



An Intelligent Comparative Evaluation of the MDDM Framework for Secure Data Encryption Using Hill Cipher, Playfair and AES-128 -GCM

Ramya Krishnan M. K.^{1,*}, M. Raji²

¹ Research Scholar, Department of Mathematics, Vels Institute of Science, Technology and Advanced Studies, Chennai, Tamil Nadu, India.

² Assistant Professor, Department of Mathematics, Vels Institute of Science, Technology and Advanced Studies, Chennai, Tamil Nadu, India.

ARTICLE INFO

Article history:

Received 18 May 2026

Received in revised form 16 June 2026

Accepted 08 July 2026

Keywords: Graph cipher; MDDM; Hill cipher; Playfair; AES-GCM; integrity verification

ABSTRACT

The paper discusses a systematic comparative evaluation of MDDM (Matrix based Dominating set Driven Message Cipher) with three reference algorithms: Playfair Cipher, Hill Cipher, and AES-128-GCM. The aim of this study is not to place MDDM as a substitute for verified standard encryption, but to analyse how the developed graph-algebraic framework acts compared to classical matrix/substitution based cipher approach and an advanced engineering reference model. 57 plaintext cases, including both single-block and decomposed block inputs with each case repeats 10 times, are evaluated for the comparison. MDDM is evaluated along with two shared key modes: the unimodular/triangular key mode and the random invertible key mode. In the comprehensive run MDDM attains 14.38% average bit avalanche under triangular/unimodular key policy and 15.84% under random-invertible key policy, which is above Hill Cipher (8.45%) and Playfair (5.90%) but remains far below from AES-128-GCM (49.97%). MDDM also provides two internal integrity checks IC1 & IC2 that detected all 2,400 performed tampering tests, while Hill cipher and Playfair does not have such an integrated tamper protection. These contributions come with a clear observations that: In Python/SymPy Implementation MDDM is slower and the cipher text expansion is highest, approximately 20-21x. And the analysis support placing MDDM as a Cipher framework demonstrating graph-algebraic pipeline along with the integrity verification rather than a competing/reference method to AES-GCM.

1. Introduction

Cryptography is a word with Greek origins, means “secret writing”. However it is the science and art to transform the messages to make them secure and immune against security attacks. It is the technique to provide secure communication in presence of adversaries to maintain information securities such as data confidentiality, data integrity, authentication, and non-repudiation. The processes of cryptographic algorithms from classical to modern methods show continuous progress in protecting digital information.

There are two classifications of encryption algorithms namely: symmetric key algorithm is utilizing the same key, this type of cryptography plays a crucial role in securing data because the same key

* Corresponding author.

E-mail address: rajialagumurugan@gmail.com

is used for both encryption and decryption and asymmetric key algorithm is applying to different keys for encryption and decryption process, a public key and a private key respectively [9].

MDDM is a Matrix based Cipher framework derived from Dominating set together with two integrity checkers is a symmetric algorithm framework that convert Plain text into a Cipher through different stages of matrix operations. MDDM transform the plain text into a graph and provide node and edge weight, construct weighted adjacency matrix, and choose a minimum weight dominating set lead to prepare the Cipher matrix using a shared invertible key [1]. Since the framework is symmetric thus this paper choose symmetric algorithms for the comparison.

A careful comparison is essential for new encryption framework against the existing methods. For MDDM, a valid comparison should include both structurally related classical encryption framework and a modern authenticated encryption framework. The Hill cipher is the most comparable historical matrix-based framework. Playfair is a traditional substitution framework with different diffusion characteristics. AES-128-GCM is modern authenticated encryption framework.

This paper presents systematic comparison over a shared plaintext data and some common measures like Encryption-decryption time, size of cipher text and expansion ratio, bit-level avalanche, key space estimate, correlation between plaintext-cipher text and data integrity verification [7], [8].

The avalanche effect is a fundamental property of cryptographic algorithms, where a small change in the input causes a significant change in the output, thereby enhancing security [12]. Alam and Khan [13] and Singh and Dutta [14] compared symmetric cryptographic algorithms and highlighted the trade-off between security, computational efficiency, and performance in secure communication and cloud environments. Mandal et al. [15] and Bhat et al. [16] demonstrated that AES outperforms DES in terms of security and execution efficiency, making it more suitable for modern applications. Marzan and Sison [17] enhanced the Playfair cipher by improving key security and resistance to cryptanalysis. James and Priya [18] proposed a dynamic key-dependent S-box for IoT security, while Taher et al. [19] evaluated differently sized S-boxes using the avalanche effect and showed that well-designed S-boxes provide stronger diffusion properties. Abdulrazaq [20] developed a dynamic AES S-box based on a modified hexadecimal Playfair cipher, achieving improved randomness, nonlinearity, and resistance to cryptanalytic attacks while maintaining computational efficiency.

