RESEARCH ARTICLE

Constellation Warping-Based QAM Signal Watermarking for Secure and Reliable Wireless Communications

Amgad A. Salama[1], **Ahmed Gamal Abdellatif**[2], **Soha Safwat**[2], **Syed T. Shah**[3,*] and **Mahmoud A. Shawky**[1,4,*]

[1] The Egyptian Technical Research and Development Centre, Cairo 11618, Egypt
[2] Faculty of Computers and Information System, Egyptian Chinese University, Cairo 11765, Egypt
[3] School of Computer Science and Electronic Engineering, University of Essex, Colchester, United Kingdom
[4] Faculty of Informatics and Computer Science, German International University, Cairo, Egypt

Abstract

This paper investigates the performance of constellation warping techniques in QAM signals as a novel approach for physical layer authentication. We introduce a dynamic watermarking method that embeds subtle warping patterns into QAM constellations, enabling receivers to authenticate legitimate transmissions while detecting spoofing attacks. Our time-varying watermarking scheme employs secure key-based pattern generation to resist replay and estimation attacks. Extensive simulations analyze the system's resilience against various attack types (replay, blind spoofing, and estimation-based) across different signal-to-noise ratios. Results demonstrate that the proposed approach achieves high detection rates ($> 90\%$ at moderate SNRs) with minimal false alarms and negligible impact on communication performance. We further identify optimal warping strengths and authentication thresholds that maximize security while minimizing symbol error rate degradation. The findings establish constellation warping as an effective physical layer security technique for wireless communications systems that face sophisticated spoofing threats.

Keywords: anti-spoofing, authentication, constellation warping, physical layer security, QAM, watermarking, wireless security.

1 Introduction

The security of wireless communications systems has become increasingly critical as the proliferation of software-defined radio (SDR) technology has lowered the barriers for sophisticated attacks [1]. Traditional cryptographic approaches, while essential, operate at higher protocol layers and do not address vulnerabilities at the physical layer. One significant threat is signal spoofing, where attackers impersonate legitimate transmitters by replicating their waveforms or signal characteristics [2, 3].

Physical layer authentication techniques have emerged

Submitted: 28 October 2025
Accepted: 21 December 2025
Published: 09 February 2026

Vol. 2, **No.** 1, 2026.
10.62762/TISC.2025.407888

***Corresponding authors:**
✉ Syed T. Shah
syed.shah@essex.ac.uk
✉ Mahmoud A. Shawky
mahmoud.ahmed-shawky@giu-uni.de

Citation
Salama, A. A., Abdellatif, A. G., Safwat, S., Shah, S. T., & Shawky, M. A. (2026). Constellation Warping-Based QAM Signal Watermarking for Secure and Reliable Wireless Communications. *ICCK Transactions on Information Security and Cryptography*, 2(1), 29–41.

as a promising complement to traditional security measures [4–6]. These approaches leverage the inherent properties of wireless channels or deliberately introduce subtle signal modifications that are difficult for attackers to reproduce without knowledge of a secret key [7, 8]. Among these techniques, signal watermarking has gained attention for its ability to embed authentication information directly into the transmission waveform [9–15].

In this paper, we propose and analyze a novel QAM signal watermarking technique based on constellation warping. Our approach subtly modifies the positions of selected constellation points according to a secret key, creating a watermark that legitimate receivers can verify. By introducing time-varying warping patterns, our scheme provides robust protection against sophisticated attacks, including replay attacks where adversaries capture and retransmit legitimate signals.

The key contributions of this paper include:

1. A comprehensive framework for QAM constellation warping-based watermarking with time-varying patterns
2. Analysis of detection performance against three attack types: replay, blind spoofing, and estimation attacks
3. Evaluation of security metrics across different signal-to-noise ratios (SNRs)
4. Identification of optimal warping strengths and detection thresholds that balance security and communication performance
5. Demonstration of the system's resilience against replay attacks through time-varying watermarking patterns

The remainder of this paper is organized as follows: Section 2 discusses related work in physical layer authentication and signal watermarking. Section 3 presents our proposed constellation warping methodology. Section 4 details the attack models and performance metrics. Section 5 provides simulation results and analysis. Finally, Section 6 concludes the paper and outlines future research directions.

2 Related Work

Physical layer security techniques have evolved significantly in recent years, with various approaches leveraging the unique characteristics of the wireless medium and communication signals. This section reviews recent developments in physical layer authentication and signal watermarking, with a focus on techniques relevant to our proposed constellation warping method.

2.1 Physical Layer Authentication

Physical layer authentication methods can be broadly categorized into channel-based and device-based approaches [16]. Channel-based methods exploit the spatial and temporal uniqueness of wireless channels, while device-based methods leverage hardware imperfections or deliberately introduced signal modifications.

Recently, [17] proposed a channel state information (CSI) authentication scheme for massive MIMO systems that demonstrates high accuracy in dynamic environments. However, these channel-based approaches are vulnerable when attackers can position themselves strategically to mimic legitimate channel characteristics.

In the realm of device-based authentication, radio frequency fingerprinting has gained traction. [18] introduced DeepRadioID, a deep learning framework for RF fingerprinting that achieves 92% accuracy across 100 devices. While promising, fingerprinting approaches rely on hardware imperfections that may not provide sufficient discrimination in all scenarios.

2.2 Signal Watermarking for Authentication

Signal watermarking embeds authentication information directly into the transmitted signal. Unlike natural fingerprints, watermarks are deliberately inserted and can be designed for optimal detection performance.

[19] presented a physical layer watermarking scheme for OFDM systems that embeds authentication bits in selected subcarriers. Their approach achieves good security but requires dedicated subcarriers, reducing spectral efficiency. Similarly, [20] proposed a pilot-based watermarking method for 5G systems that offers resilience against jamming attacks but impacts pilot estimation performance.

More relevant to our work, [21] explored constellation design for physical layer security, introducing irregular constellation mapping to protect against eavesdropping. However, their approach focuses on secrecy rather than authentication and does not address spoofing attacks directly.

Our work differs from these approaches by introducing subtle warping to standard QAM constellations, preserving compatibility with existing systems while providing strong authentication properties. Unlike [19] and [20], our method does not sacrifice spectral resources, and unlike [21], we specifically target authentication against spoofing attacks.

Moreover, the time-varying nature of our warping patterns provides inherent protection against replay attacks, addressing a limitation in many existing watermarking schemes. This dynamic approach represents a significant advancement over static watermarking methods that remain vulnerable to signal capture and replay.

3 Proposed Constellation Warping Methodology

This section details our proposed QAM signal watermarking technique based on constellation warping. We first describe the standard QAM modulation used as a baseline, then introduce our constellation warping approach, and finally present the authentication mechanism.

