operation provides architectural flexibility as different signal paths may operate under different analog conditions, employ different key relationships, or carry different portions of the protected information. Because each path can be recovered independently, the architecture allows information to be distributed across multiple protected channels without requiring those channels to be combined during transmission. This separation preserves the independence of each protected signal environment while contributing to the overall reconstruction process.

5. Temporal Manipulation and PLTNM

Timing relationships represent another important dimension of the Analog Guard® protection environment. As shown in Figure 4, temporal behavior itself becomes part of the encryption process.

Conventional communication systems depend heavily on precise timing relationships. Packet intervals, pulse repetition frequencies, synchronization frames, carrier timing, and symbol alignment all create observable patterns that aid reliable communications but also facilitate interception, classification, and traffic analysis.

Analog Guard® instead treats timing relationships as part of the encryption process itself. Proprietary Phase-Linked Temporal Nonlinear Modulation (PLTNM) circuitry dynamically modulates the analog-encoded data signal using one or more complex analog keys [10,11]. In doing so, the system continuously alters timing relationships within the waveform through phase-related temporal shifts while also modifying waveform amplitudes and shapes.

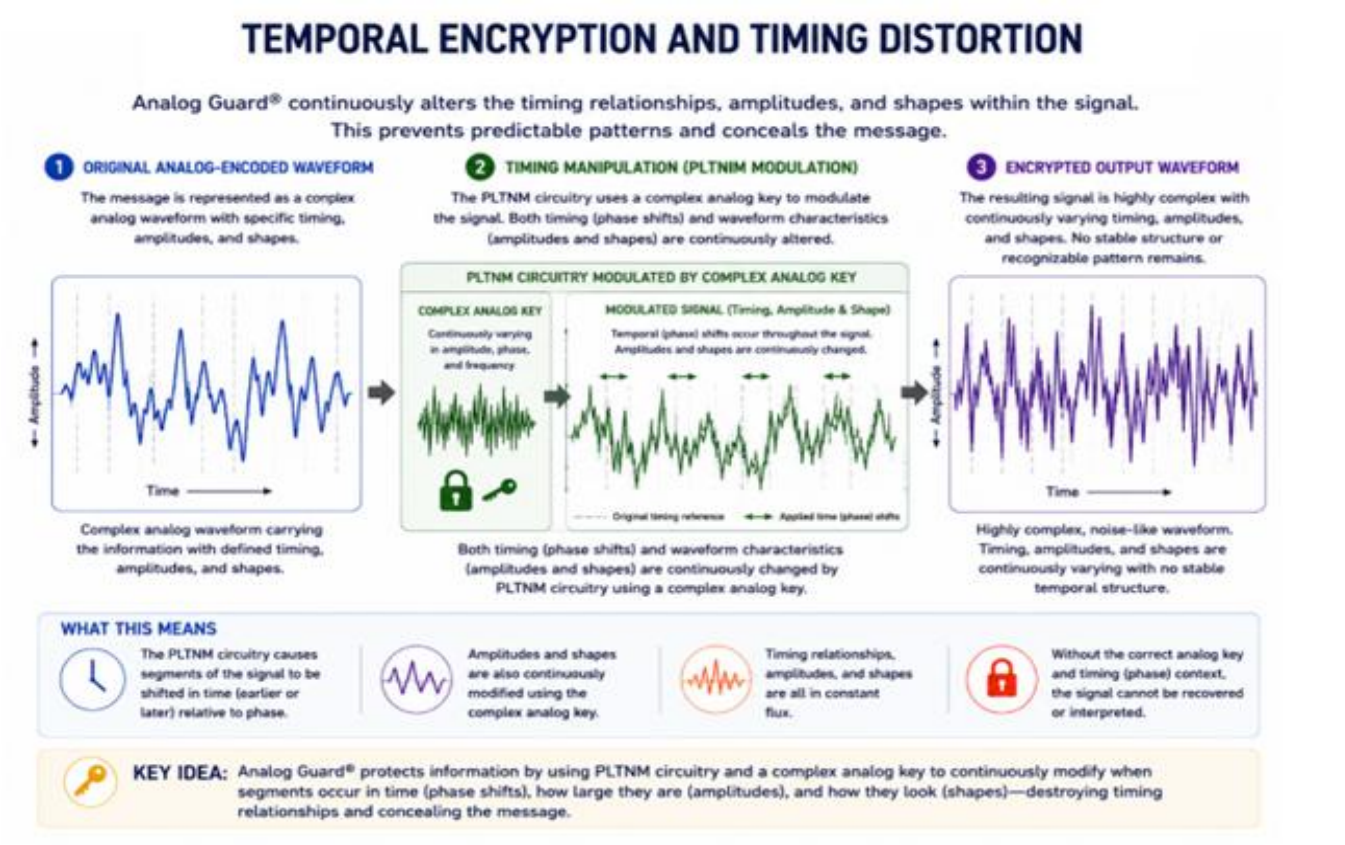

Figure 4. Temporal encryption and timing manipulation within a PLTNM processing environment

