Unpredictability as the Optimal Measure of Entropy

Linking Complexity to Entropy

The Infinite Complexity of the Mandelbrot Fractal and How JFES Extracts Entropy from the Mandelbrot Fractal

Wolfgang Flatow
JavaScript Fractal Encryption Standard / JFES
wolfgang.flatow@portalz.solutions

Contents

1 Introduction **4**

2 Complexity and Unpredictability **4**

3 Natural Entropy Sources **5**

4 Shannon's Definition of Entropy **6**

5 Recursive Sampling Changes the Problem **7**

6 The Mandelbrot Fractal **8**

7 Infinite Complexity **8**

8 JFES Does Not Scan the Mandelbrot Set **9**

9 The Significance of the Intermediate Values **9**

10 Finite Precision Does Not Define the Field **10**

11 Determinism and Entropy **10**

12 From Complexity to Unpredictability **11**

13 Equiprobability Is Not the Whole Story **11**

14 The Mozart Test **11**

15 JFES as Entropy Extraction **12**

16 JFES Mathematics **13**

16.1 Complexity of the Mandelbrot Field 14

16.2 Trajectory Complexity 14

16.3 Unpredictability 15

16.4 Finite Precision and the Mathematical Field 16

16.5 The Entropy Extraction Principle 16

17 The Research Proposition **17**

18 Conclusion **17**

Abstract

Entropy is conventionally quantified through probability distributions. In information theory, Shannon entropy measures the average uncertainty associated with a random variable. In cryptographic engineering, however, the property of greatest practical significance is **unpredictability**: the inability of an observer to determine the next relevant value from the information available to them.

This paper proposes **unpredictability as the optimal operational measure of entropy quality** and examines the relationship between complexity and access to unpredictable outcomes.

The central proposition is:

> **The best measure of entropy quality is unpredictability. In order to access unpredictability, complexity is required. The best possible complexity is infinite complexity.**

Natural entropy sources—including thermal noise, radioactive decay and turbulence—demonstrate the relationship between physical complexity and unpredictability. JFES approaches the problem differently. Rather than sampling a physical noise source, JFES uses the mathematical structure of the Mandelbrot fractal as its transformation domain.

The Mandelbrot set is not merely an aesthetically complex object. Shishikura established that the boundary of the Mandelbrot set has **Hausdorff dimension 2**, the maximum possible Hausdorff dimension for a subset of the complex plane. JFES exploits this mathematical domain through recursive navigation: a selected x, y coordinate is evaluated through Mandelbrot iteration; values generated during that iteration determine subsequent x, y locations; those locations are again evaluated within the Mandelbrot field.

Thus JFES does not linearly scan a fractal image or use a conventional random-number generator. It **navigates the Mandelbrot field recursively**, using the field's own values to determine the subsequent locations from which further values are obtained.

At present, JFES operates at finite computational precision, with the free implementation supporting up to 1024-bit coordinate precision. This is an engineering boundary rather than a boundary of the underlying mathematical field.

The paper develops this proposition and identifies the mathematical framework required to formally quantify the resulting unpredictability and entropy characteristics.

1 Introduction

Entropy is one of the foundational concepts of information theory and cryptography.

Yet the word *entropy* is used in several different contexts.

In thermodynamics it describes disorder or multiplicity of microscopic states. In information theory it quantifies uncertainty associated with a probability distribution. In cryptography it is associated with the unpredictability of secrets, keys and random values.

These perspectives share a common feature:

The observer cannot determine the outcome in advance.

This paper takes that property as the central engineering characteristic.

We therefore propose:

$$\boxed{\text{Entropy Quality} = \text{Unpredictability}}$$

This differs from Shannon's mathematical definition of entropy (below). Rather, it identifies the property that makes entropy valuable for cryptographic purposes.

The next question is immediate:

What enables unpredictability?

The answer proposed here is **complexity**.

2 Complexity and Unpredictability

Consider a process whose output is generated by a simple deterministic rule:

$$x_{n+1} = f(x_n)$$

If f is sufficiently simple and its state is known, its future behaviour can be predicted.

Now consider a process whose state evolution depends upon an enormously complex domain.

The observer must not only know the current state but must understand the transformation governing the transition through that domain.

Consequently:

$$\text{Complexity} \rightarrow \text{Difficulty of prediction} \rightarrow \text{Unpredictability}$$

This provides the conceptual link between complexity and entropy quality.

The stronger the accessible complexity, the larger the space of possible trajectories and the more difficult it becomes to predict the trajectory.

