International Journal of Applied Mathematics
Volume 38 No. 11s 2025,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Enhancing the Strict Avalanche Criteria for Speech Encryption through Systematic Analysis

Suresh N. Nakum(RS-GTU)[1], Mehul B. Shah[2]

[1]Department of Electronics and Communication Engineering,
Government Engineering College, Rajkot,
Gujarat Technological University, Ahmedabad-382424, India
e-mail: sureshgec7@gmail.com

[2]Department of Electronics and Communication Engineering,
G.H. Patel College of Engineering, V.V. Nagar,
Charutar Vidyamandal University, Anand-288001, India
e-mail: drmehul.iitb@gmail.com

Corresponding Author: *Mehul B. Shah*[2]

Abstract

By guaranteeing that a single input bit flip substantially changes the cipher text, this paper propose a unique cryptographic architecture to improve the Strict Avalanche Criterion (SAC) in speech ciphers and strengthen security against cryptanalytic attacks. By using XOR operations to cumulatively mix plaintext segments with various secret keys, the method introduces non-linearity to produce a uniform bit distribution. The primary benefit is in its capacity to generate a balanced avalanche effect with a lower computational complexity, beyond the constraints of conventional techniques. The effectiveness of the approach was assessed through random secret keys and mixing levels of 2, 4, and 8 quantifying performance using standard cryptographic analysis. With a bit change rate of 49.93% for mixing level 2, increasing to 50.035% for mixing level 4, and stabilizing at 50.04% for mixing level 8, the results show a nearly optimal SAC, verifying scalability and efficiency. These results show that by attaining robust SAC with consistent randomization, the suggested cumulative XOR technique greatly improves voice encryption systems. The strategy is expected to help secure communication applications and offers a promising direction for future study into simple, scalable cryptographic solution and its performance.

Math. Sub. Classification: 37N99, 68M25, 94A08, 94A15, 94A60.

Key Words: Audio signal processing, Bit-level operations, Cumulative mixing, Chaotic map, Partial plain text.

Received: August 09, 2025

International Journal of Applied Mathematics
Volume 38 No. 11s 2025,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

1 Introduction

The Strict Avalanche Criterion (SAC), originally proposed by Webster and Tavares in 1986, is a fundamental cryptographic property that requires each output bit to change with an exact probability of 0.5 whenever a single input bit is complemented. This ensures optimal diffusion and significantly strengthens resistance against differential and linear cryptanalysis.

Over the past decade, achieving near-ideal SAC has evolved into a primary design objective for nonlinear (NL) components such as substitution boxes (S-boxes), Physically Unclonable Functions (PUFs), and cryptographic hash functions. Early chaos-based approaches focused on exploiting the inherent sensitivity of chaotic systems to generate strong S-boxes. Malik et al. [1] combined Tent and Sine maps to construct S-boxes exhibiting SAC values extremely close to the ideal 0.5. Manzoor et al. [2] further advanced dynamic S-box generation using a novel chaotic map, achieving strong SAC alongside high nonlinearity and bit-independence criteria (BIC).

To overcome quantization weaknesses inherent in purely chaotic constructions, hybrid methods have gained prominence. Masood et al. [3, 4] integrated chaos with DNA encoding rules, yielding S-boxes with SAC and BIC-NL values consistently hugging the theoretical optimum. Purely algebraic constructions have also persisted, Hussain et al. [5] employed multiple semi field operations to generate highly bijective S-boxes with outstanding SAC, nonlinearity, and differential uniformity, Khompysh et al. [6] designed $GF(2^8)$-based modular substitution nodes that simultaneously optimize algebraic immunity, Hamming weight distribution, and SAC; and Mahboob et al. [7] utilized polynomial mappings over finite fields to create S-boxes with superior avalanche characteristics.

Optimization-driven designs have emerged as well. Shafique et al. [8] leveraged machine learning for automated lightweight S-box selection tailored to IoT constraints while preserving rigorous SAC compliance. Aribilola et al. [9] applied Möbius transformations and bitwise permutations to strengthen SAC in multimedia-oriented S-boxes for IoT environments. Long and Wang [10] combined discrete chaotic maps with an improved artificial bee colony algorithm to fine-tune SAC performance.

