International Journal on Science and Technology (IJSAT)
E-ISSN: 2229-7677 ● Website: www.ijsat.org ● Email: editor@ijsat.org

Encoding and Decoding in Cryptography Using Inverse Matrix and Nonhomogeneous Matrix Methods

Mr. Ranjeet S. Patil [1], Dr. Pravin Sonwalkar[2]

[1]Assistant Professor, Department of Basic Science and Humanities, Yashoda Technical Campus, Satara, MH, India.
[2]Assistant Professor, Department of Management, YTC, Satara, MH, India.

Abstract

Information refers to any form of digital content stored electronically. Ensuring security means safeguarding valuable assets. Data security encompasses the digital protection protocols that block unauthorised access to computers, personal databases, and online platforms. Cryptography remains an evolving field with ongoing advancements. It helps protect users by offering tools for encrypting data and verifying the identity of users. Cryptography is widely used for confidentially transmitting sensitive information. Modern information security systems focus on key principles such as confidentiality, authenticity, integrity, and non-repudiation. This paper includes encoding and decoding using the nonhomogeneous matrix method AM =X. Where A is the encoding Matrix and M is the message matrix. X is an unknown message.

Keywords: Encoding, decoding, Inverse Matrix, Nonhomogeneous Matrix method

1. Introduction

Cryptography originates from the Greek words "kryptos," meaning hidden, and "graphein," meaning writing; combined, cryptography translates to hidden writing. Cryptography involves the practice of secret messaging or confidential communication between two parties, whether individuals or groups, to ensure that the privacy of the message remains protected from unauthorised access **[1]**. Data encryption involves creating a random sequence of bits specifically for encrypting and decrypting information. Encryption is built on algorithms designed to ensure that each key generated is both unique and unpredictable. Cryptography employs two types of keys: symmetric and asymmetric. Symmetric keys have been in use the longest, relying on a single key for both the encryption and decryption of data, known as a secret key. Secret-key encryption methods are divided into two main types: stream ciphers and block cyphers. A block cypher uses a private key and an algorithm to encrypt an entire block of data at once, whereas a stream cipher processes the key and algorithm one bit at a time. Most cryptographic systems use symmetric encryption to secure data transmissions, while asymmetric encryption is used to securely exchange the secret key. Symmetric encryption, also called private key encryption, uses the same key for both encoding and decoding the data. However, a key risk in this system is that if the key is lost or intercepted, the system is compromised, and secure communication can no longer take place **[2]**. Farshid Haidary Makoui **[3]** et al. studied non-square binary matrices that have a wide range of applications across various fields, including mathematics, error-correction coding, machine learning, data storage systems, navigation signal processing,