This leads to the second proposition:

$$\boxed{\text{Access to unpredictability requires complexity}}$$

The limiting case is then:

$$\boxed{\text{Maximum complexity} = \text{infinite complexity}}$$

The significance of infinite complexity here is mathematical rather than computational. No finite implementation can calculate an infinite object in its entirety. The relevant question is whether a finite implementation can **access progressively deeper portions of an unbounded mathematical structure**.

That is precisely the architecture explored by JFES.

3 Natural Entropy Sources

Nature provides numerous examples of processes whose detailed future behaviour is unpredictable.

Examples include:

- radioactive decay;
- thermal noise;
- atmospheric noise;
- turbulence;
- ocean surf;
- quantum phenomena.

These systems contain enormous numbers of interacting variables.

A listener can recognise the output of a surf recording as surf. A detector can recognise radioactive clicks as radioactive decay. The broad class of the phenomenon is known.

Yet this does not allow the precise future microscopic output to be predicted.

The important observation is therefore:

> **A source can be recognisable while its detailed future state remains unpredictable.**

This distinguishes *classification* from *prediction*.

A bounded physical system can therefore provide excellent entropy without its output being mathematically structureless.

4 Shannon's Definition of Entropy

Shannon's entropy is defined mathematically as:

$$H(X) = -\sum_{x} P(x) \log_2 P(x)$$

For n bits, there are 2^n possible sequences. Under a uniform distribution, every sequence is assigned the same probability:

$$P(x) = \frac{1}{2^n}$$

and therefore:

$$H(X) = n$$

bits.

The important observation for this paper is that **the uniform distribution contains every possible sequence**, including an enormous number of highly predictable regular sequences.

For example, among the possible n-bit sequences are:

$$000000000000\ldots$$

$$111111111111\ldots$$

$$010101010101\ldots$$

$$101010101010\ldots$$

and repeating patterns of every width:

$$001100110011\ldots$$

$$000111000111\ldots$$

as well as arbitrary combinations and more complex structures.

Every one of these is a member of the same 2^n-element possibility space.

Consequently, **a uniform probability distribution describes maximum Shannon entropy without itself expressing the predictability of the individual sequences contained within that distribution.**

This creates an important distinction for the present work:

Maximum Shannon entropy $\neq$ maximum unpredictability of every sequence

A sequence can possess a highly regular structure and therefore be readily predictable once that structure is recognised, while still being one of the possible outcomes represented by the Shannon distribution.

The Shannon calculation answers:

> **How much uncertainty is represented by the probability distribution?**

The question introduced earlier in this paper is different:

> **How unpredictable is the actual outcome to an observer?**

That distinction provides the transition from Shannon's mathematical definition of entropy to the paper's proposed concept of **entropy quality**.

5 Recursive Sampling Changes the Problem

Consider sampling ocean surf.

A conventional sampler might produce:

$$S(t_1), S(t_2), S(t_3), \ldots$$

A more interesting sampler could use the value at one time to determine when to sample again:

$$S(t_1) \to t_2 \to S(t_2) \to t_3 \to S(t_3) \to \cdots$$

This creates a feedback relationship between the sampled value and the subsequent sampling location.

However, the underlying phenomenon remains **surf**.

The output remains constrained by the physical characteristics of the source.

JFES introduces a fundamentally different domain.

It does not recursively sample a physical noise signal.

It recursively navigates a complex Mandelbrot field.

6 The Mandelbrot Fractal

The Mandelbrot set is defined through the iteration

$$z_{n+1} = z_n^2 + c$$

where

$$c = x + iy.$$

The coordinate c is therefore a point in the complex plane.

For a given coordinate, the iteration produces a sequence of complex states:

$$z_0, z_1, z_2, \ldots, z_n.$$

The result is consequently not merely a binary value such as *inside* or *outside*.

A point provides access to an entire iterative trajectory.

This distinction is fundamental to JFES.

7 Infinite Complexity

The mathematical complexity of the Mandelbrot set is not simply an assertion that "fractals are complicated."

A rigorous result exists.

Mitsuhiro Shishikura proved:

$$\boxed{\dim_H(\partial M) = 2}$$

where M is the Mandelbrot set and ∂M is its boundary.

Essentially, the Mandelbrot set is infinitely complex.

Because the Mandelbrot set exists in the complex plane, 2 is the maximum possible Hausdorff dimension of a subset of that plane.

The result establishes that the Mandelbrot boundary possesses maximal Hausdorff dimension.

Importantly, the field is not exhausted by a finite-resolution image.

Increasing computational precision allows increasingly precise coordinates to be represented and evaluated.

JFES therefore operates on a finite representation of a mathematical object whose structure is not bounded by that representation.

8 JFES Does Not Scan the Mandelbrot Set

This distinction is central.

