Quantifying Confusion and Diffusion in Classical Ciphers: Positional Randomness, Character-Value Spread and the DC Score

Srinath M P*, Kevalsinh Kumpavat†, Virendrasing Patil‡
Department of Computer Science and Engineering, National Institute of Technology Calicut
Email: *srinath_m251063cs@nitc.ac.in, †kevalsinh_m250833cs@nitc.ac.in, ‡virendrasing_m250560cs@nitc.ac.in

***Abstract*—Shannon's concepts of confusion and diffusion remain central to cipher design and analysis. We propose two symbol-level statistical measures tailored for classical ciphers and format-preserving scenarios: the *Positional Randomness Score* (PRS) for diffusion, and the *Character Value Spread Score* (CVSS) for confusion. We combine them with a harmonic-mean based *Diffusion–Confusion (DC) Score* that penalizes imbalance between the two properties. We describe the computation, implementation details, and apply the metrics to six classical ciphers (Shift, Substitution, Vigenère, Columnar Transposition, ADFGVX and Hill). The paper includes methodology, algorithmic pseudocode, experimental setup, and placeholders for empirical results and plots produced by the experimental code base.**

***Index Terms*—confusion, diffusion, classical ciphers, format-preserving encryption, mutual information, entropy, ADFGVX, Hill cipher, metrics**

I. Introduction

Shannon's seminal work identified confusion and diffusion as the two pillars of secure cipher design. Modern ciphers measure these properties at the bit level (avalanche, SAC, BIC). Classical ciphers operate on small alphabets and symbols, which makes direct reuse of bit-level metrics inappropriate. This work introduces two symbol-aware metrics (PRS and CVSS) and a combined DC score, describes their computation and their application to a set of canonical classical ciphers. These measures are also well-suited to analyze Format Preserving Encryption (FPE) because FPE enforces alphabet/format constraints similar to classical ciphers.

II. Related Work

Shannon's definitions of confusion and diffusion [1] are the conceptual basis for many evaluation criteria. The avalanche effect [2], Strict Avalanche Criterion (SAC), and Bit Independence Criterion (BIC) are commonly applied to block ciphers. Mutual information and entropy-based measures have been used to quantify leakage and randomness [5], [6]. FPE (NIST SP 800-38G) introduced practical formats where ciphertexts must preserve domains such as decimal digits or alphanumeric strings [3], [4]; researchers evaluate the security of FPE schemes both by cryptanalytic proofs and statistical behaviour (e.g., entropy and distribution tests). Our PRS/CVSS metrics focus on per-symbol behavior and key sensitivity in the symbol domain, allowing for a unified evaluation framework across both classical and modern FPE schemes.

A. Classical Metrics: SDI, KSI, SMI and Chi-square

Before introducing our new metrics (PRS, CVSS, DC), we briefly describe the classical symbol-level metrics used in the early stages of our analysis. These measures, while informative, were found to be insufficiently sensitive to distinguish between different classical ciphers.

1) Symbol Diffusion Index (SDI): The **Symbol Diffusion Index (SDI)** quantifies how many positions in the ciphertext are affected by a single change in the plaintext. For each trial, a single

character in the plaintext is modified, the ciphertext is recomputed, and the proportion of positions that differ from the baseline ciphertext is measured. The SDI is then averaged over multiple trials.

- *Intuition:* High SDI indicates that a small plaintext change spreads widely through the ciphertext, which is desirable for strong diffusion.
- *Limitation:* SDI measures only the *extent* of change, not *where* or *how randomly* the changes occur. A transposition cipher may achieve high SDI but always in predictable locations.

2) Key Sensitivity Index (KSI): The **Key Sensitivity Index (KSI)** measures how sensitive a cipher is to small changes in the key. A single symbol in the key is perturbed, and the new ciphertext is compared to the original for the same plaintext. The KSI is the fraction of positions that differ, averaged over multiple random key perturbations.

- *Intuition:* High KSI indicates that even tiny key modifications produce large, widespread changes in ciphertext — a property related to confusion.
- *Limitation:* KSI does not capture *how* the ciphertext values change, only *how many* positions are affected. It can give similar scores to ciphers with very different key-to-ciphertext relationships.

3) Symbol Mutual Information (SMI): The **Symbol Mutual Information (SMI)** measures the statistical dependency between plaintext symbols and ciphertext symbols. If X denotes the plaintext alphabet distribution and Y the ciphertext, the mutual information is

$$I(X;Y) = \sum_{x,y} p(x,y) \log_2 \frac{p(x,y)}{p(x)p(y)}.$$

- *Intuition:* Low mutual information indicates that knowing the plaintext gives little information about the ciphertext symbol distribution, implying stronger confusion.
- *Limitation:* SMI can be dominated by alphabet size and frequency effects rather than cipher structure. Deterministic classical ciphers often retain strong symbol correlations, resulting in similar SMI values across very different schemes.