and cryptography. Also, they introduce an algorithm for generating these matrices, along with a technique for constructing a random inverse matrix. The method is further extended to non-square matrices over arbitrary fields, addressing the limitations of the Moore-Penrose and Gauss-Jordan approaches. Additionally, its relevance to public-key cryptography is explored. CH. Ravi Kishore et al. **[4]** studied a Public Key Cryptography system based on non-homogeneous linear equations, describing it as a two-stage secured algorithm. In this approach, a system of non-homogeneous linear equations is generated, followed by the development of algorithms for key generation and public encryption. The security of this method is grounded in solving systems of equations over the ring of integers, which are classified as NP-complete problems. Aswathi Thomas et al. **[5]** The transition from traditional public key algorithms like RSA and Diffie-Hellman to the Elliptic Curve Cryptosystem (ECC) has gained momentum, primarily due to ECC's efficiency in achieving equivalent security with significantly shorter key sizes. While ECC offers clear advantages, it still suffers from computational delays due to the complexity of its arithmetic operations. In response to this challenge, recent research has introduced a modified cryptosystem that integrates RSA with ECC, enhanced by the use of a newly designed Montgomery multiplier algorithm. This novel approach targets efficiency improvements, particularly in speeding up computations. The system addresses the delay issues associated with elliptic curve operations by embedding the modified Montgomery algorithm within ECC. Simulations demonstrate considerable advancements, showing marked improvements in both speed and power consumption, making the system more practical for real-world applications. Kishore Kumar et al. **[6]** studied Traditional encryption methods, while commonly used, often struggle with efficiency and robustness in the presence of noise. Recent advancements in machine learning, such as autoencoders and Masked Autoencoders (MAEs), have demonstrated their potential in image encryption due to their ability to mask and reconstruct images effectively. Additionally, neural cryptography, utilizing Tree Parity Machines (TPMs), presents an innovative approach to secure key exchange. In this context, the proposed MAN–C scheme integrates MAEs with TPMs and Shamir's Secret Sharing Scheme to enhance security in the transmission of medical images. This combination addresses the issue of image degradation from noise during transmission while ensuring confidentiality. Kenan Begovic et al. **[7]** explored various methods for detecting ransomware activities, particularly during the encryption stage. Key techniques include monitoring system calls and APIs, tracking input/output operations, and observing file system behavior. In these approaches, machine learning has played an increasingly important role by improving the accuracy and timeliness of detection. However, a disconnect remains between the advancements in academic research and the capabilities of commercial ransomware defense products. They review existing detection methods and emphasize the critical window for identifying ransomware activity during the encryption phase. They also discuss gaps between academic findings and practical implementation in the commercial cybersecurity landscape. B. Ranganatha Rao et al. **[8]** developed a public cloud security model using Hybrid Elliptic Curve Cryptography (HECC). They utilized a lightweight Edwards curve for generating cryptographic keys and integrated Identity-Based Encryption (IBE) to strengthen the security of private keys. To further optimize the system, they introduced a key reduction technique, which shortened the key length, thus improving the speed of the Advanced Encryption Standard (AES) encryption process. For secure key exchange, they employed the Diffie-Hellman protocol. They evaluated their model based on metrics such as throughput, key generation time, encryption, and decryption times. Their findings demonstrated that the proposed HECC model significantly outperformed existing cloud security methods. They achieved a key generation time of 0.000025 seconds, an encryption time of 0.00349 seconds, and a throughput of 693.10 kB/s. These results show the effectiveness of the developed technique in enhancing both the efficiency and security of public cloud systems. Edward Keitaro Heru et al. **[9]** implemented a modified version of the

Menezes-Vanstone Elliptic Curve Cryptography (ECC) algorithm to enhance the security of text, image, audio, and video data. This algorithm, recognized for its efficiency in providing strong encryption with smaller key sizes, was integrated into a program designed for file encryption and decryption across these data types. The researchers compared the performance of their modified ECC approach with alternative encryption methods, focusing on metrics such as encryption speed and file size. Their study results demonstrated that the proposed method achieved better efficiency, particularly in terms of file size reduction. The encrypted files produced by the modified ECC program were smaller compared to those encrypted by other techniques, indicating its potential for optimizing storage and transmission in secure communications. The findings emphasize the effectiveness of the Menezes-Vanstone ECC algorithm in providing robust data security while maintaining lower overhead. Volodymyr Rudnytskyi et al. **[10]** identify and analyze contradictions that exist between the development of encryption algorithms for information security systems and encoding algorithms used to protect data in computer systems and networks. They propose that one effective solution to these challenges is the establishment of a theory of cryptographic encoding.The authors delve into the origins of research surrounding information encoding processes, particularly focusing on the role of cryptographic primitives. Through a comprehensive synthesis and analysis of encryption algorithms viewed from the perspective of discrete devices, they aim to reassess the classification of cryptographic algorithms. This approach facilitates the identification of potential directions for developing new cryptographic algorithms, as well as enhancing existing ones. the authors analyze the relationships between symmetric and asymmetric ciphers, proposing a novel approach for constructing asymmetric stream ciphers. They also present methodologies for increasing both the block length of information and the key length for both newly developed and established encryption algorithms. The article includes various implementation options and examples of encryption algorithms, showcasing their findings and suggesting practical applications. Overall, this work contributes to the field of cryptography by offering fresh perspectives on algorithm design and presenting strategies to improve the robustness and efficiency of cryptographic systems.