Importantly, the waveform is not simply shifted uniformly in time. Continuously changing analog modulation processes alter the overall waveform structure, timing relationships, amplitudes, and signal geometry simultaneously.

The resulting encrypted waveform no longer exhibits stable periodic timing relationships or recognizable signal organization. This matters because timing relationships themselves can reveal information about a transmission. Even when encrypted data remains unreadable, traffic-analysis systems can infer operational behavior by observing synchronization patterns, periodic transmission behavior, carrier stability, and temporal structure.

Analog Guard® acts to conceal not only message contents, but also recognizable behavioral characteristics of the transmission itself. The resulting signal therefore appears highly irregular, dynamically changing, broadband, and structurally difficult to classify or analyze.

Temporal manipulation is only one component of the broader waveform-transformation environment. The architecture can simultaneously influence multiple aspects of waveform behavior, creating a continuously evolving signal environment that affects recoverability.

6. Resonance, Phase Behavior, and Negative Group Delay

The emphasis is not on hardware components alone, but on how signal behavior changes dynamically as it moves through the encryption environment. The system progressively reshapes waveform structure through resonance, phase manipulation, and timing-distortion processes. Each transformation alters the signal in a different way, increasing complexity while reducing recognizable structure.

The architecture may incorporate resonant analog circuitry and negative group delay architectures intended to further manipulate waveform timing and phase behavior [9-11].

Negative group delay is often misunderstood because it appears counterintuitive [9]. It does not imply information traveling backward in time or violating causality. Instead, it refers to carefully engineered phase interactions in which portions of a waveform envelope can appear to emerge earlier than expected due to resonant energy redistribution and phase-slope behavior within the system.

In practical terms, the effect can be viewed as another way of altering how different portions of a signal relate to one another in time. The importance is not the phenomenon itself, but how it contributes to the overall complexity of the signal environment.

A useful way to visualize the effect is to imagine a waveform passing through a carefully engineered environment that continuously redistributes energy and phase relationships. Portions of the output waveform may appear to respond earlier than expected, not because information has traveled backward in time, but because the system has reshaped the waveform through predictable physical processes occurring within the analog environment.

Within Analog Guard®, these effects appear intended to increase waveform unpredictability, distort recognizable synchronization behavior, and complicate unauthorized reconstruction. The final encrypted waveform therefore becomes highly irregular and structurally difficult to interpret.

These transformations are depicted conceptually in Figure 5.