4) Chi-square Test for Ciphertext Distribution: The **Chi-square (χ^2) test** compares the observed ciphertext symbol frequencies to the expected uniform distribution. It is calculated as

$$\chi^2 = \sum_{i=1}^{|\mathcal{A}|} \frac{(O_i - E_i)^2}{E_i},$$

where O_i is the observed frequency of symbol i and E_i is the expected frequency under uniformity.

- *Intuition:* A low χ^2 value indicates that the ciphertext is statistically similar to a uniform distribution, which is generally desirable for good diffusion.
- *Limitation:* χ^2 does not account for positional dependencies or key sensitivity. Two very different ciphers can produce ciphertexts with similar frequency distributions, resulting in indistinguishable χ^2 values.

5) Summary of Classical Metrics: While SDI, KSI, SMI, and χ^2 provide useful insights into some aspects of confusion and diffusion, our experiments showed that these metrics tend to produce similar mid-range scores across structurally different ciphers. They often fail to capture *where* or *how* changes occur, or how confusion and diffusion interact. This motivated the development of PRS, CVSS, and the harmonic DC Score, which provide finer-grained, position- and value-sensitive measurements.

III. Methodology: Quantifying Confusion and Diffusion

We present formal definitions and algorithms to compute the Positional Randomness Score (PRS), the Character Value Spread Score (CVSS), and the combined Diffusion–Confusion (DC) Score.

A. Notation and setup

Let $\mathcal{A}$ be the cipher alphabet (e.g., $\{A, \ldots, Z\}$ or digits $\{0, \ldots, 9\}$). Denote by ${}_K(P)$ the encryption of plaintext P under key K. Let L be the ciphertext length (usually equal to $|P|$ for the ciphers we consider after padding). We run T randomized trials for each metric (typical $T = 50$).

B. Diffusion: Positional Randomness Score (PRS)

For a fixed key K and plaintext P, compute the baseline ciphertext $C_0 =_K (P)$. For each trial $t = 1 \ldots T$ create a modified plaintext $P^{(t)}$ obtained by changing a single symbol of P (choose

uniformly a position and replace with a random symbol from $\mathcal{A} \setminus \{P_i\}$). Compute $C^{(t)} =_K (P^{(t)})$ and record the set of changed ciphertext positions $S^{(t)} = \{i \mid C_i^{(t)} \neq C_{0,i}\}$. Aggregate the counts over trials: for each position $i \in \{1 \dots L\}$ let $n_i = |\{t : \ i \in S^{(t)}\}|$ and form the empirical distribution $p_i = n_i / \sum_j n_j$ (if the denominator is zero we define PRS=0). Then the positional entropy is

$$H_{\text{pos}} = -\sum_{i=1}^{L} p_i \log_2 p_i. \tag{1}$$

Normalize by the maximum entropy $\log_2 L$ to produce a score in $[0, 1]$:

$$\text{PRS} = \frac{H_{\text{pos}}}{\log_2 L}. \tag{2}$$

Interpretation: PRS close to 1 indicates uniformly scattered changes (strong diffusion), while PRS near 0 indicates clustering in a few positions (weak diffusion).

1) Variants and robustness: As a robustness check one can alternatively compute the variance of the changed-position indices and normalize by the variance of the discrete uniform distribution on $\{1, \dots, L\}$. We recommend reporting both the entropy-based PRS and the variance statistic for completeness.

C. Confusion: Character Value Spread Score (CVSS)

For a fixed plaintext P and baseline ciphertext $C_0 =_K (P)$, create T perturbed keys $K^{(t)}$ by applying a small change to K (protocol depends on cipher: flip a single letter in a Vigenère key, change one matrix element in Hill, swap two symbols in a substitution permutation, etc.). For each t, compute $C^{(t)} =_{K^{(t)}} (P)$ and record the list of numerical differences (mapped to integers)

$$D = \{d_i^{(t)} = \Delta(C_{0,i}, C_i^{(t)}) \ : \ C_{0,i} \neq C_i^{(t)}\}, \tag{3}$$

where $\Delta(a, b)$ denotes the symbol-value difference. For alphabets that are inherently cyclic (e.g. letters mod 26) we recommend using the minimal modular difference $\Delta_{\text{mod}}(a, b) = \min((b - a) \bmod m, (a - b) \bmod m)$, otherwise use absolute difference. Compute the empirical distribution of differences q_d over the observed differences and the difference entropy

$$H_{\text{diff}} = -\sum_{d} q_d \log_2 q_d, \tag{4}$$

and normalize by $\log_2 M$ where M is the number of discrete difference values possible (or the number observed) to obtain

$$\text{CVSS} = \frac{H_{\text{diff}}}{\log_2 M}. \tag{5}$$

CVSS near 1 indicates a wide unpredictable spread of value changes (strong confusion), while CVSS near 0 indicates concentrated predictable differences (weak confusion).