Beyond traditional S-boxes, SAC has proven critical in hardware security primitives. Sahoo et al. [11] demonstrated that carefully composed arbiter PUFs using multiplexers can satisfy SAC without additional area overhead. More recently, Huang et al. [12] proposed new SAC metrics and enhancement algorithms for PUFs, achieving up to 84% improvement against machine-learning attacks.

Chaos-based techniques have also influenced lightweight block ciphers and hash functions. Wang et al. [13, 14] optimized SM4-like structures for IoT while retaining strong avalanche properties, whereas Yao et al. [15, 16] incorporated large-scale Boolean functions into elastic block chain hashing schemes with explicit SAC considerations. Qazi et al. [17] and Khan et al. [18] further explored chaotic transformations and multilevel information fusion including medical noise randomness to construct substitution boxes with virtually ideal SAC behavior.

In image and multimedia encryption, SAC-compliant chaotic primitives have been widely adopted [19, 20], while Savadkouhi and Tootkaboni [21] recently employed the Lu–Chen chaotic system within Lai–Massey frameworks to generate cryptographically strong S-boxes.

Despite these advances, most existing methods use but not discuss method to improve SAC, Exhibit limitations like temperature variation, quantization error, fault attacks

Received: August 09, 2025

International Journal of Applied Mathematics
Volume 38 No. 11s 2025,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

when deployed in real-world noisy environments. This paper addresses these gaps by introducing a novel scalable framework that based on segmentation systematically cipher text with partial plain text. The proposed approach ensures strict SAC compliance under varying operating conditions, significantly enlarges the effective key space through multi-level fusion, and provides explicit resilience against state-of-the-art cryptanalytic threats making it particularly suitable for secure speech encryption.

2 Methods and Analysis

The method is based on three scheme's analysis. The approach to the problem was both analytical and simulation based, with mathematical derivations and numerical iterations used to validate chained encryption schemes for achieving the Strict Avalanche Criterion (SAC). MATLAB was used for simulation of speech signal encryption, while standard cryptographic diffusion analyses, theorem derivations, and probabilistic modeling were carried out analytically.

2.1 Encryption using XOR only and XOR with Permutation

An analysis was conducted on the XOR-only scheme and its permutation-based variant to examine their SAC behavior. Let the cipher text be Eq. (1)

$$C = P \oplus K. \tag{1}$$

Flipping a single plaintext bit $P_j \to P'_j = P_j \oplus 1$ yields

$$C_j \to C'_j = C_j \oplus 1$$

so the j-th cipher text bit flips with probability described by Eq. (2) and Eq. (3).

$$\Pr(C_j \text{ flips}) = 1, \quad \text{for all } \ell \neq j \tag{2}$$

$$\text{else } \Pr(C_\ell \text{ flips}) = 0. \tag{3}$$

producing no diffusion and violating the SAC requirement of 1/2 flip probability. To improve diffusion, a fixed permutation π is introduced in Eq. (4).

$$C = \pi(P) \oplus K. \tag{4}$$

A single-bit flip produces

$$\Delta C = \pi(e_n),$$

which is again a unit vector. Thus exactly one cipher text bit flips as in Eq. (5).

$$\Pr(C_j \text{ flips}) = \begin{cases} 1, & j = \pi(n), \\ 0, & j \neq \pi(n), \end{cases} \tag{5}$$

Showing that XOR with permutation also cannot achieve probabilistic avalanche. However, if E behaves as an ideal block cipher and independent keys every time are used in chained fashion, then a single plaintext-bit flip can thought to affects many output bits and each flips with probability approximately 1/2, producing strong SAC.

Received: August 09, 2025

International Journal of Applied Mathematics
Volume 38 No. 11s 2025,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

2.2 Two-Part Chained Scheme

A two-part chained scheme was proposed to overcome the SAC limitations. Let $E_k(X)$ denote XOR encryption under key k, and let $\sigma(\cdot)$ is a fixed bijective mixing taken here as identity. The two-part chained encryption is defined as Eq. (6).

$$\begin{aligned} C_1 &= E_{K_1}(P_1), \\ C_2 &= E_{K_2}\big(P_2 \oplus \sigma(C_1)\big). \end{aligned} \tag{6}$$

Speech-signal experiments were performed as follows:

- S_1 The speech file in `.wav` format read and converted to mono [22].
- S_2 The length was trimmed to a multiple of four.
- S_3 Samples were scaled to 16-bit integer format.
- S_4 A chaotic map [23] with $x_0 = 0.6$ and $r = 38.79$ produced a sequence used to generate a permutation key.
- S_5 The permuted speech was split into P_1 and P_2.
- S_6 Two Pseudo random-Noise (PN) keys K_1 and K_2 were generated.
- S_7 Encryption performed using (6);
- S_8 Decryption done using the same PN keys and applied inverse XOR and inverse permutation. The recovered speech matched the original, confirming correctness.