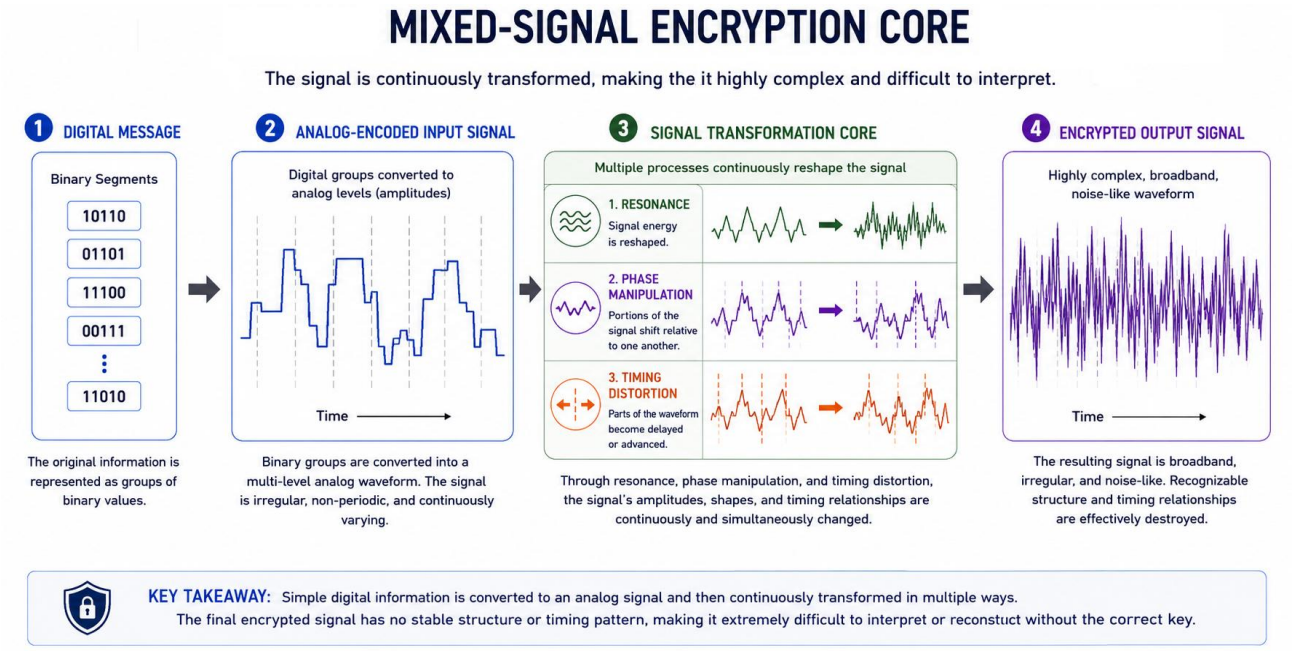

Figure 5. Continuous waveform transformation through resonance, phase behavior, and timing distortion

These individual transformation mechanisms need not operate in isolation. Multiple mechanisms may act concurrently, producing a multidimensional protection environment whose behavior evolves continuously during operation.

7. Coordinated Analog Transformation Domains

The waveform transformations described in the preceding sections need not occur independently. In practice, several analog processes may operate simultaneously, each contributing to the evolving behavior of the protected signal. As the architecture scales outward, Analog Guard® can apply multiple simultaneous analog transformation processes throughout the signal environment. Rather than relying on a single modulation effect, the system continuously reshapes multiple waveform characteristics simultaneously, allowing the protected signal environment to evolve across several interacting dimensions.

The result is a signal whose behavior continuously evolves across several analog dimensions at once. This is important because modern interception and signal-analysis systems depend heavily on stability and repeatability. Predictable carrier structures, stable timing relationships, fixed modulation behavior, and recognizable spectral characteristics all make signals easier to classify and analyze.

An observer attempting to characterize such a transmission is no longer evaluating a single waveform property. Instead, timing behavior, phase relationships, carrier characteristics,

amplitude structure, and spectral content may all be changing simultaneously. Even if one aspect of the signal can be partially characterized, the overall transmission environment may continue evolving through interactions among the remaining transformation domains.

As a result, analysis of any single signal characteristic may provide only a partial understanding of the overall transmission. The behavior of the protected signal emerges from the combined interaction of multiple evolving analog processes rather than from any one observable feature.

Analog Guard® is designed to disrupt stable reference points by allowing several analog transformation mechanisms to operate simultaneously within the signal environment [8,10,11]. The protected information therefore no longer exists inside a stable and easily recognizable transmission structure. Instead, the waveform becomes a continuously evolving analog process whose observable characteristics remain in flux. This creates a different security model from conventional digital encryption systems. Rather than protecting information solely through computational complexity, Analog Guard® distributes protection throughout the physical behavior of the signal itself.

Multiple analog transformation mechanisms may operate simultaneously within the protection environment. Figure 6 depicts this interaction through several coordinated transformation domains acting on the protected waveform. These transformations are not necessarily separate transmission channels carrying different message segments. Instead, they represent multiple interacting physical-layer modulation and signal-conditioning processes acting on the protected waveform.