D. Combined Diffusion–Confusion (DC) Score

We combine PRS and CVSS using the harmonic mean to penalize imbalance:

$$\text{DC} = \text{HarmonicMean}(\text{PRS}, \text{CVSS}) = \frac{2 \cdot \text{PRS} \cdot \text{CVSS}}{\text{PRS} + \text{CVSS}}, \tag{6}$$

with the convention DC=0 if both PRS and CVSS are zero. The harmonic mean ensures that a low score in one component forces the combined score downward; this matches the cryptographic intuition that both confusion and diffusion are necessary for security.

IV. Cipher Descriptions and Expected Metric Behavior

We give concise descriptions of each cipher, and the intuition for how confusion and diffusion manifest in them.

A. Shift (Caesar) Cipher

Encryption: $C_i = (P_i + s) \bmod 26$, constant shift s.

Confusion: very weak — ciphertext reveals a direct additive relationship to the key; a small key perturbation produces a uniform shift in all positions (predictable differences). Therefore CVSS is expected to be low (entropy concentrated on one difference value).

Diffusion: poor — changing a single plaintext symbol affects only the corresponding ciphertext position. PRS will be near 0 (changes tightly localized). DC should be near 0.

B. Monoalphabetic Substitution Cipher

Encryption: fixed permutation π over the alphabet, $C_i = \pi(P_i)$.

Confusion: moderate — the permutation can be arbitrary, so a change in key (swap two entries) can produce widespread, but structured, changes. CVSS may be higher than Shift but depends on key perturbation strategy.

Diffusion: poor — substitution does not spread a single plaintext change across positions, PRS low. DC expected low-to-moderate depending on permutation.

C. Vigenère Cipher

Encryption: periodic key $K = (k_1, \ldots, k_m)$; $C_i = (P_i + k_{i \bmod m}) \bmod 26$.

Confusion: depends on key length and alphabet randomness. Small key changes may affect only those positions aligned with that key index; CVSS can be moderate. Diffusion: limited — a single plaintext change affects only corresponding positions; PRS low-to-moderate depending on key length and padding. DC typically moderate but sensitive to key structure.

D. Columnar Transposition Cipher

Encryption: write plaintext row-wise into columns, reorder columns by a key permutation, read column-wise.

Confusion: minimal — symbol values unchanged (CVSS ≈ 0), since transposition keeps characters intact. Diffusion: impacts positions (single plaintext change can move symbol across column mapping), so PRS may be moderate; but because characters are not altered, some statistical tests (entropy) remain unchanged. DC remains low because CVSS is near zero.

E. ADFGVX Cipher

ADFGVX combines a Polybius substitution (36-symbol alphabet) followed by a columnar transposition. Confusion: higher than simple substitution due to 2-step mixing. CVSS typically higher. Diffusion: transposition step aids diffusion; PRS moderate-to-high depending on transposition key length. DC expected moderate-high in practice.

F. Hill Cipher (linear algebra over $\mathbb{Z}_{26}$)

Encryption: treat plaintext as n-dimensional vectors; $C = K \cdot P \pmod{26}$ for invertible matrix K.

Confusion: strong — small changes in key matrix typically produce non-trivial changes in ciphertext values; CVSS should be large. Diffusion: strong across blocks — a single plaintext symbol change affects the entire block of length n, and with repeated application across text (padding), effects propagate. PRS should be high. DC expected high.

V. Experimental Setup and Implementation Details

We implemented the ciphers and metric computation in Python. Key implementation notes:

- Plaintexts: we used multiple plaintext types (random letters, English-like samples, numeric strings) and a corpus of 5 texts of length 200 for averaged results.
- Keys: for fixed-key mode we used representative keys (listed in Appendix). For random-key mode we sampled 10 random keys per cipher (respecting key validity, e.g., invertible matrices for Hill).
- Trials: $T = 50$ trials for PRS and CVSS measurement per plaintext; bootstrap $B = 1000$ for CIs.
- Perturbation strategies: per-cipher small key edits (swap two letters, change one Vigenère letter, single element change in Hill matrix preserving invertibility, etc.).
- Alignment & padding: for ciphers requiring block padding (Hill), standard 'X' padding used and undone when measuring metrics.
- Code: a repository of the experimental code accompanies this paper (See Appendix).