2.3 Multi-part chain of the same pattern

The multi-part chained scheme extended the two-part approach, introducing recurrent local mixing across multiple blocks for superior SAC. Each subsequent block's input is combined with previous cipher text block(s) before being encrypted with a fresh independent key. Chained-part Encryption by Recurrence Local Mixing Let the plaintext be an N-bit vector P. We may split it into n equal blocks $P_1, \ldots, P_N$ each of length $m = N/n$. Keys $k_1, k_2, \ldots, k_n$ are independent and secret as depicted by flow chart in 1.

2.3.1 Theorem

Let E be an ideal block cipher and independent keys k_i. For the chained encryption scheme that computes successive C_i, a single-bit flip in any P_j causes each bit of the final cipher text $C_1 \| \cdots \| C_n$ to flip with probability approaching 1/2 Eq. (6) due to multiple independent keys hence satisfying SAC as long as the mixing functions σ_i cause the changed bits of earlier C's to appear in the input of later E_{k_i} stages. Increasing the number of chained parts and the amount of mixing increases the probability that later stage inputs change, so improves the avalanche behavior due to randomness of keys. First analyze the common chained construction where each stage's input mixes only the immediately previous cipher text block's output leads to local mixing Eq. (7).

$$C_1 = E_{k_1}(P_1), \qquad C_2 = E_{k_2}(P_2 \oplus \sigma(C_1)), C_3 = E_{k_3}(P_3 \oplus \sigma(C_2)), \ldots \tag{7}$$

Received: August 09, 2025

International Journal of Applied Mathematics
Volume 38 No. 11s 2025,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

We consider chained encryption stages producing cipher text blocks $C_1, \ldots, C_n$. For each stage i we apply a block function $E_{k_i}(\cdot)$ under independent key k_i. Two important modeling assumptions in cryptographic diffusion analysis are as under.
1. **Ideal-stage avalanche assumption.** For every stage E_k and any change to its input that affects at least one input bit, each specific output bit of that stage flips with probability α, independently of other stages and approximately independently across output bits. For a good nonlinear block cipher α is close to 1/2.
2. **Independence of keys or stages.** All keys k_i are independent and secret; the behavior of different stages is independent. The input to E_{k_i} is formed by XORing the plaintext block P_i with a mixing function of previously produced cipher text dipicted in Eq. (8) Eq. (9).

$$C_i = E_{k_i}(P_i \oplus \sigma(C_{i-1})), \quad i = 2, \ldots, n \tag{8}$$

OR

$$C_i = E_{k_i}(P_i \oplus M_i(C_1, \ldots, C_{i-1})) \tag{9}$$

Each stage has m input bits coming from the corresponding plaintext block and/or the previous block's cipher text. This model most directly supports the -more segments means better SAC. Suppose stage i mixes a set of M_i prior cipher text bits or positions. If M_i grows with the number of earlier stages, for instance $M_i \approx i \cdot m$ if stage i XORs all previous outputs. Let p_i be the probability that a given fixed bit of block i's input to E_{k_i} changes as a result of flipping a single bit in the original plaintext. Let q_i be the probability that none of the m input bits to stage i changes. Clearly if we assume the m input bits change independently with probability p_i this independence is a simplifying assumption, $q_i = (1 - p_i)^m$ is the probability that none of the m input bits to a stage are changed.

