Calligraphy Encryption: A Mathematical Framework for True Random Generation Based on Complex Domain Analysis of Handwriting Images

Lanhaijian

Hongqiao University Science and Technology Academic Network, hongqiao.tech

Abstract

This paper proposes a true random generation mathematical model—Calligraphy Encryption—that uses human handwritten calligraphy images as the physical entropy source. The model extracts the global frequency and phase structure of handwriting images through two-dimensional complex Fourier transform, captures multi-scale local geometric and topological features using complex-valued wavelet transform, and constructs a unified complex-valued F-field to achieve fusion and dimension-up representation of the above features. Topological invariants and statistical invariants are extracted from the complex-valued F-field, and a high-entropy true random sequence is obtained through cryptographic hash function mapping. The paper rigorously proves the existence, uniqueness, unpredictability and verifiability of the framework, and gives the lower bound estimation of randomness. Theoretical analysis shows that the system does not rely on algorithmic pseudo-randomness; its randomness originates from the physical non-replicability of real writing behavior, with mathematical self-consistency and cryptographic security, providing a brand-new physical entropy source and generation paradigm for cryptography encryption.

Keywords: Calligraphy Encryption; Complex Fourier Transform; Complex Wavelet Transform; True Random Number Generation; F-field; Topological Invariants; Cryptographic Hash

1 INTRODUCTION

Calligraphy, as a typical form of traditional Oriental art, integrates human subjective will, motor nerve control and physical environment disturbances during creation. Each real writing has natural uniqueness in microstructure, providing an ideal physical entropy source for true random number generation, which is also the core foundation of cryptography encryption.

Current random number generation methods are mainly divided into two categories: pseudo-random number generation and physical random number generation. Pseudo-random numbers are generated by deterministic algorithms and are essentially predictable, making it difficult to meet high-level encryption security requirements. Physical random numbers mostly rely on quantum noise, thermal noise or circuit noise. Although they have true randomness, they lack humanistic interpretability, traceability and scenario adaptability. The mathematical framework of calligraphy encryption proposed in this paper deeply combines human writing behavior, complex domain signal analysis and topological invariants for the first time, constructs a strict mathematical path from artistic creation features to cryptographically secure random sequences, and fills the theoretical gap of humanistic physical entropy source application in the encryption field.

The structure of this paper is as follows: Chapter 2 gives basic space and symbol definitions; Chapter 3 constructs global features in the complex Fourier domain; Chapter 4 constructs multi-scale features in the complex wavelet domain; Chapter 5 proposes the definition and construction of the complex-valued F-field; Chapter 6 gives the generation mapping of true random sequences for encryption; Chapter 7 provides complete theoretical proof and analysis; Chapter 8 is the efficiency optimization and anti-quantum security verification of the calligraphy chain identity authentication system; finally, the conclusion, references and acknowledgments are given.

2 BASIC SPACES AND SYMBOL DEFINITIONS

Let Ω be a bounded closed rectangular region on a two-dimensional plane, representing the domain of the calligraphy image.

The handwriting image is represented as a function defined on Ω:

$$f(x, y) : \Omega \to [0, 1]$$

f belongs to the square-integrable function space $L^2(\Omega)$ and satisfies the Hölder continuity condition.

Core symbols used in this encryption framework:

1. $\mathcal{F}$: two-dimensional complex Fourier transform operator
2. $\mathcal{W}$: two-dimensional complex-valued wavelet transform operator
3. $F(x, y)$: complex-valued F-field
4. $A(u, v)$: amplitude component of Fourier transform
5. $\varphi(u, v)$: phase component of Fourier transform
6. $\mathcal{H}$: cryptographic hash operator (SHA3-512)
7. S_f: encryption true random sequence generated from handwriting image f

3 CONSTRUCTION OF ENCRYPTION FEATURES IN COMPLEX FOURIER DOMAIN

Perform two-dimensional complex Fourier transform on the normalized calligraphy image f:

$$\mathcal{F}f(u, v) = A(u, v) \cdot e^{i\varphi(u,v)}$$

It can be decomposed into amplitude and phase. The amplitude corresponds to the global structural information of the image, while the phase is highly sensitive to tiny perturbations and is the core carrier of the encryption entropy source. This paper only uses the high-frequency phase region as the global encryption entropy source, because high-frequency components best reflect the microscopic unique differences in writing and provide a high-entropy basis for the encryption random sequence.

3.1 Definition 3.1 Global Encryption Phase Feature Set

$$\mathcal{F}f(u, v) = A(u, v) \cdot e^{i\varphi(u,v)}$$

3.2 Proposition 3.1

For images $f_1 \neq f_2$ generated by any two real writings, their global encryption phase features are almost surely different, meeting the uniqueness requirement of encryption entropy sources.

