ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Volume 13, Issue 4, April 2026

A Multilayered Cryptographic Framework using 24-Hour Angular Displacement and Base-10 Inversion

[1] S. Ravichandran

[1] Independent Researcher, Economics, Law, Computer Applications, and Linguistics
Corresponding Author Email: [1] saktheee2009@gmail.com

Abstract*— Modern encryption systems rely heavily on binary computation and mathematical factorization. While powerful, these systems may face vulnerabilities from quantum computing and advanced pattern recognition. This paper proposes Maraikilavi 360, a multilayered cryptographic framework that transforms numeric data into geometric-temporal and chromatic representations. The method integrates a 24-hour angular displacement model, Base-10 inversion masking, and visual chromatic encoding to produce a dynamic, image-based encrypted payload. The approach introduces moving-target entropy and visual steganography, allowing encrypted data to appear as simple graphical patterns rather than conventional code. The system also preserves a human-centric fallback mechanism enabling manual decoding using a 24-hour circular clock reference.

I. INTRODUCTION

Contemporary digital security systems such as RSA and AES depend primarily on number theory and binary representation. Although effective, these approaches remain susceptible to emerging quantum computational techniques and sophisticated pattern-analysis attacks. Additionally, deep packet inspection systems can identify recognizable encryption structures.

Maraikilavi 360 introduces an alternative paradigm: transforming data into geometric orientation and chromatic visual structures rather than textual or binary forms. The concept draws inspiration from ancient linguistic concealment principles known as “Maraikilavi,” meaning hidden speech or concealed meaning.

II. PROBLEM STATEMENT

Traditional encryption techniques expose identifiable digital signatures. These may be targeted by frequency analysis, algorithmic cryptanalysis, or machine-learning pattern recognition systems.

The core challenge addressed in this research is the design of a cryptographic framework in which the encrypted payload does not appear as code at all, but rather as an ordinary image composed of colored geometric elements.

III. RESEARCH OBJECTIVES

- Integrate classical linguistic concealment principles with modern computational geometry.
- Develop a Base-10 inversion masking system to eliminate predictable numerical patterns.
- Implement a time-dependent moving target defense using a 24-hour circular angular key.
- Convert encrypted data into a chromatic geometric payload suitable for image-based transmission.

IV. PROPOSED METHODOLOGY

The Maraikilavi 360 architecture consists of three primary phases:

Phase A: 24-Hour Angular Base

The circular geometry of 360 degrees is mapped to a 24-hour clock framework.

Hour constant = 360 / 24 = 15 degrees per hour.

Minute constant = 3 degrees per minute (customized scale for security variation).

Phase B: Numerical Masking (Base-10 Inversion)

Each digit D in the original data is masked by the transformation:

M = 10 – D

This inversion removes direct numeric patterns and produces balanced symbolic weight.

Phase C: Chromatic Representation

Masked data is transformed into colored geometric dots representing magnitude layers:

Maroon – Lakhs (10^5)

Purple – Thousands (10^3)

Blue – Units (10^0)

These dots are rotated to the angular position determined by the temporal key.

V. PROOF OF CONCEPT

Example encryption scenario:

Target Data: 5,00,000

Time of Transmission: 15:10 (3:10 PM)

Temporal Key: ku

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Volume 13, Issue 4, April 2026

Angle_hour = 15 × 15 = 225°
Angle_minute = 10 × 3 = 30°
Total Angular Orientation = 225° + 30° = 255°
Numerical Mask:
Original digit = 5
Masked value = 10 − 5 = 5
Visual Output:
Five maroon dots positioned along a radial vector rotated to approximately 255° forming a chromatic payload image.

VI. TECHNICAL INNOVATION AND SECURITY ANALYSIS

Dynamic Entropy:

Because the encryption orientation changes every minute, identical data transmitted at different times generates completely different geometric signatures.

Visual Steganography:

The encrypted payload is embedded in an image format such as PNG or JPG, allowing it to bypass conventional network scanning systems.

Human-Centric Resilience:

In emergency situations the encoded information can be manually interpreted using the 24-hour circular clock geometry without digital assistance.

Persistent Hidden Partition'."

"I propose that these hidden envelopes should be integrated as a Default System Feature. Even if the OS is reinstalled or the phone is sent for repair, the encrypted data remains Indestructible and Intact in a non-volatile memory sector."

"To a hacker or a technician, the phone looks like a fresh, empty device. But for the user, their secret data is safe behind the Invisible Layer, waiting to be triggered. This makes security not just an 'App', but a permanent part of the Mobile Architecture."

VII. FUTURE SCOPE

- Development of a mobile application capable of camera-based decoding of chromatic dot sequences.
- Integration with blockchain technologies for time-dependent private key generation.
- Application in secure diplomatic communication and low-bandwidth covert signaling systems.
- Expansion toward AI-assisted pattern generation and automated cryptographic visualization.

VIII. CONCLUSION

Maraikilavi 360 presents a conceptual shift from traditional alphanumeric encryption toward geometric-temporal cryptography. By combining time-based angular displacement, numerical inversion masking, and chromatic visualization, the system produces encrypted data that appears visually innocuous while maintaining structural complexity.

This fusion of cultural linguistic logic and modern cybersecurity principles may provide an alternative pathway for resilient secure communication architectures.

REFERENCE

[1] Ravichandran, S. (2026). Alphanumeric Cryptographic Framework. JETNR, Vol. 4, Issue 2, Paper ID: JETNR2602042.