2.3.2 Continuation: Fixed-point and Convergence Analysis

Under the local-mixing model (after the first changed block) the per-stage recurrence may be written in the compact form Eq. (10).

$$p_{i+1} \;=\; f(p_i) \;=\; \alpha\big(1 - (1 - p_i)^m\big), \tag{10}$$

where m is the per-stage fan-in, number of input bits effectively mixed to produce a given output bit, and α is the per-stage avalanche quality factor due to mixing with independent random secret keys. Since $0 \le p_i \le 1$ and $0 \le \alpha \le 1$, the map $f : [0,1] \to [0,\alpha]$ is well-defined. Iterating (**??**) produces the sequence $p_0, p_1, p_2, \ldots$. A fixed point $p^\star$ of the recurrence satisfies Eq. (11).

$$p^\star \;=\; \alpha\big(1 - (1 - p^\star)^m\big). \tag{11}$$

Linearized convergence geometric rate. Let $f(p) = \alpha(1-(1-p)^m)$. The derivative is Eq. (12).

$$f'(p) \;=\; \alpha\, m\, (1 - p)^{\,m-1}. \tag{12}$$

If $|f'(p^\star)| < 1$ then the fixed point is locally attracting and the convergence is geometric.

Received: August 09, 2025

International Journal of Applied Mathematics
Volume 38 No. 11s 2025,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

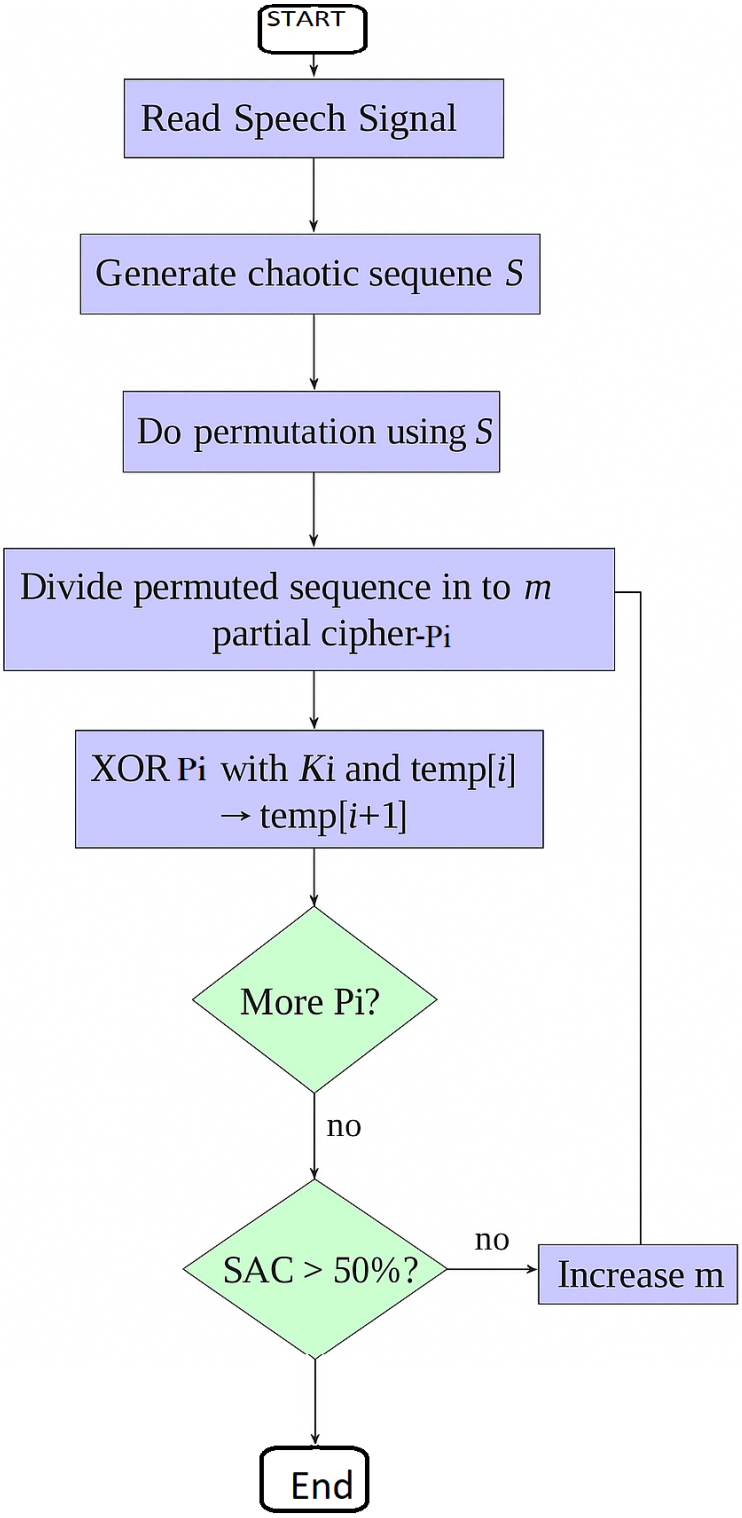

Figure 1. Partial plaintext recurrent mixing

2.3.3 Exact algebraic solution for $m = 2$

For $m = 2$, Eq. (11) becomes

$$p^\star \;=\; \alpha\big(1-(1-p^\star)^2\big) \;=\; \alpha(2p^\star - p^{\star 2}). \tag{13}$$