Graph Cipher tool provides a detailed description of the MDDM framework along with illustrations. The run time and size of encryption and decryption was evaluated and stored for various length inputs [2]. The comparison is deliberately limited. MDDM is implemented in Python with Exact algebraic computation, while AES-GCM uses a well optimized cryptographic library. Therefore in timing comparison reflect both the algorithmic and implementation quality. Diffusion, expansion and integrity characteristics under the defined evaluation framework are the strongest comparison claims.

2. Baseline Selection

2.1 MDDM

MDDM converts plain test into matrices derived from graphs and then construct the final cipher matrix.

$$C = M_4 \times K \quad (1)$$

Where K is the shared key matrix. The comparison describes two key modes; first uses the triangular/unimodular key modes with bound is equal to 10 and the second uses the random invertible key mode. In both modes, shared keys are consistent per block dimensions during the process so any plaintext alteration is not mixed with key variation.

2.2 Hill Cipher

Hill cipher is a classical cryptographic method invented by L.S Hill in 1929. It is a polygraphic substitution cipher. The Hill Cipher uses a number of mathematical techniques, which correlate too many key techniques in traditional cryptography. It is considered as the matrix-cipher framework because matrix multiplication is used to encrypt data [3], [4]. The introduced framework uses the 28-character MDDM alphabet and a fixed invertible 3 by 3 key over $Z = 28$.

2.3 Playfair Cipher

Playfair is a manual encryption framework and was the literal digram substitution cipher. The framework was invented in 1854 by Charles Wheatstone but was named after Lord Playfair who promoted the use of the cipher. The approach encrypts pairs of letters rather than single letters. It is adapted to MDDM 28-character alphabet using a 4 by 7 grid generated from the keyword GRAPHCIPHER.

2.4 AES-128-GCM

AES-128-GCM is included as a modern authenticated encryption framework, not as a peer validated research. It is designed as a 128-bit-key and an authenticity through GCM/GMAC [5], [6]. The comparison framework uses systematic testing keys and unique values for consistency.

3. Experimental Methodology

3.1 Corpus

All frameworks are evaluated on the same selected 57 case dataset from 28-character alphabet. The dataset contains the original six small single-block illustrations, arbitrary generated single-block cases with distinct vertex values, original block-mode messages, and randomly constructed longer block-mode messages.

One input message was excluded from the process because the selected Playfair framework did not recover it exactly. MDDM block-mode cases use deterministic block size 10.

3.2 Metrics

Timing is evaluated through Python `time.perf_counter()` over 10 repeats per plaintext. The size of Cipher text is measured in bytes under each frameworks defined serialization. The ratio between cipher text size and plaintext length is the expansion ratio. The result table shows average timing; median and standard deviation are stored in the JSON artefact.

Avalanche is evaluated by altering in plaintext characters and comparing the generated cipher text bit streams. In MDDM each matrix entry is converted into fixed-width binary representation using two's-complement and then these binary values serialized into bit stream. Hill cipher and Playfair adopt 5-bit character encoding because the size of alphabet is 28. AES-GCM uses byte-wise cipher text/nonce encoding.

The average absolute Pearson correlation between Plaintext bits and the prefix-aligned cipher text bit stream is referred as the plaintext-cipher text correlation. Correlation values should be considered as illustrative rather than conclusive.

4. Results

The comparison allows to analyse the act of MDDM framework against with the established substitution or matrix based structurally related frameworks. MDDM compares the avalanche, correlation, diffusion, performance, cipher text expansion and Integrity behaviour against with Hill cipher, Playfair and AES-GCM-128.

4.1 Summary Table

The comparison results of MDDM framework against with Hill cipher, Playfair and AES-GCM-128 along with both the triangular/unimodular family and the random invertible family are summarised in Table 1.