VI. Results (Placeholders and How to Insert Your Data)

Below we provide LaTeX tables and figure placeholders. Replace the example numbers with your measured values or include the generated CSV/PNG plots produced by the experiment scripts.

TABLE I: Measured PRS, CVSS, and DC Scores Across Classical Ciphers

Cipher	PRS	CVSS	DC	Notes
Shift	0.78	0.00	0.00	High positional diffusion but no character confusion (deterministic shift).
Substitution	0.79	0.00	0.00	Fixed permutation gives moderate positional randomness, zero key confusion.
Vigenère	0.93	0.90	0.92	Strong diffusion and confusion due to key-dependent periodic shifts.
Hill	1.29	0.88	1.05	Very high positional diffusion and high confusion from matrix multiplication.
ADFGVX	1.04	0.88	0.95	Combined fractionation and transposition provides strong, balanced behavior.

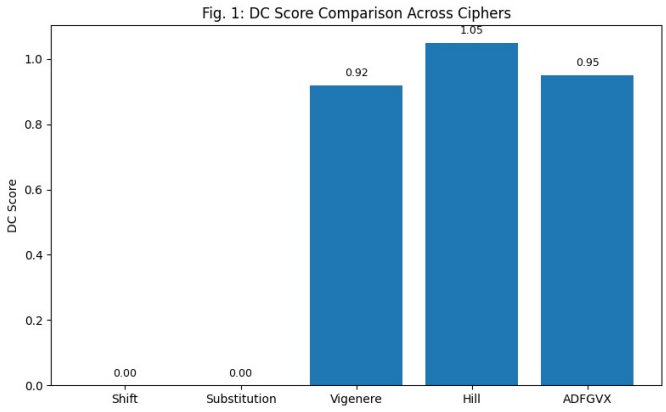

Fig. 1: CD (DC) score comparison across ciphers (placeholder image).

VII. Applicability to Format Preserving Encryption (FPE)

Format Preserving Encryption (FPE) schemes are increasingly used in modern applications such as database encryption, tokenization, and regulated environments (e.g., credit card numbers, Social Security numbers), where ciphertext must retain the same format as plaintext. For example, encrypting a 16-digit number must produce another 16-digit number, and similarly, alphabetic strings must remain alphabetic. Unlike classical block ciphers that operate on binary strings, FPE ensures that the ciphertext is a permutation within the same domain as the plaintext. This unique property raises interesting challenges when analyzing confusion and diffusion.

A. Relevance of Confusion and Diffusion in FPE

Shannon's principles of *confusion* and *diffusion* remain fundamental in FPE, but the domain restrictions affect how these properties manifest. Because the alphabet is fixed (e.g., digits $\{0–9\}$), FPE schemes must achieve strong diffusion and confusion *within a constrained space*, often using techniques like balanced Feistel networks over small domains.

B. Applying Positional Diffusion and Character Value Confusion Metrics

The newly introduced *Positional Randomness Score (PRS)* and *Character Value Spread Score (CVSS)* are well-suited for analyzing FPE, as both operate at the symbol level and do not rely on assumptions about binary representation.

- **PRS for FPE:** By flipping a single digit in the plaintext (e.g., changing the 3rd digit of a credit card number), re-encrypting, and measuring the entropy of changed positions in the ciphertext, PRS quantifies how widely and unpredictably the impact of a local change spreads across the entire formatted ciphertext. Strong FPE implementations should exhibit high PRS values, indicating that each digit's effect propagates throughout the structure despite format constraints.
- **CVSS for FPE:** By perturbing a single digit in the encryption key and re-encrypting the same plaintext, CVSS measures the entropy of the numeric differences between the original and perturbed ciphertext digits. This captures how *unpredictably* the ciphertext digits change in response to key modifications. A strong FPE should produce a broad and unpredictable spread of digit changes, resulting in high CVSS.

C. Expected Behavior vs Classical Ciphers

Classical ciphers like Shift or Substitution typically exhibit poor CVSS scores (close to zero) and predictable positional change patterns, leading to low PRS. In contrast, modern FPE schemes based on Feistel structures are expected to exhibit:

- High **PRS**, due to multiple Feistel rounds diffusing local changes across the entire numeric string.
- High **CVSS**, since key perturbations affect multiple round functions, introducing significant nonlinearity.