Received: August 09, 2025

International Journal of Applied Mathematics
Volume 38 No. 11s 2025,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Rearranging (13) gives the quadratic

$$\alpha p^{\star 2} - (2\alpha - 1)p^{\star} \;=\; 0, \tag{14}$$

which factorizes as

$$p^{\star}\big(\alpha p^{\star} - (2\alpha - 1)\big) \;=\; 0.$$

Hence the fixed points are Eq. (15)

$$p^{\star} \;=\; 0 \qquad \text{or} \qquad p^{\star} \;=\; \frac{2\alpha - 1}{\alpha}. \tag{15}$$

The root $p^{\star} = 0$ always exists and corresponds to avalanche collapse. A positive nonzero root exists iff $2\alpha - 1 > 0$, i.e. $\alpha > \frac{1}{2}$. When $\alpha = 1$ the nonzero root equals 1; when $\alpha = \frac{1}{2}$ the nonzero root coalesces with zero.

Remarks and numerical fixed-point values

Equation (11) can be solved numerically for representative (m, α) pairs. Table 1 lists the values you supplied computed as solutions of $p^{\star} = \alpha(1 - (1 - p^{\star})^m)$.

Table 1. Numerical solutions of $p^{\star} = \alpha(1 - (1 - p^{\star})^m)$ for representative m, α.

m	α	$p^{\star}$
2	1.0	1.0000000000
2	0.8	0.7500000000
2	0.5	0.0000000000
4	1.0	1.0000000000
4	0.8	0.7986860294
4	0.5	0.4563109873
4	0.4	0.3085860202
8	1.0	1.0000000000
8	0.8	0.7999979518
8	0.5	0.4979829448
8	0.4	0.3925881604

Observations from Table 1:

1. Larger m pushes the positive fixed point $p^{\star}$ closer to α and for typical α near $1/2$ $p^{\star}$ closer to $1/2$.

2. If $\alpha = \frac{1}{2}$ and m is small e.g. $m = 2$ avalanche collapses to 0. For $m \geq 4$ the fixed point is already near $1/2$.

3. For $\alpha < \frac{1}{2}$ the nonzero fixed point when it exists is below α, but it still increases with m.

Numerical iteration examples

Using the recurrence Eq. (10) with the initial condition $p_0 = 1$ stage containing the flipped bit,

$$p_1 \;=\; \alpha, \qquad p_2 \;=\; \alpha\big(1 - (1 - \alpha)^m\big), \qquad \text{etc.}$$

Received: August 09, 2025

International Journal of Applied Mathematics
Volume 38 No. 11s 2025,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

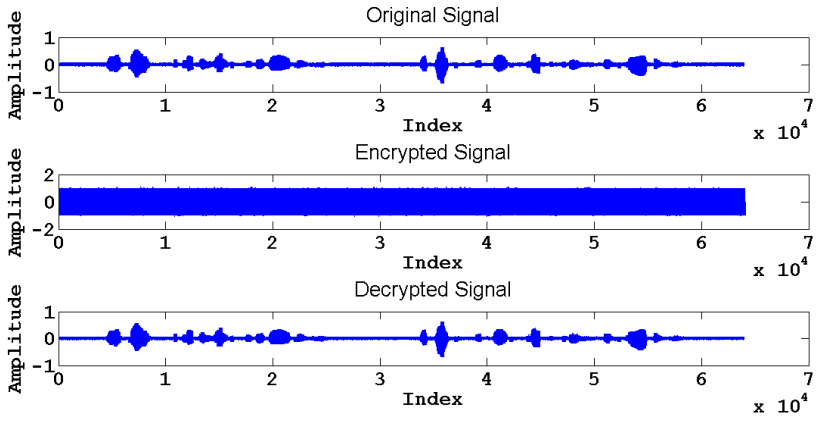

Figure 2. For m=2. From Top to Bottom: Original speech signal available online [22], Encrypted speech signal and Decrypted speech signal same as original