Table 1 Overview of the comparison results

Metric	MDDM triangular	MDDM random	Hill (n=3)	Playfair	AES-128- GCM
Key-space estimate (bits)	207.7	439.2	43.3	97.9	128.0
Average encryption time (ms)	22.4784	29.6018	0.0426	0.0076	0.0026
Median encryption time (ms)	8.0959	10.4309	0.0128	0.0035	0.0019
Average decryption time (ms)	47.8274	87.0701	0.0439	0.0063	0.0018
Median decryption time (ms)	21.8350	47.2885	0.0133	0.0025	0.0010
Average cipher text size (bytes)	599.2	620.4	29.6	29.0	56.6
Average expansion ratio	20.25x	21.00x	1.10x	1.04x	4.09x
Average bit avalanche (%)	14.38	15.84	8.45	5.90	49.97
Average absolute correlation	0.1065	0.0813	0.1018	0.1181	0.1035
Integrity verification	IC1 + IC2	IC1 + IC2	None	None	GCM tag

4.2 Diffusion

Average bit-level avalanche of MDDM's expanded data set is 14.38% under the triangular/unimodular key policy and 15.84% under random invertible key policy. This is stronger than both classical baselines in the same test frameworks: Hill cipher attains 8.45% and Playfair attains 5.80%. AES-128-GCM attains far stronger value at 49.97%, as expected for a well-established modern block-cipher technique.

The observations supports a narrower claim that MDDM enables a better nit-level diffusion that the opted classical frameworks under this expanded test framework, but it should not be reported as AES-GCM like on avalanche. An alteration in the Plaintext character affects weights of the graph, structure of the shortest path, matrices derived from dominating set, and the final cipher matrix, but block-mode serialization and consistent shared-key evaluation generates a more approximate avalanche estimate than the initial six-case run.

4.3 Performance

The current implementation of MDDM is slower than all opted frameworks. This is expected because the MDDM implementation focuses on accurate arithmetic and interpretability. It construct graphs, compute matrix transformation and use exact symbolic computations where necessary. Hill cipher and Playfair are lightweight classical frameworks, and AES-GCM is driven by efficient cryptographic libraries. Therefore the performance result should be placed as a research-oriented design choice, not as a basis for claim MDDM compares with AES-GCM execution.

4.4 Cipher text Expansion

The expansion ratio of MDDM is larger, under unimodular/triangular keys it is 20.25x and under random invertible keys it is 21.00x. This is a consequence of the current matrix-cipher framework representation: each block generates an integer matrix. Hill cipher and playfair frameworks are almost a one to one character correspondence, while AES-GCM

MDDM has the largest expansion ratio at 20.25x under triangular/unimodular keys and 21.00x under random-invertible keys. This is inherent to the current matrix-cipher representation: each block emits an integer matrix. Hill and Playfair are near one-to-one character transformations, while AES-GCM includes nonce and tag overhead. The representation-size trade-off is also where the MDDM framework gains its structural transparency. The output matrix of the framework supports intermediate verification and analyse the dataset that do not provided by the classical character-level ciphers.

4.5 Correlation

The low average absolute plaintext-cipher text correlation in the measured dataset of all algorithms are low. Average absolute correlation of MDDM under triangular/unimodular key policy is 0.1065 and under random-invertible key policy it is 0.0813. These values are comparable to Hill cipher (0.1018), Playfair (0.1181) and AES-GCM (0.1035). This evaluation is reasonably interpreted as a supporting indicator rather than a formal leakage analysis.

4.6 Integrity Behaviour

Message integrity in cryptographic framework is the process of checking the message authenticity. It ensures the message or input is not been altered or manipulated. The major feature of MDDM is its two internal integrity verifications: IC1 (the spectral integrity checker using the Laplacian spectrum) and IC2 (the hash based integrity checker).

- i. IC1 verifies the Cipher matrix against with the Laplacian spectrum driven from the adjacency matrix of complete graph. It is a pre-decryption verification, the receiver can check any alteration is occur before the expensive decryption process.
- ii. IC2 verifies the plaintext carrying matrix M_3^* through SHA-256 serialization. The forge-rate experiments in the repository, 8 tampering strategies were applied among 6 plaintexts with 50 trials per strategy, lead 2,400 trials total. IC1 and IC2 generates zero false accepts.

The results of the dual integrity verifications (IC1 & IC2) of different entry alterations are summarized in Table 2.

Table 2 Overview of the alterations in Dual Integrity verification

Strategy Group	Trials	IC1 false accepts	IC2 false accepts
Single-entry alterations	900	0	0
Multi-entry alterations	600	0	0
Raw/column interchange	600	0	0
Entry-wise scaling	300	0	0
Total	2,400	0	0

This should not be a strong claim as a formal message-authentication proof. IC1 and IC2 are two internal integrity checkers under the defined threat model. The standardized authenticated-encryption scheme GCM tag provides confidentiality and integrity protection to AES-GCM. Hill cipher and Playfair do not have a built-in integrity verification.