4 CONSTRUCTION OF ENCRYPTION FEATURES IN COMPLEX WAVELET DOMAIN

Let ψ be a two-dimensional complex-valued mother wavelet satisfying the admissibility condition. Perform multi-scale complex wavelet transform on f:

$$\mathcal{W}f(s, x, y) = \langle f, \psi_{s,x,y} \rangle$$

This transform can extract local details such as stroke contours, stroke tips, flying white, turning points, and ink color changes at different scales. The phase of complex wavelet coefficients has unique recognition ability for the natural singularity of human writing and is the core source of local high-entropy encryption features.

4.1 Definition 4.1 Multi-scale Encryption Phase Feature Set

$$\Psi_f = \{\arg(\mathcal{W}f(s, x, y)) \mid s \in \mathbb{R}_+, (x, y) \in \Omega\}$$

4.2 Proposition 4.1

The phase features of real human writing are essentially different from those of AI-generated images. Ψ_f of any two real writings is almost surely different, which can effectively avoid the risk of forgery of encryption entropy sources.

5 DEFINITION AND ENCRYPTION FEATURE CONSTRUCTION OF COMPLEX-VALUED F-FIELD

The complex-valued F-field is the core mathematical structure that fuses global complex Fourier information and local complex wavelet information, providing a carrier for unified extraction and dimension-up of encryption features. Its invariants are the core basis for generating encryption random sequences.

5.1 Definition 5.1 Complex-Valued F-Field

$$F(x, y) = F_R(x, y) + i \cdot F_I(x, y)$$

Where:

- Real part F_R: fused by Fourier amplitude and local energy to ensure the stability of encryption features
- Imaginary part F_I: fused by global phase and multi-scale wavelet phase to ensure the uniqueness and high entropy of encryption features

The F-field upgrades the handwriting image from two-dimensional space to a complex-valued field, endowing it with richer topological and geometric invariants to meet the dual requirements of stability and uniqueness for encryption features.

5.2 Definition 5.2 Encryption F-Field Invariant Set

Extract the following stable invariant features from the F-field as the core feature source of the encryption random sequence, denoted as the invariant set $\mathcal{I}(F)$:

1. Statistical moments of phase (mean, variance, skewness, kurtosis)
2. Density and distribution of amplitude zeros (singular points)
3. Curl and winding number of the phase field
4. Topological features of connected domains (number, boundary length, fractal dimension)

6 MATHEMATICAL CONSTRUCTION OF TRUE RANDOM SEQUENCES FOR ENCRYPTION

Encode the F-field encryption invariants into a fixed-length sequence, and then map it through a cryptographic hash to obtain the final true random sequence for encryption. The whole process follows cryptographic security specifications to ensure the unpredictability and collision resistance of the sequence.

6.1 Definition 6.1 True Random Sequence Mapping for Encryption

$$S_f = \mathcal{H}\left(\text{Encode}\left(\mathcal{I}(F)\right)\right)$$

Where:

1. Encode: binary encoding of invariants to ensure standardized conversion of features
2. $\mathcal{H}$: SHA3-512 cryptographic hash function meeting the security requirements of encryption hash algorithms
3. S_f: 512-bit binary encryption true random sequence, which can be directly used as core carriers such as encryption keys and seeds

6.2 Proposition 6.1 Uniqueness

If $f_1 \neq f_2$, then $S_{f_1} \neq S_{f_2}$ holds almost surely, ensuring the uniqueness of encryption keys.

6.3 Proposition 6.2 Unpredictability

S_f cannot be predicted in advance by any deterministic algorithm or model, has cryptographic security strength, and meets the core security requirements of encryption for random sequences.

7 THEORETICAL ANALYSIS: EXISTENCE, UNIQUENESS, STABILITY AND ENTROPY LOWER BOUND

7.1 7.1 Basic Physical Assumptions of the Encryption Framework

Real writing can be expressed as:

$$f = f^* + \xi$$

Where f^* is the ideal template, and ξ is physical noise (hand tremor, ink halo, paper texture, writing fluctuation). $\xi \neq 0$ and has infinite-dimensional information entropy, which is the fundamental source of true randomness of the calligraphy encryption framework and provides an irreproducible physical entropy basis for encryption.

7.2 7.2 Core Theorems and Proofs

7.2.1 Theorem 7.1 Chaotic Sensitivity of Complex Fourier Phase

Let $f_1 = f + \xi_1$, $f_2 = f + \xi_2$, $\xi_1 \neq \xi_2$. Then in the high-frequency region, $\varphi_{f_1}(u, v) \neq \varphi_{f_2}(u, v)$ holds almost surely.

The complex Fourier phase has exponentially sensitive characteristics to the input signal, and any tiny perturbation will be amplified by high-frequency components. Since ξ_1 and ξ_2 are not equal, their phase differences cannot be eliminated in the frequency domain, so the global phases of the two writings are necessarily distinguishable, ensuring the unique identification of the encryption entropy source.