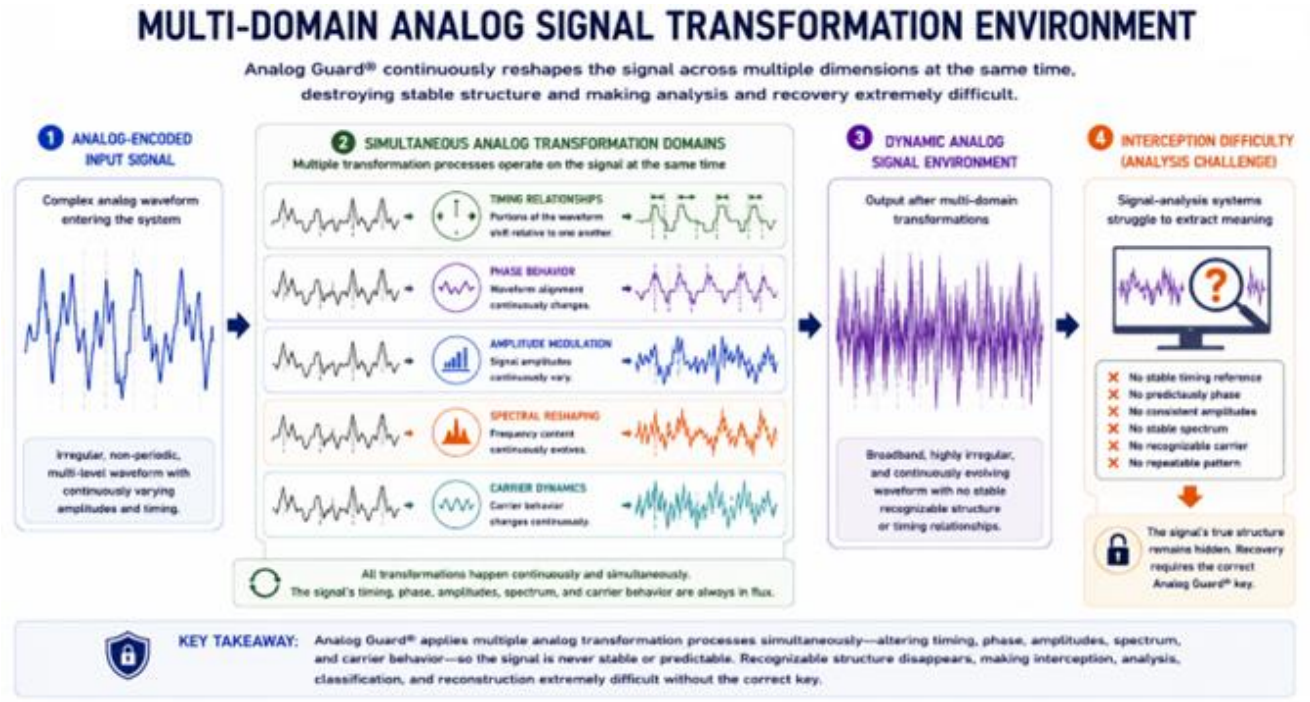

Figure 6. Multiple coordinated physical-layer transformation domains acting on the protected waveform.

8. Matched Analog Reconstruction and Recovery Failure

Figure 7 illustrates one of the invention's most important characteristics: successful decryption depends not only on possessing the correct key relationship, but also on reproducing the correct analog operating environment.

If the receiver successfully reproduces the proper analog conditions, the encrypted waveform can collapse back into recoverable information. If the analog conditions are incorrect, the recovered signal deteriorates into distortion and noise.

The concept is analogous to recreating a specific physical environment rather than simply supplying a password. Successful recovery depends on reproducing the collection of analog-state relationships that existed during protection, including timing, phase, carrier, and waveform conditions. If those relationships are not recreated with sufficient accuracy, the recovered information may be degraded or unrecoverable.