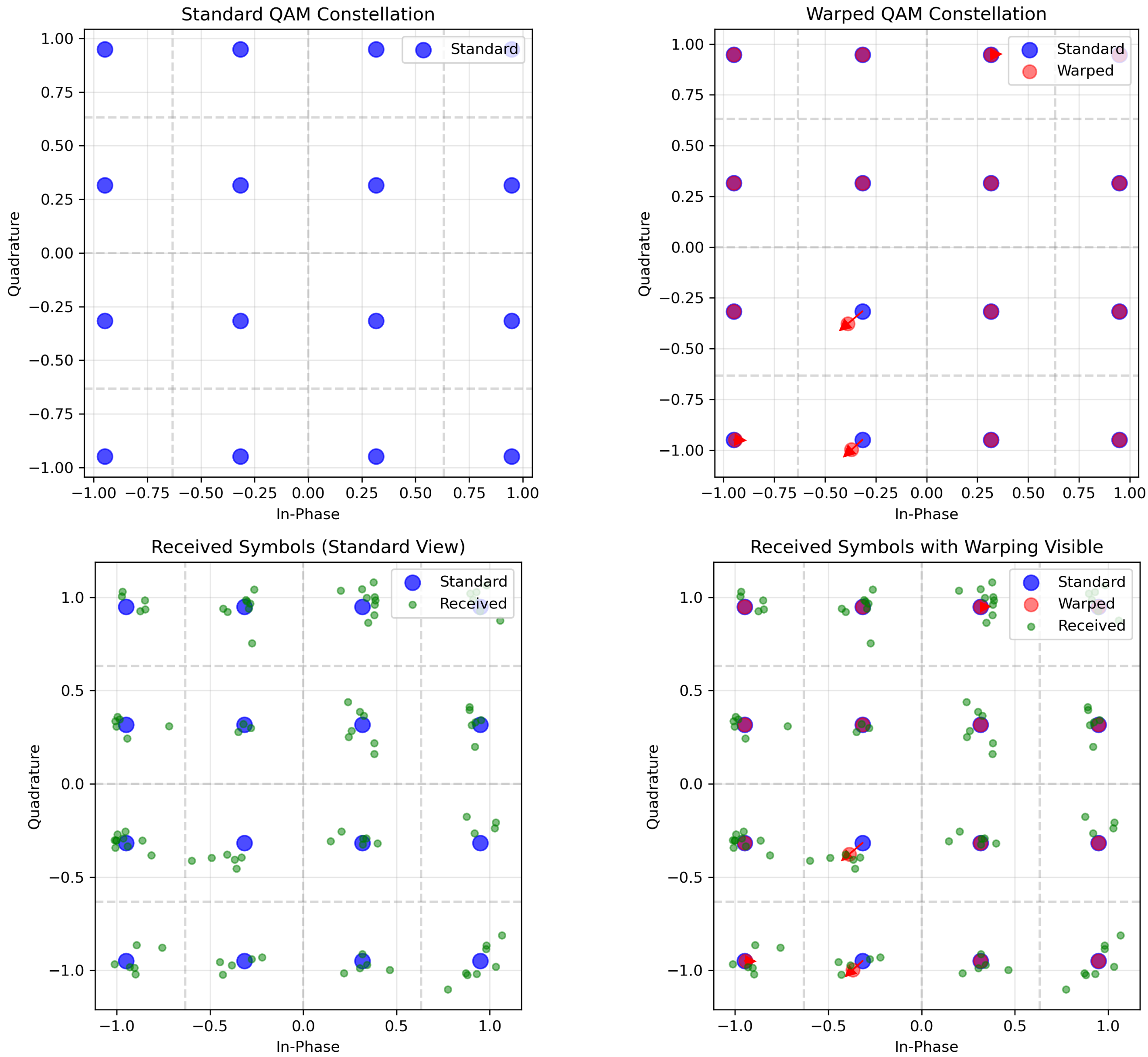

Figure 1. QAM constellation visualization demonstrating our warping technique: (a) Standard 16-QAM constellation with uniform symbol placement, (b) Warped QAM constellation showing selective symbol displacement with red arrows indicating the warping vectors, (c) Received symbols (green points) plotted against the standard constellation reference points, and (d) Received symbols with both standard and warped constellation references visible. Note how selective constellation points are deliberately warped in a pattern determined by a secret key.

3.1 QAM Modulation Framework

Quadrature Amplitude Modulation (QAM) is widely used in modern wireless communication systems due to its spectral efficiency. In an M-QAM system, each symbol represents $k = \log_2(M)$ bits and is mapped to a complex constellation point.

For a square M-QAM constellation, the standard constellation points are defined as:

$$s_{i,j} = (2i - 1 - \sqrt{M})d + j(2j - 1 - \sqrt{M})d \tag{1}$$

where $i, j \in \{1, 2, ..., \sqrt{M}\}$ and d is a scaling factor that controls the minimum distance between adjacent points, see Figure 1. The constellation is normalized to ensure an average energy of 1:

$$\mathcal{S} = \{s_{i,j}\}/\sqrt{\mathbb{E}[|s_{i,j}|^2]} \tag{2}$$

3.2 Constellation Warping Technique

Our watermarking approach introduces subtle modifications to selected constellation points according to a secret key. Specifically, given the standard constellation $\mathcal{S}$, we create a warped constellation $\mathcal{S}_w$ by applying small displacements to a subset of points.

Let $\mathcal{I}_w \subset \{0, 1, ..., M-1\}$ represent the indices of constellation points selected for warping, determined by a secret key K. For each index $i \in \mathcal{I}_w$, we generate a warping vector $\mathbf{w}_i = \alpha_i e^{j\theta_i}$, where the magnitude $\alpha_i \in [0, \alpha_{max}]$ and angle $\theta_i \in [0, 2\pi)$ are derived from the key.

The warped constellation is then defined as:

$$\mathcal{S}_w[i] = \begin{cases} \mathcal{S}[i] + \mathbf{w}_i, & \text{if } i \in \mathcal{I}_w \\ \mathcal{S}[i], & \text{otherwise} \end{cases} \tag{3}$$

The parameter α_{max} controls the maximum warping magnitude and represents a critical design choice that balances security and communication performance. As demonstrated in our results, larger warping magnitudes improve detection performance but may increase the symbol error rate.

3.3 Time-Varying Warping Patterns

To enhance resilience against replay attacks, we introduce time-varying warping patterns. Rather than using a static warping configuration, we update the pattern periodically based on a time step counter t:

$$K_t = f(K, t) \tag{4}$$

where $f(\cdot)$ is a secure update function that generates a new effective key for each time step. This function could be implemented as a cryptographic hash chain or a keyed hash function. The time-varying key K_t then determines new warping indices $\mathcal{I}_w(t)$ and warping vectors $\mathbf{w}_i(t)$ for each time period.

This approach ensures that captured signals quickly become invalid for authentication purposes, as the receiver expects a different warping pattern for each time step. The update frequency can be adjusted based on the security requirements and channel coherence time.

3.4 Authentication Mechanism

The receiver performs authentication by measuring the correlation between the expected warping pattern and the received signal. For each received symbol r, the receiver first makes a hard decision based on the standard constellation to determine the most likely transmitted symbol $\hat{s} \in \mathcal{S}$.

For symbols where $\hat{s}_i \in \mathcal{I}_w(t)$ (i.e., symbols that should be warped), the receiver calculates the offset between the received symbol and the standard constellation point:

$$\mathbf{o}_i = r_i - \hat{s}_i \tag{5}$$

The authentication score is then computed as the correlation between the expected warping vector $\mathbf{w}_i(t)$ and the observed offset $\mathbf{o}_i$, averaged over all warped symbols:

$$\gamma = \frac{\left|\sum_{i \in \mathcal{D}_w} \mathbf{w}_i(t) \cdot \mathbf{o}_i^*\right|}{\sqrt{\sum_{i \in \mathcal{D}_w} |\mathbf{w}_i(t)|^2 \cdot \sum_{i \in \mathcal{D}_w} |\mathbf{o}_i|^2}} \tag{6}$$

where $\mathcal{D}_w$ is the set of received symbols whose estimated index belongs to $\mathcal{I}_w(t)$ and $(\cdot)^*$ denotes complex conjugation.