JFES does not perform:

$$(x_1, y_1), (x_2, y_2), (x_3, y_3), \ldots$$

as a predetermined linear scan.

Instead, the Mandelbrot field determines the navigation.

The process is conceptually:

$$(x_1, y_1) \to V_1 \to (x_2, y_2) \to V_2 \to (x_3, y_3) \to V_3 \to \cdots$$

where V_n is derived from the Mandelbrot evaluation at the current location.

The next location is therefore dependent upon the value obtained from the previous location.

Consequently:

$$(x_{n+1}, y_{n+1}) = G(V_n)$$

and

$$V_{n+1} = M(x_{n+1}, y_{n+1}).$$

This creates recursive navigation through the Mandelbrot field.

9 The Significance of the Intermediate Values

A coordinate does not simply produce one isolated value.

The Mandelbrot iteration itself generates:

$$z_0, z_1, z_2, \ldots, z_n.$$

Each z_n is a complex value.

Thus a single location in the Mandelbrot plane provides an iterative sequence of states, each produced from the preceding state.

JFES can exploit these values as transformation material.

The resulting architecture is therefore not:

$$\text{coordinate} \to \text{random number}$$

but:

$$\text{coordinate} \to \text{complex trajectory} \to \text{new coordinate} \to \text{new complex trajectory} \to \cdots$$

This recursive relationship is the mechanism through which JFES accesses the complexity of the Mandelbrot field.

10 Finite Precision Does Not Define the Field

JFES must operate on finite computational representations.

The current free implementation supports coordinate precision up to **1024 bits**.

This does not mean that the Mandelbrot field has 1024-bit complexity.

It means:

$$\text{JFES computational precision} \leq 1024 \text{ bits}$$

while the underlying mathematical object remains unbounded in precision.

The distinction is analogous to observing a physical phenomenon with an instrument of finite resolution.

The instrument has a limit.

The phenomenon does not acquire that limit merely because the instrument does.

11 Determinism and Entropy

A conventional objection to deterministic entropy generation is straightforward:

> A deterministic function cannot create entropy from nothing.

JFES accepts the principle.

JFES does not rely upon a conventional `RND()` operation.

It does not claim that an ordinary deterministic function magically converts a short seed into an equivalent quantity of entropy.

Its architecture is different.

The deterministic process is operating **inside the Mandelbrot field**, and the field's values recursively determine subsequent positions within that field.

The proposition under investigation is therefore not:

$$\text{short seed} \rightarrow \text{deterministic expansion} \rightarrow \text{entropy}$$

but:

$$\text{Mandelbrot field} \rightarrow \text{recursive navigation} \rightarrow \text{complex trajectory} \rightarrow \text{transformation output}.$$

The distinction is fundamental.

12 From Complexity to Unpredictability

The central JFES hypothesis can now be stated more precisely.

A deterministic trajectory is predictable when an observer possesses a sufficiently effective description of its future evolution.

JFES places the trajectory inside a mathematical domain with extremely rich structure and recursively uses the domain's output to determine subsequent locations.

Therefore the relevant cryptographic property is not simply the statistical appearance of the resulting bytes.

It is:

Can an observer predict the future trajectory from the information available to them?

This gives us the proposed hierarchy:

Complexity → Trajectory complexity → Unpredictability → Entropy quality

13 Equiprobability Is Not the Whole Story

A sequence can contain approximately equal numbers of zeroes and ones while remaining predictable.

For example:

$$0101010101010101\ldots$$

has equal proportions of zero and one.

Yet its next value is immediately predictable.

Therefore:

$$\text{equiprobability} \neq \text{unpredictability}.$$

Equiprobability is valuable because it contributes to high Shannon entropy.

But for cryptographic purposes, **unpredictability is the operational property of greatest interest**.

The deeper question is whether the output contains a structure that permits an attacker to predict future values.

JFES therefore places the emphasis on the trajectory that generates the output, rather than solely on the statistical distribution of the final bytes.

14 The Mozart Test

A useful conceptual experiment illustrates the distinction.

Imagine sampling an unpredictable physical process such as ocean surf.

Now suppose the recursive sampling mechanism suddenly produces a perfect high-fidelity orchestral performance of Mozart.

The remarkable property is not that Mozart is "random."

Mozart is highly structured.

The remarkable property is that the particular structured outcome was **not predictable before it occurred**.

This demonstrates an important principle:

Unpredictability does not require noise.

An unpredictable outcome can possess extraordinary structure.

This is relevant to JFES because the desired output need not resemble conventional physical noise in its generative mechanism.

What matters is whether the trajectory leading to the output can be predicted.