5. Discussion

The strongest result of the comparative study is not AES-level diffusion [10]; the expanded test harness provides a more conservative conclusion. The average bit-level avalanche is above the two opted classical framework and far below AES-GCM. Its strongest key contribution remains the dual integrity checker: IC1 and IC2 detect all tested non-synchronized alterations.

The core trade-offs are performance and expansion [11]. The research implementation of MDDM is with exact arithmetic thus the framework is slower. It expands the cipher text because the framework generate matrix valued output rather than a byte string. These are major implementation drawback.

The comparison therefore support the following characterization:

- i. MDDM is a graph-algebraic research framework.
- ii. Under the expanded dataset MDDM is stronger than Hill and Playfair on diffusion, but not comparable to AES-GCM on avalanche or the execution rate.
- iii. It should not be introduced as an execution rate alternative for AES-GCM.
- iv. The novelty of MDDM is the integration of matrix generation, graph-theoretic diffusion, and the dual integrity checker.

6. Threats to Validity

There are several limitation for the comparison:

- i. The dataset contains 57 accepted cases, but this is still small relative to production cryptographic evaluation.
- ii. MDDM is evaluated under both triangular/unimodular key modes and the random invertible key mode; if the formal key bound, size of the block, or graph family changes the result should be regenerated.
- iii. The comparison related to timing combine with exact Python/SymPy code with AES-GCM based on an optimized library implementation.
- iv. Playfair processing with repeated node digraphs discarding the information, so the dataset neglect those cases.
- v. The integrity verification tests illustrative tampering examples; it is not a complete authentication proof.

7. Reproducibility

The comparison can be reproduced with:

Python tools/comparison_run.py

Python tools/comparison_run_expanded.py

Python tools/ic_forge_analysis.py

Python tools/avalanche_analysis.py

Primary artifacts:

- i. papers/paper4_comparison/comparison_results.json
- ii. papers/paper4_comparison/comparison_results_expanded.json
- iii. papers/paper1_algorithm/ic_forge_analysis.json
- iv. papers/paper1_algorithm/avalanche_results.json
- v. tools/comparison_harness.py
- vi. tools/baselines.py

8. Conclusion

The security of a cryptosystem depends on the architecture of the algorithm. This section analysis the cryptosystems in the basics of key generation, key length, block size and number of rounds used for encryption and decryption process. The rate at which a particular algorithm encrypts the data is an essential parameter in analysing the performance of encryption algorithms. This paper provides an analytical study on various symmetric encryption algorithms Hill cipher, Playfair, AES-GCM with MDDM framework. Each of the encryption techniques has its own strong and weak points. In order to apply a suitable cryptography algorithm to an application, we should have knowledge regarding performance, strength and weakness of the algorithms. The systematic comparison shows that MDDM exceeds the opted classical frameworks on bit-level avalanche under the expanded test framework and provides a dual internal integrity checkers that detected all tested tampering attempts. The expanded experimental results also corrects an important initial claim: MDDM should not be described as an avalanche like AES-GCM. AES remains far stronger on diffusion and data processing rate. Also it is implemented in suitable engineering standard for production authenticated encryption.

Author Contributions

Conceptualization, Ramya Krishnan M. K.; methodology, Ramya Krishnan M. K.; software, Ramya Krishnan M. K.; validation, Ramya Krishnan M. K.; formal analysis, Ramya Krishnan M. K.; investigation, Ramya Krishnan M. K.; resources, Ramya Krishnan M. K.; data curation, Ramya Krishnan M. K.; writing—original draft preparation, Ramya Krishnan M. K.; writing—review and editing, Ramya Krishnan M. K.; visualization, Ramya Krishnan M. K.; supervision, M. Raji; project administration, M. Raji. All authors have read and agreed to the published version of the manuscript.

Funding

This research received no external funding.

Data Availability Statement

The data supporting the findings of this study are available from the corresponding author upon reasonable request. No publicly archived datasets were generated or analyzed during the current study.

Conflicts of Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgement

The authors express their sincere gratitude to the Department of Mathematics, Vels Institute of Science, Technology and Advanced Studies, Chennai, Tamil Nadu, India, for providing the necessary facilities and support to carry out this research. This research was not funded by any grant.