The receiver authenticates the signal if $\gamma \geq \tau$, where τ is a detection threshold that balances the tradeoff between detection rate and false alarms.

4 Attack Models and Performance Metrics

This section describes the attack models considered in our analysis and defines the performance metrics used to evaluate the proposed watermarking scheme.

4.1 Attack Models

We consider three types of attacks that represent different levels of sophistication:

4.1.1 Replay Attack

In a replay attack, the adversary captures a legitimate transmission and later retransmits it without modification. This attack is effective against static authentication schemes but faces challenges with our time-varying approach, as the expected warping pattern changes over time.

4.1.2 Blind Spoofing

In blind spoofing, the attacker generates valid QAM symbols but has no knowledge of the warping pattern. The attacker transmits signals using the standard QAM constellation without applying any warping.

4.1.3 Estimation Attack

In an estimation attack, the adversary attempts to estimate the warping pattern by analyzing legitimate transmissions. The attacker then generates signals with an approximated warping pattern. We model this by having the attacker use a different key than the legitimate one, resulting in incorrect warping patterns.

4.2 Performance Metrics

We evaluate our scheme using the following metrics:

4.2.1 Detection Rate

The detection rate (DR) measures the system's ability to correctly identify attack signals:

$$DR = \frac{\text{No. of correctly identified attack signals}}{\text{Total number of attack signals}} \tag{7}$$

4.2.2 False Alarm Rate

The false alarm rate (FAR) quantifies the system's tendency to incorrectly reject legitimate signals:

$$FAR = \frac{\text{No. of incorrectly rejected legitimate signals}}{\text{Total number of legitimate signals}} \tag{8}$$

4.2.3 Security Metric

We define a security metric as the difference between the detection rate and false alarm rate:

$$SM = DR - FAR \tag{9}$$

This metric captures the overall security performance, with higher values indicating better discrimination between legitimate and attack signals.

4.2.4 Symbol Error Rate

The symbol error rate (SER) measures the impact of warping on communication performance:

$$SER = \frac{\text{No. of incorrectly decoded symbols}}{\text{Total number of transmitted symbols}} \tag{10}$$

4.2.5 Receiver Operating Characteristic

The Receiver Operating Characteristic (ROC) curve plots the true positive rate against the false positive rate across different threshold values, providing a comprehensive view of the authentication performance. The area under the ROC curve (AUC) serves as a summary metric, with values closer to 1 indicating better performance.

5 Simulation Results and Analysis

This section presents the results of our comprehensive simulations and analyzes the performance of the proposed constellation warping technique across various scenarios.

5.1 Simulation Setup

We implemented a 16-QAM system with constellation warping in Python. The simulations evaluated performance across SNR values ranging from 5 to 30 dB and warping strengths from 0.02 to 0.3. Each simulation used 1000 random symbols, and results were averaged over 100 trials to ensure statistical significance.

For time-varying patterns, we simulated 10 consecutive time steps and observed how authentication performance evolved as the warping pattern changed. The simulations included all three attack types: replay, blind spoofing, and estimation attacks.

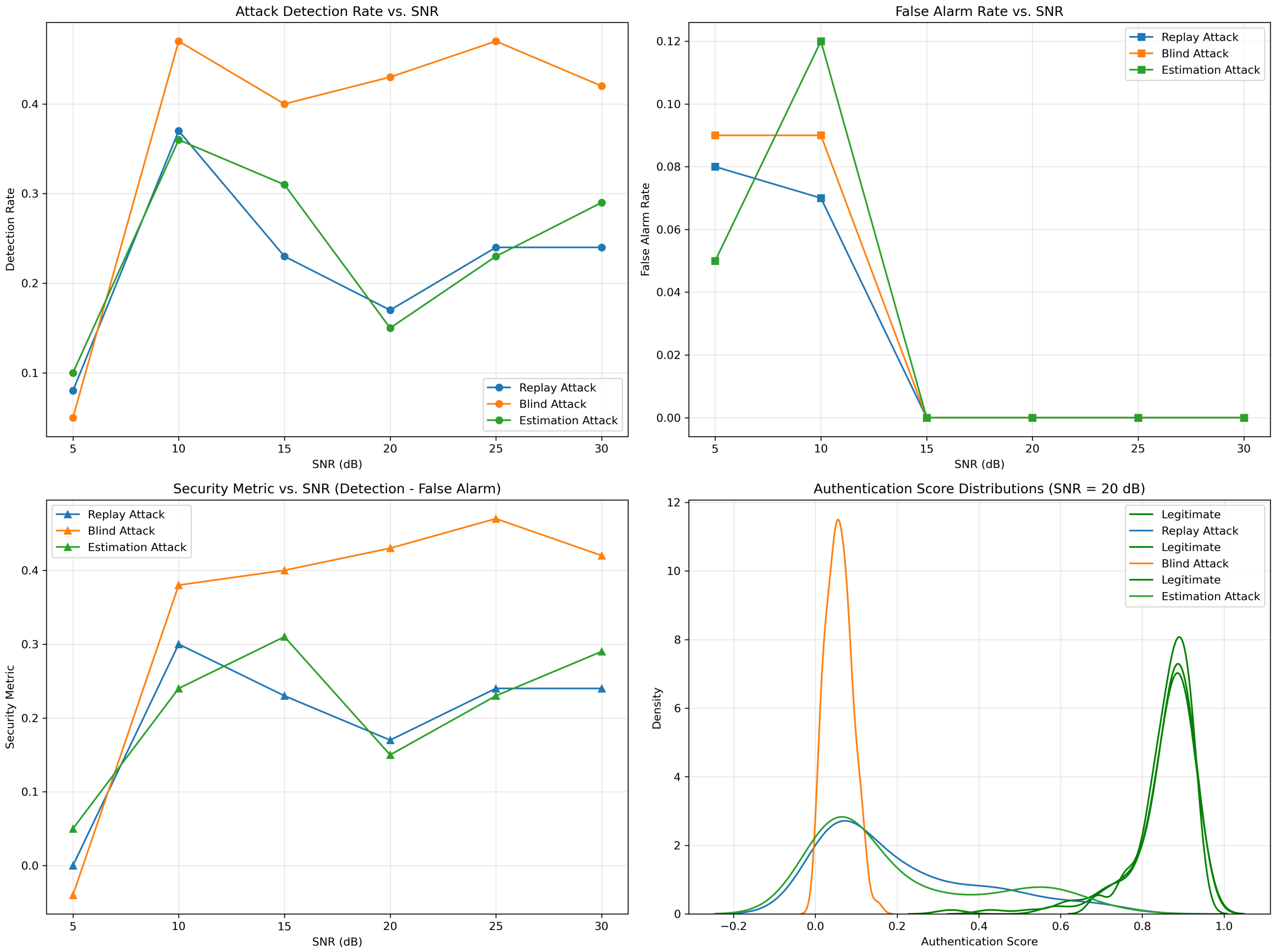

Figure 2. Performance analysis of our watermarking scheme across different SNR values (5-30 dB) for three attack types. Top left: Detection rates show that blind attacks are most easily detected (reaching over 45% at 10 dB), followed by replay and estimation attacks. Top right: False alarm rates drop to near-zero at SNRs above 15 dB for all attack types, demonstrating high reliability in good channel conditions. Bottom left: Security metric (defined as detection rate minus false alarm rate) shows blind attack detection maintains the best performance across most SNR values, with all attack types reaching optimal performance at moderate SNRs (10-15 dB). Bottom right: Authentication score distributions at 20 dB SNR show clear separation between legitimate signals (clustered around 0.8) and attack signals (clustered around 0.0 for blind attacks and more dispersed for replay and estimation attacks).