15 JFES as Entropy Extraction

JFES therefore proposes a different approach to entropy generation.

It does not introduce a conventional random-number generator.

Instead, it accesses the Mandelbrot field through recursive navigation.

The mechanism can be summarised as:

$$\boxed{(x, y) \rightarrow \text{Mandelbrot iteration} \rightarrow \text{complex values} \rightarrow \text{new } (x, y)}$$

repeated continuously.

The resulting trajectory constitutes the transformation source from which JFES derives its output stream.

Importantly, the JFES algorithm itself cannot predict what the next (x, y) coordinate or the resulting complex value will be at any iterative stage. It must execute the Mandelbrot calculation at the current location in order to discover the resulting value, which then determines the location of the next iteration.

Thus, although the process is deterministic, the future trajectory is not available to the algorithm without performing the transformation that produces it.

The distinction is fundamental:

$$\boxed{\text{Deterministic} \neq \text{Predictable without processing}}$$

JFES does not contain a separate prediction mechanism that can short-circuit the Mandelbrot navigation. The next state is obtained by processing the current state through the field itself.

The term *entropy extraction* is therefore used to describe the process of accessing unpredictable transformation material from the Mandelbrot field through recursive navigation.

16 JFES Mathematics

The mathematical foundation of JFES is the recursive navigation of the Mandelbrot field. JFES does not perform a linear scan of the Mandelbrot set. Instead, the complex value obtained at one location determines the subsequent location, creating a dynamically generated trajectory through the field.

Let the current location be represented by the complex number

$$c_n = x_n + iy_n.$$

At that location, the Mandelbrot iteration is evaluated according to

$$z_{k+1} = z_k^2 + c_n, \qquad z_0 = 0.$$

The resulting sequence

$$z_1, z_2, \ldots, z_m$$

contains complex values generated by the Mandelbrot function at c_n. JFES uses these values as transformation material from which the next location in the field is determined.

Thus, the JFES navigation can be represented generally as

$$c_{n+1} = G(z_1, z_2, \ldots, z_m),$$

where G represents the JFES coordinate-transformation operation.

The complete transformation is therefore

$$c_n \xrightarrow{M} (z_1, z_2, \ldots, z_m) \xrightarrow{G} c_{n+1}.$$

Defining

$$T = G \circ M,$$

the JFES trajectory becomes

$$\boxed{c_{n+1} = T(c_n)}$$

and consequently

$$c_1 \to c_2 \to c_3 \to \cdots \to c_n.$$

Each c_n is itself another point in the Mandelbrot field. The process therefore does not merely sample the field; it recursively navigates the field using values obtained from the field itself.

16.1 Complexity of the Mandelbrot Field

The choice of the Mandelbrot field is mathematically significant. Shishikura established that the boundary of the Mandelbrot set has Hausdorff dimension

$$\boxed{\dim_H(\partial M) = 2}$$

which is the maximum Hausdorff dimension possible for a subset of the complex plane.

This result establishes structure at arbitrarily fine scales. The significance for JFES is that the transformation engine is operating within a mathematical field possessing structure at every scale of observation, rather than within a finite table of predetermined values.

JFES accesses this structure recursively.

The distinction is fundamental:

$$\boxed{\text{Mandelbrot field} \neq \text{table of random values}}$$

Instead,

$$\boxed{\text{Mandelbrot field} \to \text{recursive evaluation} \to \text{new coordinates} \to \text{recursive evaluation}}$$

The complexity is therefore not merely observed. It is traversed.

16.2 Trajectory Complexity

At a selected precision p, divide the accessible field into a finite collection of distinguishable regions represented by a partition

$$\mathcal{P}_p.$$

The JFES trajectory produces a symbolic sequence

$$s_1, s_2, s_3, \ldots$$

where s_n identifies the partition element containing c_n.

For a trajectory of length n, let

$$N_p(n)$$

denote the number of distinct distinguishable trajectory sequences obtainable under the selected precision and transformation rules.

The corresponding trajectory complexity rate can be expressed as

$$\boxed{h_p = \limsup_{n\to\infty} \frac{\log_2 N_p(n)}{n}}$$

measured in bits per trajectory step.

This provides a mathematical bridge between the complexity of the field and the information generated by recursive navigation:

$$\boxed{\text{Field complexity} \to N_p(n) \to h_p}$$

The larger the number of distinguishable trajectories, the larger the space of possible future states.

16.3 Unpredictability

The relevant property for entropy extraction is not simply the existence of a large state space. It is the inability to determine the subsequent trajectory without performing the transformation.

Given

$$c_{n+1} = T(c_n),$$

the next coordinate is obtained by evaluating the Mandelbrot transformation and applying the JFES coordinate transformation.