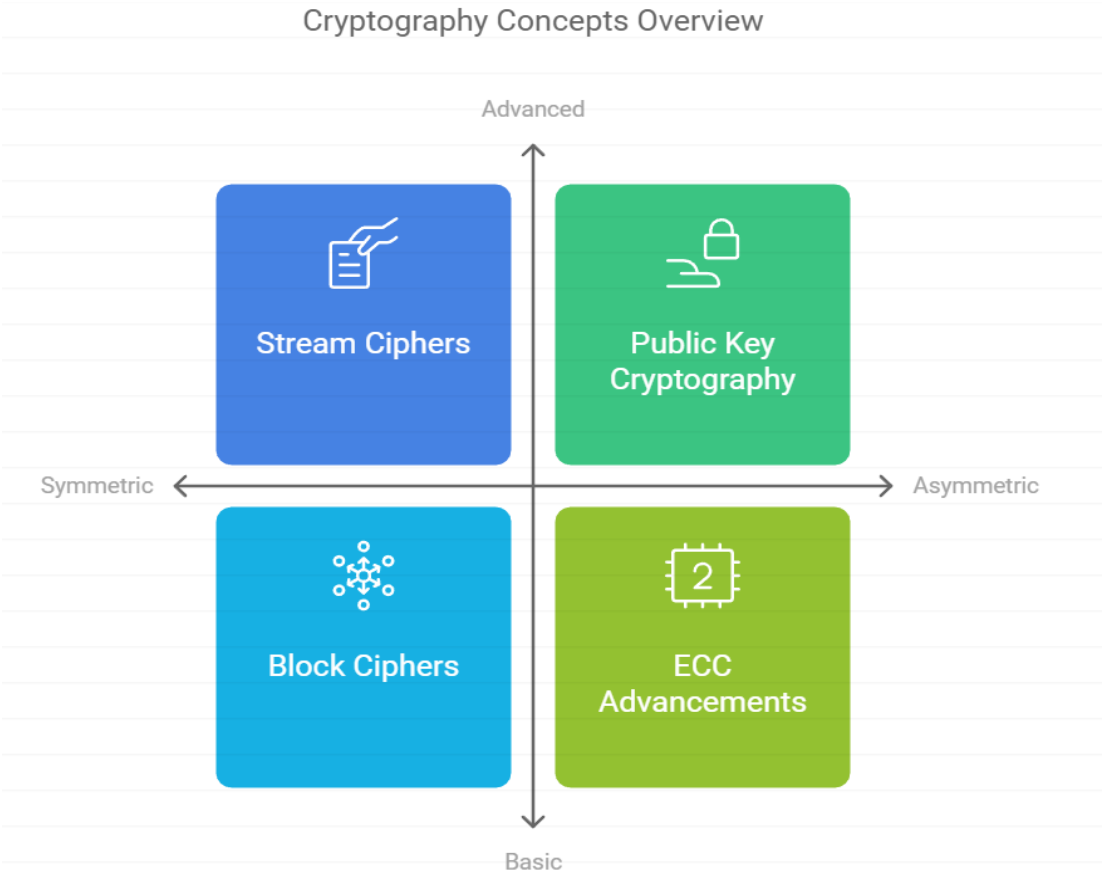

Fig. 1.1 Cryptography Concepts Overview

2. Procedure to encrypt using the Nonhomogeneous Matrix Method

Assigning numbers to each letter in the alphabet:

1	2	3	4	5	6	7	8	9
A	B	C	D	E	F	G	H	I
10	11	12	13	14	15	16	17	18
J	K	L	M	N	O	P	Q	R
19	20	21	22	23	24	25	26	0
R	T	U	V	W	X	Y	Z	Space