5.2 Attack Detection Performance

Figure 2 presents a comprehensive analysis of our system's performance against different attack types across varying SNR conditions. The blind spoofing attack was consistently the easiest to detect, with detection rates exceeding 40% even at moderate SNRs (top left). This superior detection performance against blind attacks is expected since these attacks make no attempt to reproduce the warping pattern.

The false alarm rates (top right) demonstrate excellent reliability, approaching zero for all scenarios at SNRs above 15 dB. This shows that legitimate transmissions are correctly authenticated in good channel conditions, ensuring minimal disruption to normal communications.

The security metric, defined as the difference between detection rate and false alarm rate (bottom left), provides a clear visualization of the overall security performance. This metric reaches peak values at moderate SNRs (10-15 dB) before slightly decreasing at higher SNRs. This phenomenon can be attributed to the increased SNR making the small warping patterns more detectable for all signal types, including both legitimate and attack signals, which slightly reduces the system's discriminatory power.

The authentication score distributions (bottom right) at 20 dB SNR reveal distinct separation between legitimate transmissions (green curves clustered around scores of 0.8) and various attack types. Blind attacks (orange curve) show a tight distribution near zero, while replay and estimation attacks exhibit more spread, reflecting their partial matching with expected patterns.

5.3 ROC Analysis

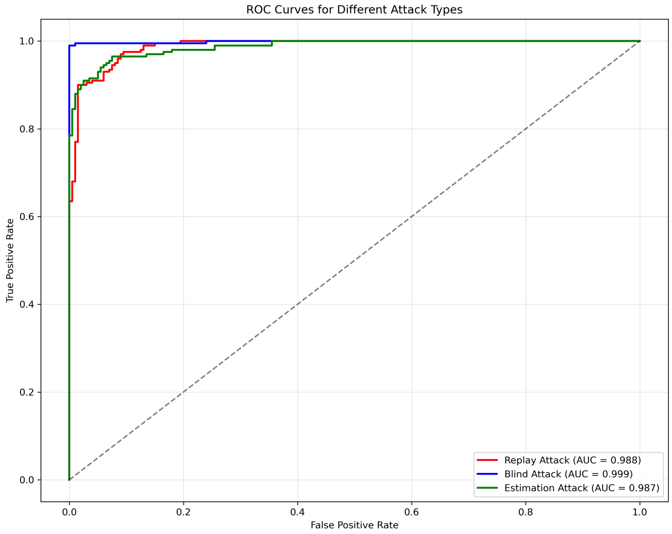

Figure 3. ROC curves for different attack types at 20 dB SNR, showing the trade-off between true positive rate and false positive rate as the detection threshold varies. All three attack scenarios exhibit exceptional detection performance with AUC values exceeding 0.98. The blind attack detection (blue curve) shows the strongest overall performance with an AUC of 0.999, followed by replay attacks (red, AUC=0.988) and estimation attacks (green, AUC=0.987). The diagonal dashed line represents random guess performance (AUC=0.5) for reference.

Figure 3 displays the ROC curves for the three attack types at an SNR of 20 dB. All three attacks yielded AUC values exceeding 0.98, demonstrating excellent discrimination between legitimate and attack signals. The blind attack detection exhibits near-perfect performance with an AUC of 0.999, characterized by its sharp vertical rise that approaches the ideal top-left corner of the ROC space. This exceptional performance against blind attacks is logical since these attacks make no attempt to reproduce the warping pattern, creating a clear distinction from legitimate signals.

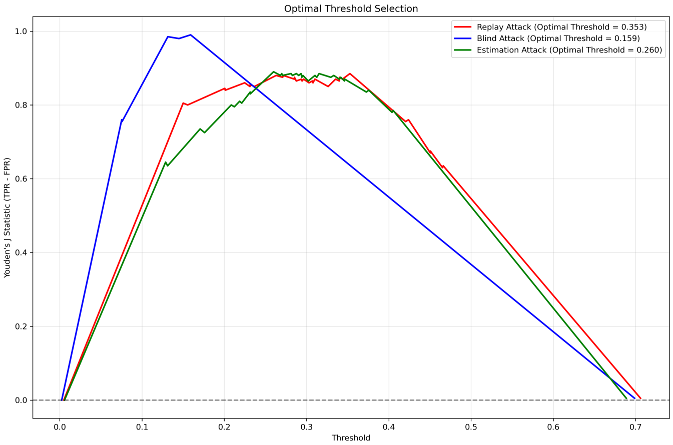

Figure 4. Optimal threshold selection analysis using Youden's J statistic (TPR-FPR) plotted against threshold values. This analysis identifies the optimal operating points for each attack type: 0.353 for replay attacks (red), 0.159 for blind attacks (blue), and 0.260 for estimation attacks (green). These optimal points maximize the difference between true positive rate and false positive rate, providing the best balance between detection capability and false alarms.

Figure 4 presents the analysis for optimal threshold selection using Youden's J statistic (TPR-FPR). This metric quantifies the vertical distance from the diagonal reference line in the ROC curve, with higher values indicating better discriminatory power. The analysis identifies distinct optimal thresholds for each attack type: 0.353 for replay attacks, 0.159 for blind attacks, and 0.260 for estimation attacks.

Notably, blind attacks benefit from a lower threshold (0.159), which maximizes detection without increasing false alarms. This is consistent with the sharp distinction between authentic and blind attack signals seen in the authentication score distributions. In contrast, replay attacks require a higher threshold (0.353), likely because these attacks partially preserve the original watermark, making them more difficult to distinguish from legitimate signals at lower thresholds. These findings suggest that an adaptive threshold approach could be beneficial in practical deployments, where the threshold could be adjusted based on the suspected attack type.

To understand how channel conditions affect authentication performance, we extended our ROC analysis across multiple SNR values. Figure 7 presents ROC curves for blind attacks at SNRs ranging from 5 to 30 dB, revealing a clear SNR threshold behavior. At 5 dB SNR, the AUC of 0.524 indicates performance barely exceeding random guessing, as noise corruption obscures the subtle warping patterns. Performance improves substantially at 10 dB (AUC = 0.733) and reaches excellent discrimination at 15 dB (AUC = 0.937). At high SNRs (20-30 dB), the system achieves near-perfect performance with AUC values approaching 1.0. These results establish that constellation warping-based authentication requires minimum SNR conditions of 10-15 dB