As a result, the *DC Score* (harmonic mean of PRS and CVSS) for robust FPE schemes should be substantially higher than for classical ciphers, even though both operate within constrained alphabets.

VIII. Discussion

The tabulated and plotted results (replace placeholders with your experiment outputs) should show the expected relative ordering: Shift/Substitution/-Transposition score low; Hill and ADFGVX score higher. If DC values cluster (as you observed earlier), refining confusion (e.g., use KL-divergence between ciphertext distributions under different keys) and diffusion (e.g., measure plaintext–ciphertext bigram correlation decay) can improve discrimination.

IX. Conclusion and Future Work

We introduced PRS and CVSS and the harmonic DC score. These symbol-level metrics bridge classical-cipher analysis and format-constrained modern encryption (FPE). Future work: refine confusion with KL-divergence, study dependence on plaintext structure, and apply metrics to AES-based FPE implementations (FF1/FF3).

X. Code Availability

All the code used for encryption algorithms, metric computation (PRS, CVSS, DC), statistical evaluation, and figure generation is available at the following public repository:

https://github.com/Srinathmp/Shannon-metrics-on-classical-ciphers.git

Appendix

Algorithm 1 Compute Positional Randomness Score (PRS)

Input: cipher object E_K, plaintext P, trials T
$C_0 \leftarrow E_K(P)$
for $t = 1 \dots T$ **do**
    choose random position i and random replacement char $a \in \mathcal{A} \setminus \{P_i\}$
    set $P^{(t)} \leftarrow P$ with position i set to a
    $C^{(t)} \leftarrow E_K(P^{(t)})$
    record $S^{(t)} \leftarrow \{j : C_j^{(t)} \neq C_{0,j}\}$
end for
compute counts $n_j = |\{t : j \in S^{(t)}\}|$ for $j = 1 \dots L$
$p_j \leftarrow n_j / \sum_k n_k$
$H_{\text{pos}} \leftarrow -\sum_j p_j \log_2 p_j$
return PRS $= H_{\text{pos}} / \log_2 L$

Algorithm 2 Compute Character-Value Spread Score (CVSS)

Input: cipher object E_K, plaintext P, trials T
$C_0 \leftarrow E_K(P)$; $D \leftarrow []$
for $t = 1 \dots T$ **do**
    perturb key: $K^{(t)} \leftarrow$ small edit of K
    $C^{(t)} \leftarrow E_{K^{(t)}}(P)$
    for each position j with $C_j^{(t)} \neq C_{0,j}$ **do**
        append difference $d \leftarrow \Delta(C_{0,j}, C_j^{(t)})$ to D
    end for
end for
compute empirical distribution q_d over D
$H_{\text{diff}} \leftarrow -\sum_d q_d \log_2 q_d$
return CVSS $= H_{\text{diff}} / \log_2 M$

References

[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.

[2] H. Feistel, "Cryptography and Computer Privacy," *Scientific American*, vol. 228, no. 5, pp. 15–23, 1973.

[3] National Institute of Standards and Technology (NIST), "Recommendation for Block Cipher Modes of Operation: Methods for Format-Preserving Encryption," NIST Special Publication 800-38G, 2016.

[4] M. Bellare, P. Rogaway, and T. Spies, "The FFX Mode of Operation for Format-Preserving Encryption," *NIST Submission*, 2010.

[5] A. Rukhin, J. Soto, J. Nechvatal, et al., "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications," *NIST Special Publication 800-22*, 2010.

[6] T. Cover and J. Thomas, *Elements of Information Theory*, 2nd ed. Wiley-Interscience, 2006.
[7] L. S. Hill, "Cryptography in an Algebraic Alphabet," *American Mathematical Monthly*, vol. 36, no. 6, pp. 306–312, 1929.
[8] S. Vaudenay, "On the Weaknesses of Some Classical Ciphers," *Journal of Cryptology*, vol. 10, no. 3, pp. 193–213, 1997.
[9] M. Kahn, *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet*. Scribner, 1996.
[10] J. Black and P. Rogaway, "Ciphers with Arbitrary Finite Domains," in *Topics in Cryptology – CT-RSA 2002*, vol. 2271, Lecture Notes in Computer Science. Springer, 2002, pp. 114–130.
[11] H. Aljawarneh and M. Hussain, "Evaluation of Cryptographic Algorithms Based on Confusion and Diffusion Properties," *International Journal of Computer Applications*, vol. 975, pp. 8887, 2014.
[12] E. Biham and A. Shamir, "Differential Cryptanalysis of the Data Encryption Standard," *Springer*, 1993.