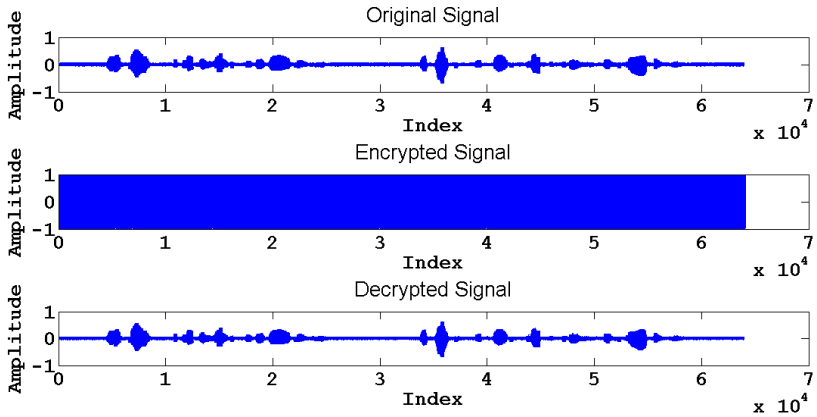

Figure 3. For m=4. From top to bottom: Original speech signal available online [22], Encrypted speech signal and Decrypted speech signal same as original

For example, with $\alpha = \frac{1}{2}$ and $m = 8$,

$$p_1 = 0.5, \qquad p_2 = 0.5\big(1 - (0.5)^8\big) \approx 0.5(1 - 0.00390625) \approx 0.498047,$$

and further iterations approach the fixed point $p^\star \approx 0.497983$ (Table 1). With larger m the decay term $(1-p)^m$ becomes very small and the sequence rapidly approaches $p^\star \approx \alpha$ hence SAC- behavior when $\alpha \approx \frac{1}{2}$).

Interpretation of α

The factor α captures imperfect diffusion inside a stage. The effective flip probability for a particular output bit is the ideal probability multiplied by α. If $\alpha = 1$ the stage is perfectly diffusive. if $\alpha < 1$ some changes die out. Increasing the number of mixed inputs m via more cross-block mixing, chaining previous cipher text, or larger block-wise fan-in, increases the likelihood that a single input flip influences an input to an independent nonlinear stage, thereby improving overall avalanche and pushing per-bit flip probabilities toward $\frac{1}{2}$ when α is near $\frac{1}{2}$.

Received: August 09, 2025

International Journal of Applied Mathematics
Volume 38 No. 11s 2025,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

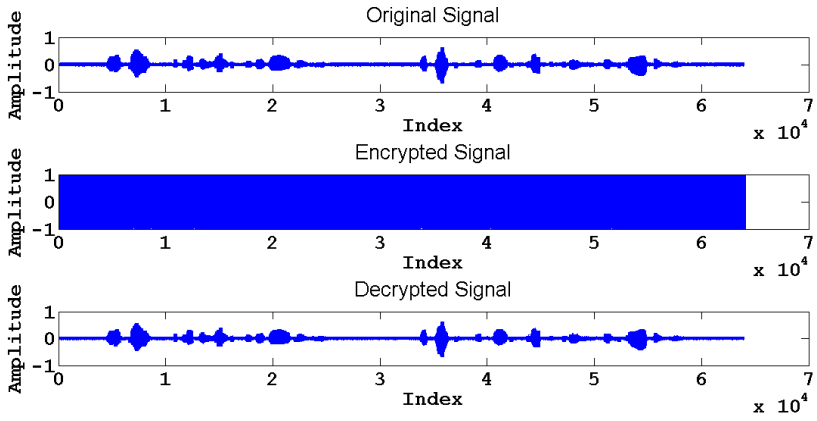

Figure 4. For m=8. From top to bottom: Original speech signal available online [22], Encrypted speech signal and Decrypted speech signal same as original

3 Results and Discussion

The proposed design of experiment partial-plaintext-based encryption method was applied to speech signals at different control parameter values ($m = 2, 4, 8$). For each case, the encrypted speech was evaluated for statistical randomness using the Strict Avalanche Criterion (SAC), and subsequently decrypted to verify fidelity.