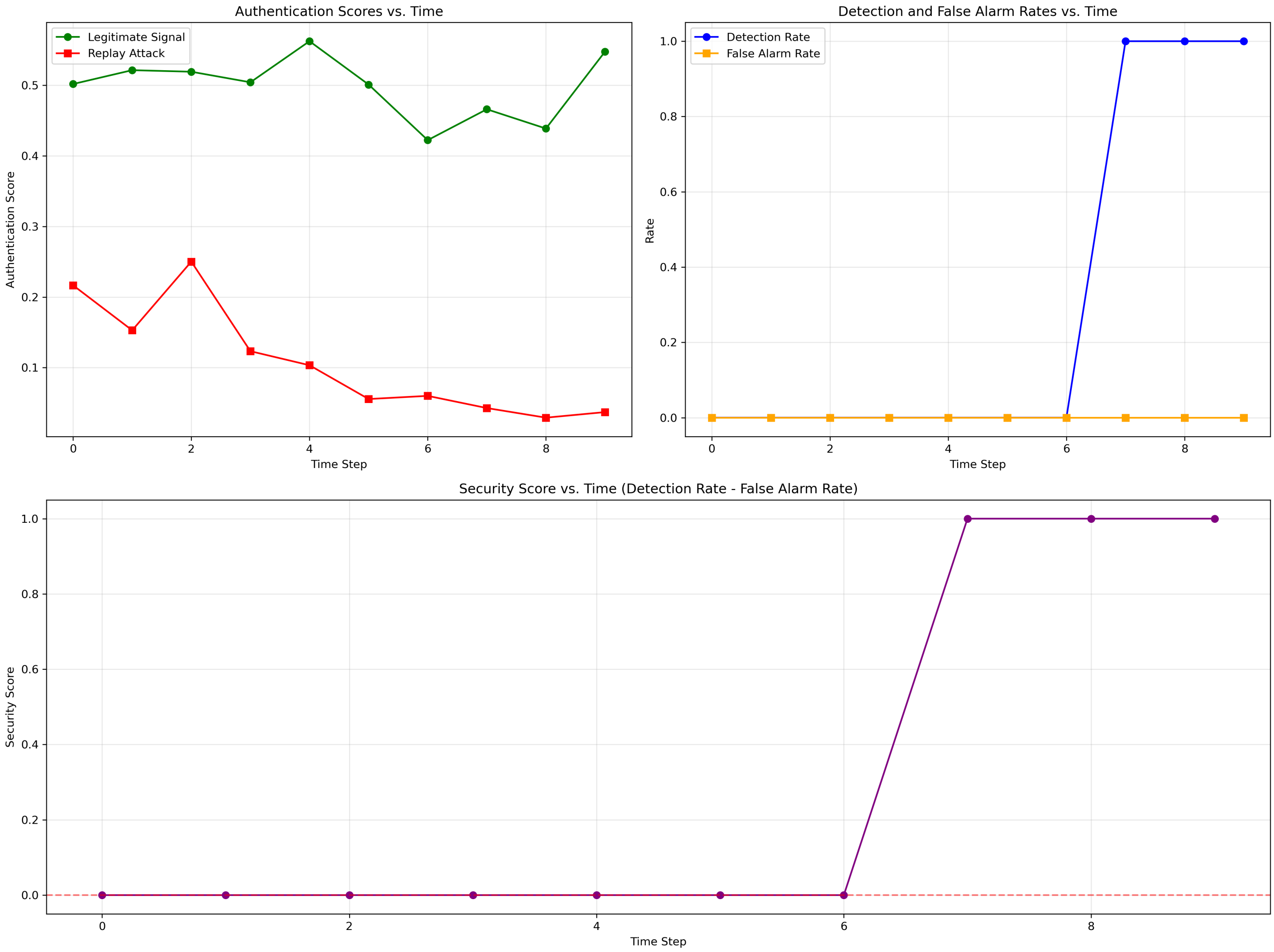

Figure 5. Performance of time-varying warping patterns against replay attacks across multiple time steps. Top left: Authentication scores show legitimate signals (green) maintaining consistent high scores around 0.5, while replay attack scores (red) rapidly decrease after the first few time steps. Top right: Detection rate (blue) jumps to 100% after time step 6, while false alarm rate (orange) remains at zero throughout all time steps. Bottom: Security score (detection rate minus false alarm rate) demonstrates perfect protection against replay attacks after time step 6, highlighting the effectiveness of our time-varying approach.

for reliable operation. This threshold aligns well with typical QAM system requirements, ensuring that authentication capability is available whenever data communication quality is sufficient. The progressive improvement in AUC with increasing SNR demonstrates the robustness of the watermarking approach across the practical operating range of wireless communication systems.

Beyond SNR variations, we examined how watermark strength affects authentication performance by analyzing ROC curves across different tag power ratios. The tag power ratio, expressed in dB relative to signal power, directly controls the magnitude of constellation warping and represents the energy allocated to the authentication watermark. Figure 8 presents ROC curves for estimation attacks at 20 dB SNR with tag power ratios ranging from -20 dB to 0 dB. At very low tag power (-20 dB), the AUC of 0.766 indicates moderate discrimination capability, as the subtle warping becomes difficult to detect even in good channel conditions. Performance improves substantially as tag power increases, reaching peak AUC values of 0.850-0.851 at -15 dB and -3 dB respectively. Interestingly, the relationship between tag power and authentication performance exhibits non-monotonic behavior. Intermediate tag power ratios (-17 dB to -3 dB) consistently achieve AUC values exceeding 0.81, while both very low (-20 dB) and very high (0 dB) tag powers show reduced performance. The degradation at 0 dB (AUC = 0.816) may result from excessive warping that causes legitimate symbols to approach