The sequence therefore has the form

$$c_1 \to T(c_1) \to T^2(c_1) \to T^3(c_1) \to \cdots$$

with

$$c_n = T^{n-1}(c_1).$$

The output at each stage becomes the input to the next stage.

Consequently, JFES does not obtain its transformation stream by selecting values from a precomputed random table. The stream is generated by recursively evaluating the mathematical field.

The relationship proposed by this work is therefore

$$\boxed{\text{Complexity} \rightarrow \text{recursive trajectory space} \rightarrow \text{unpredictability} \rightarrow \text{entropy}}$$

This is the mathematical basis for treating JFES as an entropy-extraction mechanism.

16.4 Finite Precision and the Mathematical Field

JFES implementations operate at finite precision. For example, the current free JFES implementation uses 1024 bits of coordinate precision.

This implementation limit does not define the mathematical extent of the Mandelbrot field.

Let the coordinate precision be p. Increasing p permits progressively finer distinctions between points:

$$p_1 < p_2 < p_3 < \cdots$$

and therefore permits access to progressively finer structure within the field.

The mathematical field itself has no corresponding maximum precision.

Thus:

$$\boxed{\text{Implementation precision} \neq \text{mathematical complexity of the field}}$$

JFES extracts a finite stream from an underlying mathematical structure that remains accessible at increasing precision.

16.5 The Entropy Extraction Principle

The mathematical architecture can therefore be stated compactly.

A starting coordinate

$$c_1 = x_1 + iy_1$$

is supplied to the Mandelbrot transformation. The resulting complex trajectory determines successive coordinates:

$$c_1 \rightarrow c_2 \rightarrow c_3 \rightarrow \cdots$$

Each coordinate is evaluated through the Mandelbrot function, and the resulting complex values determine the next coordinate.

JFES therefore performs

recursive navigation of the Mandelbrot field

rather than linear sampling.

The entropy-extraction model proposed by this work is consequently:

Mandelbrot complexity → JFES recursive navigation → trajectory complexity → unpredictability → entropy

This is the mathematical foundation of the JFES entropy-extraction hypothesis.

17 The Research Proposition

The complete proposition can now be stated:

> **A deterministic transformation does not obtain entropy merely by expanding a finite-entropy input. JFES instead accesses the mathematical complexity of the Mandelbrot field through recursive navigation, where the value obtained at one coordinate determines the next coordinate.**

This gives rise to a testable proposition:

Mandelbrot complexity + recursive navigation → unpredictable trajectory

The empirical question is then whether the resulting trajectory demonstrates the characteristics expected of a high-quality entropy source.

JFES provides an experimental platform for that investigation.

18 Conclusion

The argument developed in this paper begins with a simple observation:

> **The practical value of entropy is its unpredictability.**

From there:

Unpredictability requires access to complexity.

And:

The greatest possible mathematical complexity is unbounded complexity.

The Mandelbrot fractal provides a uniquely interesting mathematical domain because its boundary has been proven by Shishikura to possess Hausdorff dimension 2—the maximum possible dimension in the complex plane.

JFES does not merely scan that structure.

It navigates it.

A coordinate is evaluated through Mandelbrot iteration. The resulting values determine the next coordinate. That coordinate is again evaluated in the Mandelbrot field. The process therefore forms a recursively generated trajectory through the field.

$$\boxed{(x_1, y_1) \to V_1 \to (x_2, y_2) \to V_2 \to (x_3, y_3) \to \cdots}$$

The underlying mathematical field has no 1024-bit boundary. The 1024-bit limit belongs to the free JFES implementation. The commercial version is configurable.

The fundamental research proposition is therefore not that deterministic arithmetic magically creates randomness.

It is that **recursive navigation through an infinitely complex mathematical field provides access to an enormous space of possible unpredictable trajectories whose unpredictability can be harvested as entropy-quality transformation material.**

Principal References

- C. E. Shannon, "Communication Theory of Secrecy Systems," *Bell System Technical Journal*, 28(4), 656–715, 1949.
- M. Shishikura, "The boundary of the Mandelbrot set has Hausdorff dimension two," *Astérisque* 222, 389–405, 1994.
- M. Shishikura, "The Hausdorff dimension of the boundary of the Mandelbrot set and Julia sets," *Annals of Mathematics*, 147, 225–267, 1998.
- G. Tiozzo, "Topological entropy of quadratic polynomials and dimension of sections of the Mandelbrot set," *Advances in Mathematics*, 273, 651–715, 2015.
- https://portalz.solutions/jfesGauge/JFES-Gauge.html