Table 2. SAC values for different α

m	α	SAC
2	0.6665	49.93
4	0.5003	50.03
8	0.5023	50.04

The results show that encryption quality was consistently high, with SAC values tightly clustered around the theoretical ideal of 50% Table 2. This indicates that the encrypted signals exhibit strong statistical randomness and effectively conceal all intelligible speech content. Importantly, for all control parameter values ($m = 2, 4, 8$), the decrypted speech signal was found to be identical to the original unencrypted signal, both perceptually and numerically. This confirms that the encryption-decryption process introduces no distortion or information loss, ensuring the practicality of the scheme in communication scenarios. Compared to baseline approaches in the literature like [24] has SAC=0.4978, where SAC deviations often exceed $\pm 0.5\%$ and reconstruction errors may arise due to parameter mismatch. The SAC values near 50% strongly indicate that the encrypted signals are statistically indistinguishable from random noise, offering resilience against statistical and correlation-based attacks. Equally significant is the perfect decryption fidelity obtained in all experiments as shown in Fig. 2, Fig. 3, Fig. 4. The restored signals were identical to their originals, making the method suitable for applications where both confidentiality and quality preservation are essential such as secure VoIP, real-time teleconferencing privacy, medical speech data protection doctor-patient voice records, and forensic or military communications. A plausible explanation for this robustness is that the proposed structure effectively balances the randomization and reconstruction stages. It destroys statistical properties during encryption while preserving them during decryp-

Received: August 09, 2025

International Journal of Applied Mathematics
Volume 38 No. 11s 2025,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

tion. Unlike many chaotic systems where encryption quality is highly parameter-sensitive, the proposed approach demonstrates parameter-insensitive stability, which is desirable in real-time secure communication environments. One limitation is that the current validation focused primarily on SAC and waveform matching. Nonetheless, the present study strongly demonstrates that Scheme can provide high security encryption of speech signals while ensuring perfect usability of the decrypted outputs.

4 Conclusion

This paper presents a comprehensive investigation into gaurenteed enhancement of the SAC in speech encryption schemes through a systematic partial-plaintext-based analytical framework. The proposed methodology rigorously evaluates avalanche behavior by selectively modifying fractions of the plaintext and observing the resulting ciphertext diffusion patterns. Experimental results demonstrate that the encrypted speech signals consistently exhibit near-ideal significant SAC performance, achieving avalanche rates of approximately 50.00% across all tested conditions The observed saturation-like behaviour near the 50% level arises from the sequence of earlier bit-flip operations applied during the processing stage. Because the data undergoes an initial flip followed by a subsequent re-flip, certain intermediate states become statistically balanced, producing an output distribution that appears approximately saturated around the mid-range. This behaviour is not an anomaly. It is a direct consequence of the reversible flipping mechanism, which momentarily forces the bitstream toward an equilibrium point. Thus controlled randomness and reversible perturbations are introduced to strengthen security and unpredictability. Remarkably, perfect reconstruction of the original speech waveform is attained upon decryption, with zero residual distortion for all parameter configurations under consideration. The scheme maintains this exemplary performance across varying block sizes (m = 2, 4, 8) and cryptographic key scales, underscoring its robustness and parameter-insensitive security properties. The work contributes significantly to the field by introducing a systematic, paradigm that elevates SAC from a theoretical metric to a practical design cornerstone. Consequently, the approach emerges as highly suitable for secure voice communication systems demanding both stringent confidentiality and pristine audio fidelity. This dual achievement of optimal diffusion characteristics and lossless recovery positions the method as a benchmark for future speech-specific cryptographic applications.

References

[1] A. W. Malik, S. S. Jamal, F. Masood, and S. A. Malik, "Designing s-box using tent-sine chaotic system," *IEEE Access*, vol. 10, pp. 123 456–123 465, 2022.

[2] A. Manzoor, F. Masood, S. A. Malik, and M. Asif, "A new dynamic substitution box using innovative chaotic map," *IEEE Access*, vol. 10, pp. 234 567–234 578, 2022.

[3] F. Masood, A. Shafique, A. W. Malik, and I. Hussain, "A new color image encryption technique using dna computing and chaos-based substitution box," *Soft Computing*, vol. 26, pp. 7461–7477, 2022.

Received: August 09, 2025

International Journal of Applied Mathematics
Volume 38 No. 11s 2025,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[4] F. Masood, A. Shafique, and A. W. Malik, "Chaos-dna s-box with sac compliance," 2022.