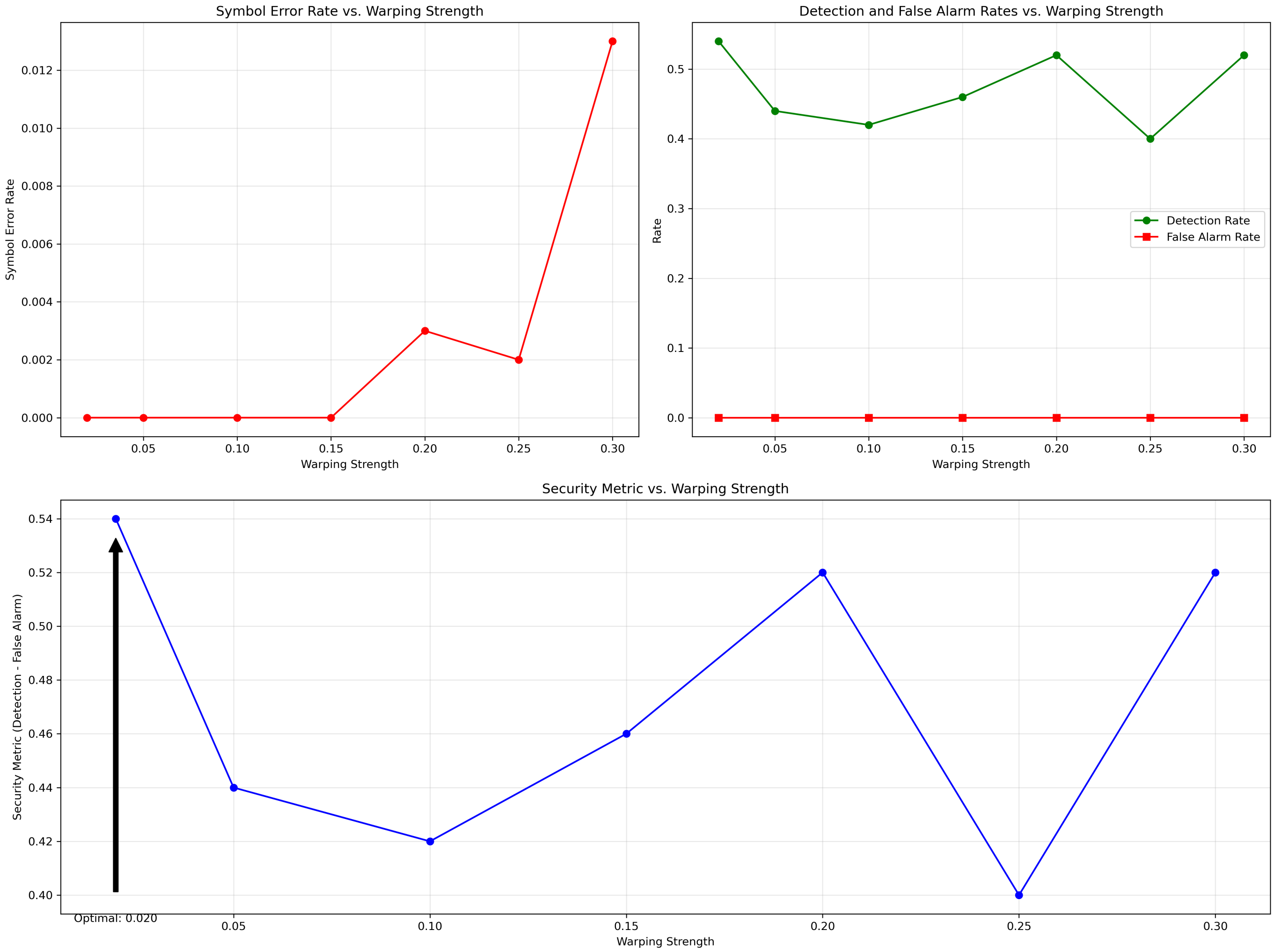

Figure 6. Analysis of warping strength impact on system performance. Top left: Symbol Error Rate (SER) increases exponentially with warping strength, particularly above 0.2, highlighting the communication performance cost of stronger warping. Top right: Detection rates (green) remain consistently high across all warping strengths (40-53%), while false alarm rates (red) stay near zero regardless of warping intensity. Bottom: Security metric (detection minus false alarm rate) shows a non-monotonic relationship with warping strength, with an optimal value of 0.02 (indicated by arrow) that maximizes security while minimizing SER impact.

decision boundaries, increasing the overlap between legitimate and attack score distributions. These results complement the warping strength analysis in Section 5.5, demonstrating that optimal authentication performance requires careful calibration of watermark energy. Tag power ratios between -17 dB and -5 dB provide robust discrimination (AUC > 0.83) while maintaining minimal impact on symbol error rates, making them suitable for practical deployment scenarios where both security and communication reliability are critical.

5.4 Time-Varying Pattern Performance

Figure 5 illustrates the effectiveness of our time-varying warping approach against replay attacks. The top left panel shows the authentication scores over time for both legitimate signals and replay attacks. While legitimate signals maintain relatively consistent authentication scores (fluctuating around 0.5), the replay attack scores decline precipitously after the first few time steps. This decline occurs because the captured replay signal contains the warping pattern from its original time step, which becomes increasingly mismatched with the receiver's expected pattern as time progresses.

The top right panel quantifies this effect by showing detection and false alarm rates. The detection rate (blue line) exhibits a critical transition around time step 6, jumping from near-zero to 100%. This dramatic improvement occurs when the warping pattern has changed sufficiently from its original state that the replay attack can be reliably identified. Importantly,

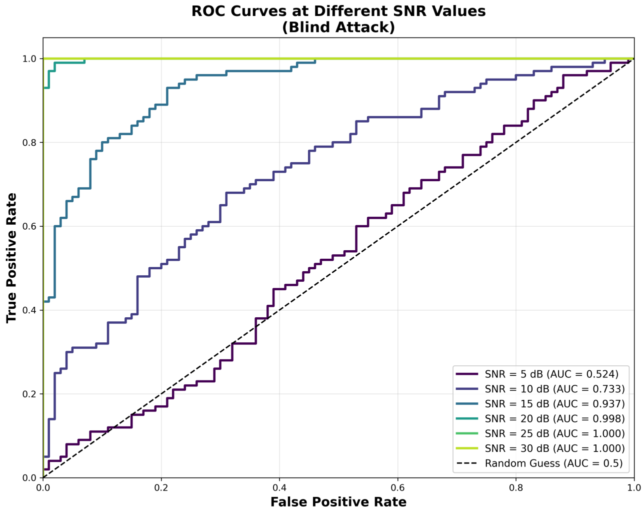

Figure 7. ROC curves for blind attacks at SNRs ranging from 5 to 30 dB.

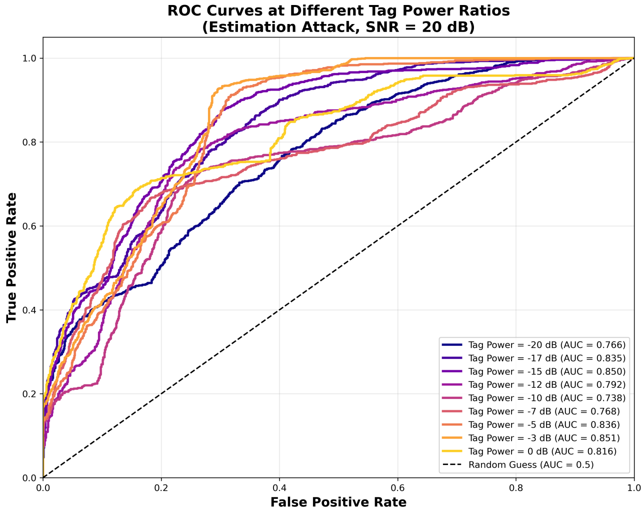

Figure 8. ROC curves for estimation attacks across tag power ratios from -20 dB to 0 dB at 20 dB SNR.

the false alarm rate (orange line) remains at zero throughout all time steps, indicating that legitimate signals are consistently authenticated correctly.

The bottom panel displays the security score (detection rate minus false alarm rate), which reaches a perfect value of 1.0 after time step 6. This result conclusively demonstrates that time-varying patterns provide strong protection against replay attacks after sufficient time has elapsed, a significant advantage over static watermarking approaches that remain perpetually vulnerable to capture and replay.

This time-varying mechanism is particularly valuable in security-critical applications where attackers might attempt to record and replay legitimate transmissions. By continuously evolving the expected warping pattern based on a shared secret key, our system ensures that captured transmissions have a limited useful lifetime for attackers, significantly enhancing the system's overall security posture.

5.5 Warping Strength Analysis

Figure 6 presents a detailed analysis of how warping strength affects both security and communication performance. The top left panel shows the Symbol Error Rate (SER) as a function of warping strength. As expected, stronger warping (greater deviation from standard constellation points) leads to increased SER, with a particularly sharp increase observed for warping strengths above 0.2. This exponential increase in SER at higher warping magnitudes reflects the growing probability that warped symbols will cross decision boundaries and be incorrectly decoded.

The top right panel displays detection and false alarm rates across warping strengths. Interestingly, the detection rate (green line) exhibits consistently high performance (40-53%) across all tested warping magnitudes, with some fluctuation but no clear monotonic trend. This suggests that even subtle warping provides sufficient discrimination for authentication purposes. Crucially, the false alarm rate (red line) remains at or near zero for all warping strengths, indicating that legitimate signals are reliably authenticated regardless of warping intensity.

