International Journal of Advanced Engineering: Artificial Intelligence, Robotics and Automation
ISSN 3049-396X
Vol.:2 Issue: 1
Published online on: Dec 2025
PP. 42--45

The Role of Matrices in Modern Scientific and Technological Innovation: A Cross Disciplinary Approach

Jitendra Sharma [1], Pramod Dubey[2], Sanjay Sharma[3], Anand kumar Singh[4],
[1,2,3,4]Vikrant University, Gwalior, India

ABSTRACT
Applied mathematics has many tools for the purpose of security. Amongst these tools Matrices play a significant role in the field of scientific research and technological research fields. The structured form and algebraic properties of Matrices help the researchers in elegant representation and manipulation of complex systems. This paper examines the extensive implementation of matrices in various fields; to solve modern human life problems. In the field of computer it is used for graphics rendering, machine learning and cryptography. In Physics, matrices are used to describe quantum mechanics, applied mechanics and dynamic systems, Cryptography depends on mathematical operations. Through cryptography a messages or information can be converted in any other message but these message conversion in reverse order without help of a secret key is very hard task or challenging task . These "hard problems" provide security because attackers cannot feasibly break the encryption.

KEYWORDS: Number theory, RSA algorithm, Elliptic Curve Cryptography (ECC), Post-quantum cryptography, Modular arithmetic, Digital signatures, Zero-knowledge roofs.

INTRODUCTION:

Applications of Matrices:

Matrices form the backbone of modern scientific and technological developments. From quantum mechanics and relativity to robotics, cyber security, biology, and internet search engines, their applications are vast and indispensable. Mastery of matrix operations enables understanding, modeling, and solving complex problems across nearly every field of science and engineering. Matrices play a fundamental role in mathematics, physics, engineering, computer science, biology, and many applied sciences[1,2]. They are used to represent data, model systems, perform transformations, and solve complex equations. Below is a detailed discussion of the applications of matrices across different domains. In physics, many systems are represented using state vectors, and physical quantities such as energy, momentum, or angular momentum are represented by operators, which take the form of matrices[3]. When an operator acts on a state vector, it provides measurable physical information about the system. Quantum mechanics heavily relies on matrices. The Schrödinger equation, especially in discrete or finite-dimensional systems, is solved using matrix operations[4,5]. The Hamiltonian of a system is expressed as a matrix, and its eigenvalues give the allowed energy levels. Particles like electrons exhibit spin, a quantum property.

The behaviour of spin-½ particles is described using Pauli matrices, which help calculate probabilities, angular momentum components, and other spin-related properties. In classical and quantum physics, matrices are used to describe rotations and transformations in 2D and 3D. Rotation matrices help convert coordinates between different orientations without changing the shape or size of objects[6,7,8]. The moment of inertia tensor, expressed as a matrix, relates angular velocity to angular momentum. This representation is essential in analyzing the rotation of rigid bodies. Special relativity uses Lorentz transformation matrices to convert time and spatial coordinates between observers moving at high velocities relative to each other. The geometry of space-time is described using the metric tensor, which is essentially a matrix. This matrix helps calculate space-time distances,

Corresponding Author's E-mail ID: Jitendrarajsharma@gmail.com

curvature, and gravitational effects predicted by Einstein's theory. When expressed in the language of special relativity, Maxwell's equations for electromagnetism use matrix and tensor notation, simplifying the representation of electric and magnetic fields. Crystals have symmetry operations such as rotation, reflection, and inversion. These operations are represented using transformation matrices that help classify crystal structures. Matrices are used in quantum models like the tight-binding method or Hamiltonian matrix to calculate electronic energy bands in solids. In paraxial optics, ray transfer matrices describe how light rays pass through mirrors, lenses, and other components. They simplify optical system design and analysis. Matrices help organize and store large quantities of data systematically for easy retrieval, comparison, and analysis in scientific institutions and laboratories. In industries and businesses, matrices help track the production, distribution, and counting of goods efficiently[,9,10,11].

Matrices are used in multivariate analysis, particularly in dimensionality reduction methods like PCA (Principal Component Analysis), to analyse chemical mixtures and spectral data. Matrix models are used in optimization, forecasting, and resource allocation, such as planning irrigation, crop yield prediction, and managing natural resources. Bioinformatics uses matrix-based algorithms to compare DNA sequences, analyse gene expression, and create similarity score matrices[12,13]. MRI and CT scan machines reconstruct images from raw data using matrix transformations, Fourier transforms, and numerical methods. Transition matrices in Markov chains model how diseases spread across populations, helping in epidemiology and public health planning. Matrices perform essential geometric transformations such as translation, scaling, and rotation for rendering graphics in games, simulations, and animations.