7.2.2 Theorem 7.2 Unique Separability of Complex Wavelet Features

For any two real writings $f_1 \neq f_2$, their multi-scale complex wavelet phase sets satisfy:

$$P(\Psi_{f_1} = \Psi_{f_2}) = 0$$

Human writing has natural singularities manifested in multi-scale structures such as stroke tips, flying white, and ink color changes. AI-generated images are smooth interpolation results without such singularity spectra. Therefore, the wavelet phase sets of different writings are completely separable in the probabilistic sense, which can effectively avoid artificial forgery of encryption entropy sources and ensure the anti-forgery of the encryption framework.

7.2.3 Theorem 7.3 Uniqueness of F-Field Invariants

If $f_1 \neq f_2$, then their corresponding F-field invariants satisfy: $\mathcal{I}(F_{f_1}) \neq \mathcal{I}(F_{f_2})$ holds almost surely.

The F-field fuses both the global complex Fourier phase and the local complex wavelet phase, and the aforementioned theorems have proved that both can uniquely distinguish writings. Therefore, the F-field invariants constitute a complete feature that can uniquely determine the original handwriting image, providing a unique feature basis for the encryption random sequence.

7.2.4 Theorem 7.4 Existence of Encryption True Random Sequences

For any real writing f, the encryption random sequence S_f exists and is uniquely determined.

The F-field is uniquely constructed by f, the encryption invariants $\mathcal{I}(F)$ are computable, and the hash function is a deterministic mapping. Therefore, S_f can be uniquely generated with mathematical existence and uniqueness, ensuring the effectiveness of the calligraphy encryption framework.

7.2.5 Theorem 7.5 Lower Bound of Min-Entropy

The random sequence S_f generated by the calligraphy encryption framework satisfies the lower bound of min-entropy:

$$H_\infty(S_f) \geq 512 - o(1)$$

The physical noise ξ is a continuum random source with infinite-dimensional entropy. The F-field invariants extract stable high-entropy components of ξ, and SHA3-512 maintains the output entropy close to the output length under high-entropy input. Therefore, the min-entropy of S_f approaches 512 bits, reaching the security level of cryptographic encryption and meeting the core requirements of high-level encryption for random sequence entropy values.

7.2.6 Theorem 7.6 Global Verifiability

Any third party can reproduce S_f using the public operators $\mathcal{F}$, $\mathcal{W}$, F, $\mathcal{I}$, $\mathcal{H}$ to complete independent verification.

The entire encryption process has no random parameters, no training weights, no hidden variables, and all transformations are deterministic mathematical mappings. Therefore, the system has decentralized verifiability, ensuring public verification and credibility of encryption keys.

7.2.7 Theorem 7.7 Robust Stability

Let $\tilde{f} = f + \zeta$, where ζ is tiny noise and $\|\zeta\| \leq \delta$. Then the hash distance between S_f and $S_{\tilde{f}}$ decays exponentially with δ.

F-field invariants are robust to noise and only sensitive to structural differences of the writing itself. Therefore, the system can still output consistent results stably under scanning, lighting, and slight pollution, ensuring the stability and practicality of the calligraphy encryption framework in actual engineering applications.

8 CALLIGRAPHY CHAIN AUTHENTICATION SYSTEM AND ANTI-QUANTUM SECURITY

8.1 8.1 Limitations of Traditional Authentication

In the context of advancing quantum computing, traditional digital identity authentication systems face dual crises: quantum collapse risk of mathematical ciphers, static leakage risks of biometrics, and efficiency bottlenecks of full matching schemes.

8.2 8.2 Three-level Dynamic Verification Architecture

Ultra-light Verification (ms): single stroke, edge computing, response $<$ 100ms.
Standard Verification (sub-second): single character, hash matching, response $<$ 1s.
High-level Verification (s): full writing, blockchain storage, response 3–5s.

8.3 8.3 Anti-quantum Security

Calligraphy encryption has unstructured high-dimensional dynamic features, one-time living behavior, endogenous non-landing keys, and super-exponential feature space, which are resistant to quantum attacks represented by Shor's algorithm.

9 CONCLUSION AND PROSPECT

This paper establishes a true random generation mathematical model—Calligraphy Encryption—with human writing as the physical entropy source. The framework transforms the natural uniqueness of artistic creation into cryptographically secure true random sequences, realizing the deep integration of humanistic artistic features and cryptographic encryption. It can provide theoretical support for cultural right confirmation, digital identity encryption and high-security cryptosystem construction.

References

[1] Bracewell, R.N. *The Fourier Transform And Its Applications*. McGraw-Hill, 2000.

[2] Mallat, S. *A Wavelet Tour of Signal Processing*. Academic Press, 1999.

[3] Daubechies, I. *Ten Lectures on Wavelets*. SIAM, 1992.

[4] NIST. FIPS PUB 202: SHA-3 Standard. 2015.

[5] Cover, T.M., Thomas, J.A. *Elements of Information Theory*. Wiley, 2006.

[6] Rudin, W. *Real and Complex Analysis*. McGraw-Hill, 1987.

ACKNOWLEDGMENTS

Thanks to the academic platforms and scholars who supported this research. Thanks to all peers, friends and family for their help and inspiration.