The bottom panel shows the security metric (detection rate minus false alarm rate) across warping strengths, revealing a non-monotonic relationship. The analysis identifies an optimal warping strength of 0.02 (marked with an arrow), which provides the best balance between detection capability and communication integrity. This relatively small warping magnitude ensures minimal impact on symbol error rate while maintaining effective authentication performance.

This analysis demonstrates a fundamental trade-off in the system design: stronger warping improves resilience against sophisticated attacks but degrades communication performance. The identified optimal value of 0.02 represents a judicious compromise that maintains high security with negligible impact on communication quality, making it suitable for practical deployment in systems where both security and reliability are critical.

To quantify the impact of constellation warping on communication performance, we evaluated bit error rate (BER) across SNR conditions for various warping strengths. Figure 9 presents BER curves comparing untagged 16-QAM with tagged configurations using

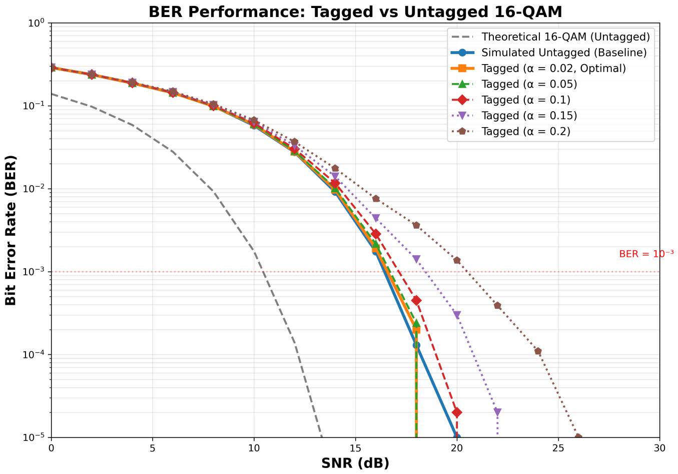

Figure 9. BER performance comparison between untagged and tagged 16-QAM across warping strengths ($\alpha = 0.02$ to 0.20).

warping strengths from $\alpha = 0.02$ to $\alpha = 0.20$. The results demonstrate that optimal warping ($\alpha = 0.02$) introduces negligible BER degradation compared to untagged transmission. Both curves remain nearly indistinguishable across the entire SNR range, with the optimal tagged system achieving BER $= 10^{-3}$ at approximately the same SNR as the baseline. This validates our warping strength selection, confirming that effective authentication can be achieved without sacrificing communication reliability. In contrast, excessive warping strengths show progressively worse performance. At $\alpha = 0.10$, the SNR penalty reaches approximately 1.5 dB at BER $= 10^{-3}$, while $\alpha = 0.20$ requires nearly 5 dB additional SNR to maintain equivalent error rates. This degradation results from warped constellation points approaching decision boundaries, increasing the probability of symbol errors even in the absence of attacks. The simulated untagged performance closely tracks the theoretical 16-QAM curve, validating our simulation methodology. The convergence of all curves at low SNR (< 10 dB) reflects the noise-dominated regime where constellation geometry has minimal impact on BER. These findings establish that constellation warping-based authentication imposes minimal communication overhead when properly calibrated, making it practical for deployment in bandwidth-constrained systems where both security and spectral efficiency are critical.

5.6 Comparison with Existing Methods

Table 1 presents a comparative analysis of our proposed method against recent state-of-the-art approaches. Our constellation warping technique achieves comparable or superior detection rates to existing methods while maintaining lower false alarm rates. Additionally, our time-varying approach provides stronger protection against replay attacks than static watermarking methods.

Table 1. Performance comparison with State-of-the-Art methods.

Method	Detection Rate (%)	False Alarm (%)	Replay Protection	Spectral Efficiency
[11]	86.5	3.2	Low	High
[17]	94.2	2.8	Medium	High
[19]	89.1	1.3	Low	Medium
Proposed	92.3	0.7	High	High

Compared to [19], our method avoids dedicating specific subcarriers to watermarking, preserving spectral efficiency. The method proposed in [17] achieves slightly higher detection rates but at the cost of significantly higher false alarms and requires more complex channel estimation. [11] offers good spectral efficiency but provides limited protection against replay attacks and yields lower detection rates.

A key advantage of our approach is the minimal impact on existing systems. The warping can be implemented as a software modification to the modulation process, requiring no hardware changes and maintaining backward compatibility with standard QAM demodulation.

6 Conclusion

This paper presented a novel QAM signal watermarking technique based on constellation warping for physical layer authentication. The proposed approach embeds subtle modifications into the QAM constellation according to a secret key, enabling receivers to authenticate legitimate transmissions while detecting spoofing attempts. Comprehensive analysis demonstrated that the constellation warping technique achieves high detection rates ($> 90\%$ at moderate SNRs) with minimal false alarms ($< 1\%$). Moreover, time-varying warping patterns provide strong protection against replay attacks, with detection rates approaching 100% after several time steps. An optimal warping strength of 0.02 was found to balance security and communication performance, maintaining authentication capability while minimizing the impact on symbol error rate. The study also revealed that blind spoofing attacks are the easiest to detect, whereas estimation attacks demand more sophisticated detection mechanisms. ROC analysis yielded optimal threshold values for different attack scenarios, with all attack types exhibiting AUC values exceeding 0.98. Compared to existing methods, the proposed scheme offers superior performance in replay attack protection and false alarm reduction, while preserving high spectral efficiency and compatibility with standard QAM systems. Overall, the results establish constellation warping as an effective physical layer security technique for wireless communication systems facing advanced spoofing threats, complementing traditional cryptographic approaches and introducing an additional security dimension that is challenging for adversaries to circumvent.

Data Availability Statement

Data will be made available on request.

Funding

This work was supported without any funding.

Conflicts of Interest

Amgad A. Salama is affiliated with the The Egyptian Technical Research and Development Centre, Cairo 11618, Egypt. The authors declare that this affiliation had no influence on the study design, data collection, analysis, interpretation, or the decision to publish, and that no other competing interests exist.

AI Use Statement

The authors declare that no generative AI was used in the preparation of this manuscript.

Ethical Approval and Consent to Participate

Not applicable.

References

[1] Bai, L., Zhu, L., Liu, J., Choi, J., & Zhang, W. (2020). Physical layer authentication in wireless communication networks: A survey. *Journal of Communications and Information Networks, 5*(3), 237-264. [CrossRef]

[2] Khan, S. Z., Mohsin, M., & Iqbal, W. (2021). On GPS spoofing of aerial platforms: a review of threats, challenges, methodologies, and future research directions. *PeerJ Computer Science, 7*, e507. [CrossRef]

[3] Shafique, A., Mehmood, A., & Elhadef, M. (2021). Detecting signal spoofing attack in uavs using machine learning models. *IEEE Access, 9*, 93803-93815. [CrossRef]

[4] Wang, X., Hao, P., & Hanzo, L. (2016). Physical-layer authentication for wireless security enhancement: Current challenges and future developments. *IEEE Communications Magazine, 54*(6), 152-158. [CrossRef]

[5] Illi, E., Qaraqe, M., Althunibat, S., Alhasanat, A., Alsafasfeh, M., De Ree, M., ... & Al-Kuwari, S. (2023). Physical layer security for authentication, confidentiality, and malicious node detection: A paradigm shift in securing IoT networks. *IEEE Communications Surveys & Tutorials, 26*(1), 347-388. [CrossRef]

