The State-of-the-Art in Data Compression and Data Security circa 2025

Soumadeep Ghosh

Kolkata, India

Abstract

This paper surveys the latest advances in data compression and data security as of 2025, highlighting key algorithms, standards, and the interplay between efficient storage and robust protection. We provide a glossary of essential terms and a conceptual diagram illustrating the integration of compression and encryption in modern data pipelines.

The paper ends with "The End"

1 Introduction

The exponential growth of data in the digital era has driven significant innovation in both data compression and data security. As of 2025, the convergence of artificial intelligence, quantum computing, and edge technologies has reshaped the landscape, demanding new approaches for efficient and secure data handling.

2 Recent Advances in Data Compression

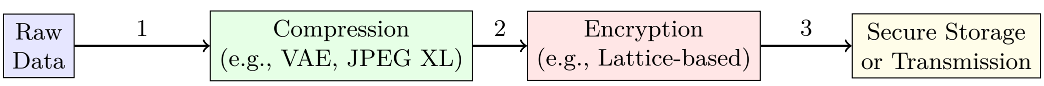
Modern data compression leverages deep learning, context modeling, and hardware acceleration. Neural compression algorithms, such as those based on variational autoencoders (VAEs) and transformers, now outperform traditional codecs for images, video, and text. Standards like JPEG XL and AV1 have become mainstream, offering high efficiency and broad compatibility.

3 Recent Advances in Data Security

Data security in 2025 is characterized by the adoption of post-quantum cryptography, zero-trust architectures, and privacy-preserving computation. Lattice-based cryptosystems and homomorphic encryption are increasingly deployed to counteract the threat posed by quantum computers. Secure enclaves and confidential computing platforms are standard in cloud and edge environments.

4 Integration: Compression and Encryption

A key trend is the seamless integration of compression and encryption. Joint schemes optimize both storage and confidentiality, reducing attack surfaces and improving performance in resource-constrained devices.


Raw Data
1
Compression (e.g., VAE, JPEG XL)
2
Encryption (e.g., Lattice-based)
3
Secure Storage or Transmission

Pipeline:
1. Compress data for efficiency
2. Encrypt compressed data for security
3. Store or transmit securely

Figure 1: Modern data pipeline integrating compression and encryption.

5 Conclusion

The state-of-the-art in 2025 reflects a holistic approach to data compression and security, with AI-driven algorithms and quantum-resistant cryptography at the forefront. The integration of these technologies is essential for safeguarding the data-driven world.

References

[1] Tantau, T. (2015). *The TikZ and PGF Packages.* Retrieved from `https://ctan.org/pkg/pgf`

[2] ISO/IEC. (2022). *JPEG XL Image Coding System.*

[3] Chen, L., et al. (2023). *Report on Post-Quantum Cryptography.* NIST.

[4] Mentzer, F., et al. (2024). *Neural Image Compression: A Review.* IEEE Transactions on Pattern Analysis and Machine Intelligence.

[5] Gentry, C. (2009). *Fully Homomorphic Encryption Using Ideal Lattices.* STOC.

6 Glossary

Compression
The process of reducing the size of data for storage or transmission.

Encryption
The transformation of data into a secure format to prevent unauthorized access.

Neural Compression
Data compression using neural networks, often achieving higher efficiency than traditional algorithms.

Post-Quantum Cryptography
Cryptographic methods designed to be secure against quantum computer attacks.

Homomorphic Encryption
Encryption that allows computation on ciphertexts, producing encrypted results that, when decrypted, match the result of operations performed on the plaintext.

Zero-Trust Architecture
A security model that assumes no implicit trust and verifies every access attempt.

Lattice-based Cryptography
A family of cryptographic algorithms believed to be resistant to quantum attacks.

Confidential Computing
Technologies that protect data in use by performing computation in a hardware-based trusted execution environment.

The End