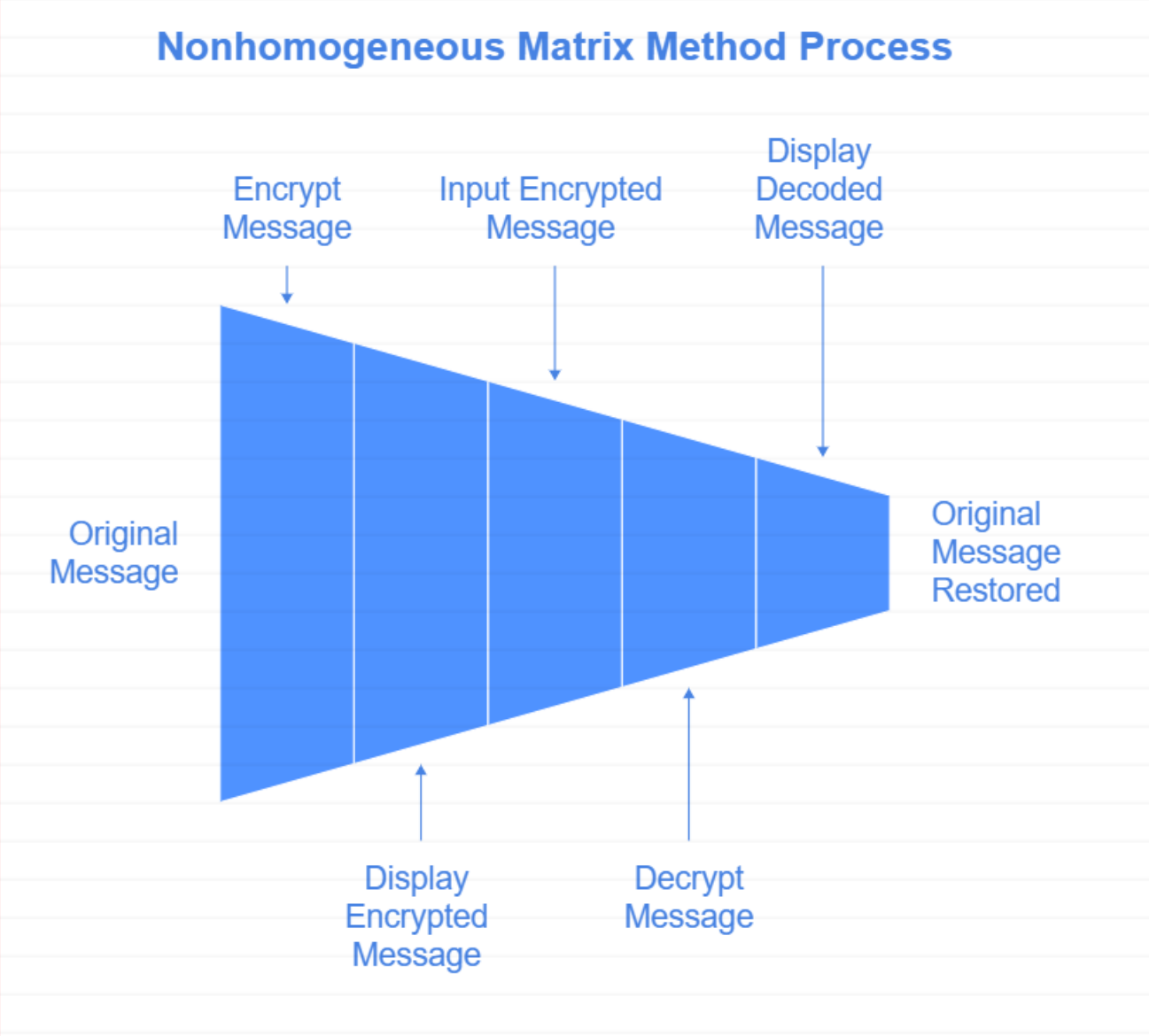

Fig. 2.1 Nonhomogenous Matrix Method Process

2.1 Matrix Encryption

Here use an Encoder as a matrix and a Decoder as its inverse matrix. For example, Let A be the encoding matrix, M be the message matrix, and X will be the encrypted matrix then,

Mathematically, the operation is

To encode X=AM

The sizes of A and M will have to be consistent.

To decode $M=A^{-1}X$

The encoding matrix A must have an inverse for this scheme to work.

Encode the message "THE EAGLE HAS LANDED"

Encoding matrix, $A=\begin{pmatrix}3&0&1&1\\1&2&5&0\\1&1&3&0\\2&0&1&1\end{pmatrix}$ (1)

Message Matrix $M=\begin{pmatrix}20&5&5&19&14\\8&1&0&0&4\\5&7&8&12&5\\0&12&1&1&4\end{pmatrix}$ (2)

Encryption –Lock

$X=AM$

$X=\begin{pmatrix}3&0&1&1\\1&2&5&0\\1&1&3&0\\2&0&1&1\end{pmatrix}\begin{pmatrix}20&5&5&19&14\\8&1&0&0&4\\5&7&8&12&5\\0&12&1&1&4\end{pmatrix}$ (3)

$X=\begin{pmatrix}65&34&24&70&51\\61&42&45&79&47\\43&27&29&55&33\\45&25&19&51&37\end{pmatrix}$ (4)

The matrix X is meaningless

2.2 Decryption –Unlock

To convert meaningless matrix to a message matrix we need an inverse matrix of A.