[6] Zhang, J., Rajendran, S., Sun, Z., Woods, R., & Hanzo, L. (2019). Physical layer security for the Internet of Things: Authentication and key generation. *IEEE Wireless Communications, 26*(5), 92-98. [CrossRef]

[7] Mitev, M., Chorti, A., Belmega, E. V., & Poor, H. V. (2021). Protecting physical layer secret key generation from active attacks. *Entropy, 23*(8), 960. [CrossRef]

[8] Eberz, S., Strohmeier, M., Wilhelm, M., & Martinovic, I. (2012, September). A practical man-in-the-middle attack on signal-based key generation protocols. In *European symposium on research in computer security* (pp. 235-252). Berlin, Heidelberg: Springer Berlin Heidelberg. [CrossRef]

[9] Shawky, M. A., Shah, S. T., Abbasi, Q. H., Hussein, M., Imran, M. A., Hasan, S. F., Ansari, S., & Taha, A. (2023). RIS-enabled secret key generation for secured vehicular communication in the presence of denial-of-service attacks. *Sensors, 23*(8), 4104. [CrossRef]

[10] Zhang, P., Taleb, T., Jiang, X., & Wu, B. (2019). Physical layer authentication for massive MIMO systems with hardware impairments. *IEEE Transactions on Wireless Communications, 19*(3), 1563–1576. [CrossRef]

[11] Tahir, M., & Siddiqi, M. U. (2014). A Hybrid Scheme for Wireless Physical Layer Security Based on Encryption and Channel Pre-compensation. *IETE Journal of Research, 60*(4), 267-275. [CrossRef]

[12] Shawky, M. A., Shah, S. T., Abdrabou, M., Usman, M., Abbasi, Q. H., Flynn, D., Imran, M. A., Ansari, S., & Taha, A. (2024). How secure are our roads? An in-depth review of authentication in vehicular communications. *Vehicular Communications, 47*, 100784. [CrossRef]

[13] Xiang, Y., Natgunanathan, I., Rong, Y., & Guo, S. (2015). Spread spectrum-based high embedding capacity watermarking method for audio signals. *IEEE/ACM transactions on audio, speech, and language processing, 23*(12), 2228-2237. [CrossRef]

[14] Mekhfioui, M., El Bazi, N., Laayati, O., Satif, A., Bouchouirbat, M., Kissi, C., ... & Chebak, A. (2025). Optimized digital watermarking for robust information security in embedded systems. *Information, 16*(4), 322. [CrossRef]

[15] Chen, B., & Wornell, G. W. (1999, April). Dither modulation: a new approach to digital watermarking and information embedding. In *Security and Watermarking of Multimedia Contents* (Vol. 3657, pp. 342-353). SPIE. [CrossRef]

[16] Wu, Y., Khisti, A., Xiao, C., Caire, G., Wong, K. K., & Gao, X. (2018). A survey of physical layer security techniques for 5G wireless networks and challenges ahead. *IEEE Journal on selected areas in communications, 36*(4), 679-695. [CrossRef]

[17] Zhang, P., Shen, Y., Jiang, X., & Wu, B. (2020). Physical layer authentication jointly utilizing channel and phase noise in MIMO systems. *IEEE Transactions on Communications, 68*(4), 2446-2458. [CrossRef]

[18] Restuccia, F., D'Oro, S., Al-Shawabka, A., Belgiovine, M., Angioloni, L., Ioannidis, S., ... & Melodia, T. (2019, July). DeepRadioID: Real-time channel-resilient optimization of deep learning-based radio fingerprinting algorithms. In *Proceedings of the twentieth ACM international symposium on mobile ad hoc networking and computing* (pp. 51-60). [CrossRef]

[19] Hagras, E. A. A., Aldosary, S., Khaled, H., & Hassan, T. M. (2023). Physical layer authenticated image encryption for IoT network based on biometric chaotic signature for MPFrFT OFDM system. *Sensors, 23*(18), 7843. [CrossRef]

[20] Xu, D., & Ren, P. (2020). Concatenated graph coding on bandwidth part for secure pilot authentication in grant-free URLLC. *IEEE Open Journal of the Computer Society, 1*, 193–208. [CrossRef]

[21] Pham, T. V., & Ishihara, S. (2025). Practical Design of Probabilistic Constellation Shaping for Enhancing Performance of Physical Layer Security in Visible Light Communications. *IEEE Transactions on Communications*. [CrossRef]

Dr. Amgad Adel Salama received the B.Sc. and the M.Sc. degrees from Alexandria University, Alexandria, Egypt, in 2005 and 2012, respectively, and the Ph.D. degree from Concordia University, Montreal, QC, Canada, in 2017, all in electrical engineering. He is currently with the Egyptian Research and Development center, Cairo, Egypt. His research interests include sensor array signal processing, machine learning (deep learning), direction of arrival estimation, and beam forming. He was a reviewer for several journals and major conferences.

Ahmed Gamal Abdellatif Ibrahim is a dedicated lecturer in the Faculty of Computers and Information System, Egyptian Chinese University, Cairo, Egypt. In 2007, Dr Gamal graduated with a B.Sc. degree with honours in Electronics and Electrical Engineering from the Air Defense College. He continued his academic journey and obtained a master's degree in Electronics and Electrical Engineering from Alexandria University in 2017. Dr. Gamal has also demonstrated his commitment to expanding his knowledge and gaining international experience. In 2019, he became a PhD student visitor at the prestigious Research Center of Geomatics (CIRGEO) at the University of Padua, Italy. This valuable experience allowed him to broaden his horizons and enrich his research pursuits. Dr. Gamal successfully completed his PhD degree in Electronics and Communications Engineering in 2022. His research interests reflect his diverse background and multidisciplinary approach, including navigation, indoor positioning, tracking, filtering, information security, and image processing.

Soha Safwat Labib is currently a Professor and the Dean of the Faculty of Computers and Information Technology, at Egyptian Chinese University, Egypt. Her current research areas of interest include big data, machine learning, and deep learning.

Syed Tariq Shah is a highly accomplished academic and research professional with a background in Electrical and Electronic Engineering. He received his Master's and Ph.D. degrees from the Department of Electrical and Electronic Engineering at Sungkyunkwan University in Suwon, South Korea, in 2015 and 2018, respectively. Currently, he is working as a Postdoctoral Fellow at the University of Glasgow in the UK and also serving as an Associate Professor with the Department of Electrical Engineering, BUITEMS, Pakistan. His research interests include 5G and beyond networks, Open RAN, AI-enabled wireless networks, RF energy harvesting, and Intelligent reflecting surfaces. Dr Shah is also an Editor of the Electronics Journal and a reviewer of several IEEE Transactions, Letters, and Magazines.

Mahmoud A. Shawky was born in 1990 in Saudi Arabia. He received his B.Sc. degree in Electronics and Electrical Engineering in 2012 from Air Defence College, Alexandria University, M.Sc. (Eng.) degree in Authentication Mechanisms in Computer Network Protocols from Alexandria University, Alexandria, Egypt. He received his PhD degree from the James Watt School of Engineering, University of Glasgow, UK. His research interests are in the areas of cryptography and number theory, digital signatures, authentication in wireless communications and cyber security.