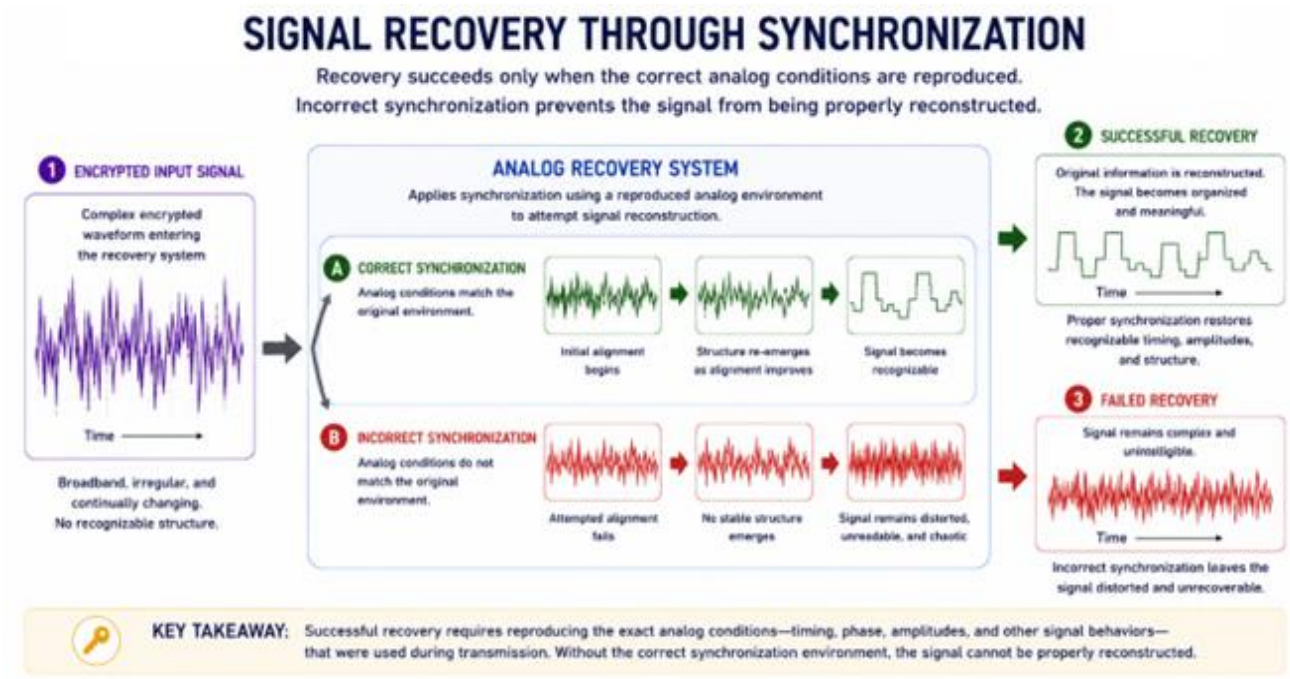

Figure 7. Matched analog conditions support recovery; mismatched conditions produce reconstruction failure.

This reconstruction requirement is one of the principal distinctions between the Analog Guard® approach and many conventional encryption architectures. In a purely digital system, possession of the correct key may be sufficient to recover information. In a reconstruction-dependent environment, recovery additionally depends on reproducing the broader collection of analog conditions that governed the original signal transformation process. The receiver must therefore recreate not only the correct informational relationship, but also the corresponding signal environment. From a security perspective, this means that successful recovery depends upon reproducing a broader set of conditions than would typically be required by a conventional digital encryption system. Recovery becomes dependent on the combined behavior of the analog environment rather than solely on possession of a digital secret. In this sense, successful recovery becomes an act of reconstruction rather than simply decryption.

The patent materials describe experimental behavior in which matched analog conditions allow recovery while mismatched conditions fail to reconstruct the original signal accurately [10,11]. Spectral analysis also shows that the encrypted waveform becomes redistributed and noise-like compared to the original transmission.

9. Strategic Implications

This low-observability property may represent one of the technology's strategically significant implications. In many modern encrypted systems, the message contents are hidden while the transmission itself remains visible and classifiable. Analog Guard® is directed to concealing both the information and the recognizable structure of the signal carrying it.

That places the architecture at the intersection of cybersecurity, advanced communications engineering, signal intelligence, electromagnetic spectrum operations, and electronic warfare [3-7].

The central design implication is that future secure communications may need to protect the signal environment, not merely the message payload [2-4]. Observable properties of the signal environment can themselves become components of the security architecture.

This perspective aligns with a broader trend toward hardware-rooted trust, physical-layer security, and signal-centric protection architectures. As signal-analysis capabilities continue to advance through automation and machine learning, future communication systems may increasingly require protection mechanisms that address not only information content but also the physical characteristics of the transmission itself.

This does not imply that traditional cryptography becomes less important. Rather, it suggests that future secure systems may increasingly combine computational security with physical-layer security mechanisms, creating multiple complementary barriers to unauthorized analysis and recovery.

For aerospace, defense, critical infrastructure, and high-assurance communications, that distinction may become increasingly important as adversaries focus on classification, detection, and exploitation of signal behavior rather than only message decryption.

10. Conclusion

Analog Guard® proposes a different model for how secure communications can be implemented. Rather than assuming that security exists only within software algorithms, the architecture treats the waveform itself as part of the protected object. The physical-layer behavior of the signal itself becomes an integral component of the encryption process.

In that sense, the technology is not merely another encryption algorithm. It proposes a broader shift in how secure communications may be designed: protection emerges not solely from mathematics, but from the dynamic behavior of the dynamic behavior of the physical-layer mixed-signal environment itself.