$A^{-1}=\begin{pmatrix}1&0&0&-1\\2&3&-5&-2\\-1&-1&2&1\\-1&1&-2&2\end{pmatrix}$ (5)

To obtain massage matrix M, multiply to meaningless matrix X by the inverse matrix A^{-1} .

i.e

$M=A^{-1}X$

$M=\begin{pmatrix}1&0&0&-1\\2&3&-5&-2\\-1&-1&2&1\\-1&1&-2&2\end{pmatrix}\begin{pmatrix}65&34&24&70&51\\61&42&45&79&47\\43&27&29&55&33\\45&25&19&51&37\end{pmatrix}$ (6)

Message Matrix $M=\begin{pmatrix} 20 & 5 & 5 & 19 & 14 \\ 8 & 1 & 0 & 0 & 4 \\ 5 & 7 & 8 & 12 & 5 \\ 0 & 12 & 1 & 1 & 4 \end{pmatrix}$ (7)

The decoded message is "The Eagle has Landed"

Conclusion

In conclusion, the research demonstrates that employing inverse matrices and non-homogeneous matrix methods can significantly enhance the security of cryptographic systems. Through effective encoding and decoding processes, this approach provides a robust framework for securing sensitive information. The application of these matrix techniques enables the development of cryptographic algorithms that are not only efficient but also resilient against unauthorized access. By harnessing the mathematical properties of inverse and non-homogeneous matrices, the study paves the way for new methodologies in cryptography, ensuring that messages remain confidential and integral throughout their transmission. As the field of cryptography continues to evolve, the insights gained from this research could prove instrumental in designing more secure communication protocols that meet the demands of modern information security.

References

1. S. M. Naser, "Cryptography: From the Ancient History to Now, Its Applications and A New Complete Numerical Model", International Journal of Mathematics and Statistics Studies, Vol.9, No.3, pp.11-30, 2021.
2. Gurdeep Singh, Prateek Kumar, Nishant Taneja, and Gurpreet Kaur, "A Research Paper on Cryptography", International Journal for Technological Research in Engineering, Volume 7, Issue 4, PP.6266-6268, December-2019.
3. Farshid Haidary Makoui and Thomas Aaron Gulliver, "Inverse matrices with applications in public-key cryptography", Intelligent Algorithms and Optimization with Applications, Volume 18: 1–10, 2024.
4. Ch. Ravi Kishore, K.Krishna Chaitanya, And P.Satish Kumar, "Public Key Cryptography With System Of Non-Homogeneous Equations", International Journal of Engineering Science and Technology, Vol. 2(10), 5432-5439, 2010.
5. Aswathi Thomas and Ebin M. Manuel, "Embedment of Montgomery Algorithm on Elliptic Curve Cryptography Over RSA Public Key Cryptography", International Conference on Emerging Trends in Engineering, Science, and Technology (ICETEST - 2015), Procedia Technology 24 (2016) 911 – 917.
6. Kishore Kumar,Sarvesh Tanwar, Shishir Kumar, " MAN–C: A masked autoencoder neural cryptography based encryption scheme for CT scan images ", MethodsX 12 (2024), Elsevier 102738.
7. Kenan Begovic, Abdulaziz Al-Ali, Qutaibah Malluhi, "Cryptographic ransomware encryption detection: Survey", Computers & Security 132 (2023) 103349.
8. B. Ranganatha Rao and B. Sujatha, "A hybrid elliptic curve cryptography (HECC) technique for fast encryption of data for public cloud security", Measurement: Sensors 29 (2023) 100870.

9. Edward Keitaro Heru, Faisal, Hady Pranoto, “File Encryption Application using Menezes-Vanstone Elliptic Curve Cryptography Based on Python”, Procedia Computer Science 227 (2023) 651–658.
10. Volodymyr Rudnytskyi, Oleksandr Korchenko, Nataliia Lada, Ruslana Ziubina, Lukasz Wieclaw, Lukasz Hamera, “Cryptographic encoding in modern symmetric and asymmetric encryption” Procedia Computer Science 207 (2022) 54–63.