Digital images are stored as pixel matrices. Operations like blurring, sharpening, filtering, compression, and edge detection use matrix convolution and transformations. Matrices are used to encode and decode messages securely. Techniques like the Hill cipher use invertible matrices as secret keys. Matrix algorithms help secure digital files, hidden channels, and web pages by scrambling data into unreadable formats except for authorized users. Complex algorithms use matrices and eigenvalues to generate secure keys and ensure safe communication, especially in defence sectors. PageRank uses a stochastic matrix to model backlinks between web pages. Eigenvectors of this matrix determine how pages are ranked in search results. These algorithms use matrix computations to analyse web structures, classify content, and determine page importance and security. Matrices are essential in robotics for: Describing robot motion (kinematics and dynamics), Performing rotations and translations of robotic arms, Designing control algorithms, Programming robotic systems efficiently with matrix operations. The size of matrices often represents the degrees of freedom of the robot, helping design precise movements[16,17].

Application of Matrix in field of Cryptography

Cryptography is used to change information into a new message or form that is without change of meaning to anyone who doesn't know about the secret key to decrypt message.

Matrices are an important keyin cryptography, primarily through techniques like the Hill cipher, which utilizes matrix multiplication for encryption and decryption. The process involves converting plaintext into numerical representations, arranging them into matrices, and then applying a secret matrix **(the "key")** through multiplication to encrypt the message. Decryption is the reverse process of encryption .it can be found as product of the encrypted matrix and reciprocalof the key matrix.

The basic idea of cryptography is that a secret message can be translated or changedby applying any encryption method and decoded by anyone who knows that encryption method. There are so many encryption techniques in which some are some very easy and some are very difficult. Most of them are connected with mathematics.

Today, very confidential announcements aresharedover the net every moment such as financial credentials, personal identifiers photos and crucial security passwords, letters or passwords for important databases, etc. All this information is encoded or encrypted.

In using of matrix-based encryption system, where an encoder matrix (K) is used to encrypt a message matrix (P), the encryption process is represented by the equation

$$\mathbf{E = K * P,}$$

Where E is the encrypted matrix. The decoder, which is the inverse of the encoder (K^{-1}), is then used to retrieve the original message by applying the operation $\mathbf{P = K^{-1} * E.}$

Matrix encryption involves converting a message into numbers, arranging converting them into matrix, and then

Corresponding Author's E-mail ID: soet_sandeep@vikrantuniversity.ac.in

multiplying it by a secret key matrix to encrypt it. For decryption, the reciprocal of the secret key matrix is used to multiply the encrypted matrix.

Example:

Step 1: Message: "VIKRANTUNIVERSITY"

Now break into blocks of 3 letters: VIK RAN TUN IVE RSI TYX

(Note: we add 'X' at the end to pad to multiple of 3.)

Step 2: Convert Letters to Numbers (A=0, B=1…….Z=25)Break into 3-letter vectors:

C_1 = [21, 8, 10]

C_2 = [17, 0, 13]

C_3 = [19, 20, 13]

C_4 = [8, 21, 4]

C_5 = [17, 18, 8]

C_6 = [19, 24, 23]

Step 3: Choose a 3x3 Key Matrix

Let's choose this invertible matrix (mod 26):

$$K = \begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}$$

This is a commonly used key matrix known to be invertible mod 26.

Encryption-We'll now multiply each vector with the key matrix mod 26.

◈ First block: [21, 8, 10]

Encrypted $P = K \cdot C \mod 26$

$$P = \begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix} x \begin{bmatrix} 21 \\ 8 \\ 10 \end{bmatrix} \mod 26$$

$$P = \begin{bmatrix} 16 \\ 7 \\ 4 \end{bmatrix}$$

Step 4: Convert Numbers Back to Letters:

16 → Q, 7 → H, 4 → E

Encrypted Message: "QHE"

Repeat this process for each block

Then we will get **"QHELNPJVFKMFWRMLDP"** as encrypted form.