The approach should be understood as complementary to strong cryptography, secure hardware, authentication protocols, and post-quantum migration efforts [1,4,7]. Its distinct contribution is the extension of trust and protection becomes embedded within the waveform environment through which information is carried, transformed, and reconstructed. Whether ultimately deployed in cybersecurity, secure communications, aerospace systems, critical infrastructure, or spectrum-dominance applications, the underlying principle remains the same: protection is no longer confined to mathematical operations performed on data. Instead, protection becomes embedded within the physical-layer mixed-signal environment through which information is carried, transformed, and reconstructed.

Stated simply, Analog Guard® seeks to move part of the security burden from software and keys into the behavior of the signal itself. Whether future systems ultimately adopt all or only portions of this approach, the underlying concept expands the range of tools available for protecting information in increasingly contested communications environments.

References

[1] C. E. Shannon, "Communication Theory of Secrecy Systems," *Bell System Technical Journal*, vol. 28, no. 4, pp. 656-715, Oct. 1949.

[2] A. D. Wyner, "The Wire-Tap Channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355-1387, Oct. 1975.

[3] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge, U.K.: Cambridge University Press, 2011.

[4] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of Physical Layer Security in Multiuser Wireless Networks: A Survey," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 3, pp. 1550-1573, 2014.

[5] J. Hall, M. Barbeau, and E. Kranakis, "Radio Frequency Fingerprinting for Intrusion Detection in Wireless Networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 12, no. 1, pp. 1-14.

[6] B. Danev, T. S. Heydt-Benjamin, and S. Capkun, "Physical-Layer Identification of RFID Devices," *USENIX Security Symposium*, 2009.

[7] R. Maes, *Physically Unclonable Functions: Constructions, Properties and Applications*. Berlin, Germany: Springer, 2013.

[8] L. Kocarev, "Chaos-Based Cryptography: A Brief Overview," *IEEE Circuits and Systems Magazine*, vol. 1, no. 3, pp. 6-21, 2001.

[9] C. M. Hymel, M. H. Skolnick, R. A. Stubbers, and M. E. Brandt, "Temporally Advanced Signal Detection: A Review of the Technology and Potential Applications," *IEEE Circuits and Systems Magazine*, vol. 11, no. 3, pp. 35-54, 2011.

[10] N A Otman, et al, *Signal Protection and Retrieval by Non-Linear Analog Modulation*, U.S. Patent 12,126,720, Oct. 22, 2024.

[11] N A Otman, et al, *Signal Protection and Retrieval by Non-Linear Analog Modulation*, U.S. Patent 12,615,149, Apr. 14, 2026.

Appendix A. Figure Inventory

Figure	Working Title	Purpose
1	Dynamic Analog Signal Environment	Transmission concealed within a continuously evolving analog environment.
2	Binary-to-Analog Conversion and Dynamic Carrier	Binary information converted into analog waveform behavior before encryption.
3	Parallel Analog-Encrypted Paths	Independent signal paths remain separate until receiver-side recovery and binary reconstruction.
4	Temporal Encryption and PLTNM	Phase-linked temporal modulation alters waveform timing, amplitude, and signal geometry.
5	Resonance and Timing Distortion	Signal behavior changes through resonant, phase, and timing-related transformations.
6	Multidimensional Transformation Domains	Multiple coordinated transformation domains act on the protected waveform.
7	Matched Reconstruction Environment	Recovery depends on reproducing the correct analog reconstruction conditions.

Appendix B. Key Terms

Term	Working Meaning in This White Paper
Analog Guard®	A mixed-signal encryption architecture that uses analog waveform behavior as part of the protection mechanism.
Dynamic carrier	A carrier environment whose behavior participates in encryption rather than merely transporting encrypted bits.
PLTNM	Phase-Linked Temporal Nonlinear Modulation; a modulation approach that alters timing, phase, amplitude, and waveform geometry through analog processes.
Analog-state environment	The carrier, timing, phase, resonance, waveform, and modulation conditions that influence recoverability.
Negative group delay	A phase-related signal effect in which waveform envelope behavior can appear advanced without implying causality violation.
Matched analog reconstruction	Recovery condition in which the receiver reproduces the analog environment needed to recover the protected information.
Low observability	Reduced recognizability of the transmission’s structure, timing, carrier behavior, spectral features, or modulation patterns.