References

- [1] Ramya Krishnan, M. K., Vibitha Kochamani, V., & Raji, M. *MDDM: A matrix-based dominating-set driven cipher framework with integrated spectral integrity verification*. Manuscript under review. (Communicated).
- [2] Ramya Krishnan, M. K., & Raji, M. *Graph Cipher: An open-source Python framework for graph-algebraic matrix cipher framework*. In *Proceedings of ICARMSEET (2025–26)*. Nova Science Publishers. (Accepted).
- [3] Hill, L. S. (1929). Cryptography in an algebraic alphabet. *The American Mathematical Monthly*, 36(6), 306–312.
- [4] Ismail, I. A., Amin, M., & Diab, H. (2006). How to repair the Hill cipher. *Journal of Zhejiang University SCIENCE A*, 7(12), 2022–2030.
- [5] National Institute of Standards and Technology. (2001). *Advanced Encryption Standard (AES)* (FIPS PUB 197).
- [6] Dworkin, M. J. (2007). *Recommendation for block cipher modes of operation: Galois/Counter Mode (GCM) and GMAC* (NIST Special Publication 800-38D). National Institute of Standards and Technology.
- [7] Webster, A. F., & Tavares, S. E. (1986). On the design of S-boxes. In *Advances in Cryptology—CRYPTO '85* (pp. 523–534). Springer.
- [8] Safdar, M. (2025). A graph-based cryptographic framework using complete graphs and lower triangular identity key matrices. *Global Integrated Mathematics*, 1(1), 66–83.
- [9] Bruen, A. A., Forcinito, M. A., & McQuillan, J. M. (2021). *The fundamentals of modern cryptography* (pp. 83–108).
- [10] Verma, R., & Sharma, A. K. (2020). Cryptography: Avalanche effect of AES and RSA. *International Journal of Scientific and Research Publications*, 10(4), 119–122.
- [11] Mushtaq, M. F., Jamel, S., Disina, A. H., Pindar, Z. A., Shakir, N. S. A., & Deris, M. M. (2017). A survey on the cryptographic encryption algorithms. *International Journal of Advanced Computer Science and Applications*, 8(11).
- [12] Kumar, A., & Tiwari, N. (2012). Effective implementation and avalanche effect of AES. *International Journal of Security, Privacy and Trust Management*, 1(3–4), 31–34. <https://doi.org/10.5121/ijspmt.2012.1303>
- [13] Alam, M. I., & Khan, M. R. (2013). Performance and efficiency analysis of different block cipher algorithms of symmetric key cryptography. *International Journal of Advanced Research in Computer Science and Software Engineering*, 3(10), 713–720.
- [14] Singh, V. K., & Dutta, M. (2014). Analysing cryptographic algorithms for secure cloud network. *International Journal of Advanced Studies in Computer Science and Engineering*, 3(4), 1–9.
- [15] Mandal, A. K., Parakash, C., & Tiwari, A. (2012). Performance evaluation of cryptographic algorithms: DES and AES. In *IEEE Students Conference on Electrical, Electronics and Computer Science* (pp. 1–4). IEEE. <https://doi.org/10.1109/SCEECS.2012.6184991>
- [16] Bhat, B., Ali, A. W., & Gupta, A. (2015). DES and AES performance evaluation. In *International Conference on Computing, Communication and Automation* (pp. 887–890). IEEE. <https://doi.org/10.1109/CCAA.2015.7148500>
- [17] Marzan, R. M., & Sison, A. M. (2019). An enhanced key security of Playfair cipher algorithm. In *Proceedings of the 2019 8th International Conference on Software and Computer Applications* (pp. 457–461). <https://doi.org/10.1145/3316615.3316689>
- [18] James, D., & Priya, T. (2023). An innovative approach for dynamic key dependent S-box to enhance security of IoT systems. *Measurement: Sensors*, 30, Article 100923. <https://doi.org/10.1016/j.measen.2023.100923>
- [19] Taher, H. M., Al-Rahman, S. Q. A., & Shawkat, S. A. (2022). Best S-box amongst differently sized S-boxes based on the avalanche effect. *International Journal of Electrical and Computer Engineering*, 12(6), 6535–6544. <https://doi.org/10.11591/ijece.v12i6.pp6535-6544>
- [20] Abdulrazaq, N. N. (2024). Generating a dynamic and secure S-box for AES block cipher system based on modified hexadecimal Playfair cipher. *Zanco Journal of Pure and Applied Sciences*, 36(5), 82–94. <https://doi.org/10.21271/ZJPAS.36.5.8>