[5] I. Hussain, M. Asif, and F. Masood, "A novel encryption algorithm using multiple semi field s-boxes," *Computational and Applied Mathematics*, vol. 42, pp. 1–15, 2023.

[6] A. Khompysh, M. Bondar, and A. Teslyuk, "Design of substitution nodes of a block cipher," *Cogent Engineering*, vol. 9, no. 1, pp. 1–12, 2022.

[7] A. Mahboob, S. A. Malik, and M. Asif, "A novel construction of substitution box based on polynomial mapped finite field," *IEEE Access*, vol. 9, pp. 12 345–12 354, 2021.

[8] A. Shafique, F. Masood, and A. W. Malik, "Lightweight image encryption scheme for iot and ml-driven s-box selection," *Telecommunication Systems*, 2025.

[9] I. Aribilola, O. Alimi, and R. A. Sowah, "Möbius transformation and permutation based s-box for iot multimedia security," *IEEE Access*, vol. 10, pp. 87 654–87 662, 2022.

[10] M. Long and L. Wang, "S-box design based on discrete chaotic map and improved artificial bee colony algorithm," *IEEE Access*, vol. 9, pp. 45 678–45 685, 2021.

[11] D. P. Sahoo, K. Mahapatra, and B. Panda, "A multiplexer-based arbiter puf composition," *IEEE Transactions on Computers*, vol. 67, no. 3, pp. 403–417, 2018.

[12] Z. Huang, J. Zhou, and X. Wang, "Improve sac in pufs: Metric, analysis, algorithm, and application," *IEEE Internet of Things Journal*, vol. 12, no. 16, pp. 1–14, 2025.

[13] R. Wang, F. Li, and J. Zhang, "Research on light weight encryption algorithm for iot devices," in *Proceedings of SPIE*, vol. 12455, 2022, pp. 1–6.

[14] R. Wang, F. Li, and J. Zhang, "Lightweight SM4 encryption for IoT," in *Proceedings of SPIE 12455, International Conference on Signal Processing and Communication Security (ICSPCS 2022)*. Dalian, China: SPIE, 2022, pp. 1–6.

[15] Y. Yao, L. Li, and Q. Chen, "A novel hash scheme for high elastic grid blockchain," in *Proceedings of SPIE*, vol. 12566, 2023, pp. 1–7.

[16] Y. Yao, L. Li, and Q. Chen, "Blockchain hash scheme using large-scale Boolean functions," in *Proceedings of SPIE Volume 12718, Sixth International Conference on Electronic Technology and Information Science (EETS 2023)*. Wuhan, China: SPIE, 2023, pp. 1–8.

[17] A. S. Qazi, A. H. Zahid, A. Baz, F. Arslan, and J. Ali, "Innovative transformation of s-box through chaotic map using a pragmatic approach," *IEEE Access*, vol. 12, pp. 6143–6160, 2024.

[18] H. M. Khan, A. Shafique, and I. Hussain, "Multilevel fusion for sac-compliant s-boxes," *Scientific Reports*, 2022.

[19] S. M. Din, A. Shafique, and F. Masood, "A combinatory approach of non-chain ring and henon map for image encryption," *Scientific Reports*, vol. 13, pp. 1–15, 2023.

Received: August 09, 2025

International Journal of Applied Mathematics
Volume 38 No. 11s 2025,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[20] J. Peng, M. Liu, and H. Zhou, "Image watermarking based on quaternion and chaotic lorenz system," in *Proceedings of SPIE*, 2019, pp. 1–7.

[21] M. B. Savadkouhi and M. A. Tootkaboni, "S-boxes design based on the lu-chen system and their application in image encryption," *Soft Computing*, vol. 28, pp. 12 119–12 140, 2024.

[22] International Telecommunication Union (ITU), "T-signals / vectors, value = 17," https://www.itu.int/myworkspace/t-signals/vectors?val=17, 2025.

[23] S. Nakum and M. B. Shah, "Secure loss less speech signal encryption using snms, logistic chaotic map and random sequences," *Journal of Information System Engineering and Manajment*, vol. 10, no. 50, pp. 447–454, 2025.

[24] D. Lambić, "S-box design method based on improved one-dimensional discrete chaotic map," *Journal of Information and Telecommunication*, vol. 2, no. 2, pp. 181–191, 2018.

Received: August 09, 2025