Decryption-For the process of decryption or to find out our correct message, we will use the inverse of the key matrix (or K^{-1}) with modulo 26:

$$K^{-1} = \begin{bmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{bmatrix} \mod 26$$

Now we will follows all steps in reverse orders:

Encrypted Vector: "QHE" → [16,7,4]

$$C = \begin{bmatrix} 16 \\ 7 \\ 4 \end{bmatrix}$$

Here we apply multiplication process with inverse key:

$$P = K^{-1} \cdot C \mod 26$$

$$P = \begin{bmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{bmatrix} x \begin{bmatrix} 16 \\ 7 \\ 4 \end{bmatrix} \mod 26$$

Compute it:

$$P = \begin{bmatrix} 8X16 + 5X7 + 10X4 \\ 21X16 + 8X7 + 21X4 \\ 21X16 + 12X7 + 8X4 \end{bmatrix} \mod 26$$

$$P = \begin{bmatrix} 203 \\ 476 \\ 452 \end{bmatrix} \mod 26$$

$$P = \begin{bmatrix} 21 \\ 8 \\ 10 \end{bmatrix}$$

Corresponding Author's E-mail ID: soet_sandeep@vikrantuniversity.ac.in

Convert Numbers Back to Letters:

$$21 \rightarrow V,\ 8 \rightarrow I,\ 10 \rightarrow K$$

Decrypted Message: "VIK"

We will continue this process till all the blocks are decrypted.

Then we will get **"VIKRANTUNIVERSITY"** in a correct format after decryption process.

Conclusion:

The conclusion of the present research paper is evaluating the active role of matrices in cryptography, where matrices contribute to secure communication by converting sensitive information into encrypted formats resistant to unauthorized access. Matrix-based encryption techniques, such as the Hill Cipher, showcase how linear algebra supports the development of strong encryption schemes founded on mathematically difficult problems. The use of invertible key matrices, modular arithmetic, and vector transformations forms the backbone of reliable encryption–decryption processes. As demonstrated through examples in the present paper, these techniques ensure that encoded messages remain inaccessible without the correct inverse key, thereby enhancing security in digital communication.

References

[1] Strang, G. (2006). Introduction to Linear Algebra (4th ed.). Wellesley-Cambridge Press.

[2] Luenberger, D. G., & Ye, Y. (2008). Linear and Nonlinear Programming (3rd ed.). Springer.

[3] Nocedal, J., & Wright, S. J. (2006). Numerical Optimization(2nd ed.). Springer.

[4] Cormen, T. H., Leiserson, C. E., Rivest, R. L., & Stein, C. (2009). Introduction to Algorithms (3rd ed.). MIT Press.

[5] Horn, R. A., & Johnson, C. R. (1985). Matrix Analysis. Cambridge University Press.

[6] Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1996).Handbook of Applied Cryptography. CRC Press.

[7] Koblitz, N. (1994).A Course in Number Theory and Cryptography(2nd ed.). Springer.

[8] Menezes, A. J. (2010).Elliptic Curve Public Key Cryptosystems. Springer.

[9] Katz, J., &Lindell, Y. (2020).Introduction to Modern Cryptography (3rd ed.). Springer.

[10] Shoup, V. (2009).A Computational Introduction to Number Theory and Algebra (2nd ed.). Cambridge University Press.

[11] Cohen, H. (2007).A Course in Computational Algebraic Number Theory. Springer.

[12] Chou,T.Y.&He,L.(2004). Matrix-Based Ciphers:A New Approach to Classical Cryptography.International Journal of Computer Science and Network Security,4(9), 110.

[13] Menezes, A. J., &Oorschot, P. C. (2006).Cryptography: A Modern Approach (2nd ed.). Addison-Wesley.

[14] Rivest, R. L., Shamir, A., &Adleman, L. (1978).A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM, 21(2), 120–126.

[15] Lang, S. (2002).Algebra (3rd ed.). Springer.

[16] Helleseth, T., &Karvonen, T. (2002).Applications of Matrices in Stream Ciphers and Cryptography.

[17] Larsen, K. L. (2005).Mathematical Cryptography: Matrix Approach to Cryptosystems. Springer.

[18] Blake, I. F., &Seroussi, G. (2005).Elliptic Curves in Cryptography. Springer.

[19] Coppersmith, D. (1996).Small Solutions to Polynomial Equations, and Applications to Cryptography. Journal of Cryptology, 10(4), 233–260.

Corresponding Author's E-mail ID: soet_sandeep@vikrantuniversity.ac.in