Hybrid Cryptosystem using Modified Polybius and Vigenere Cipher for File Encoding in GIF

Saketh N Shet[1], Chakrapani D S[2], Sathwik SM [3], Shashank HN[4], Sanjay PS[5]
[1,3,4,5] *UG Scholars ,*[2] *Assistant professor, Computer Science and Engineering, Jawaharlal Nehru New college of Engineering, Shimoga, Karnataka, India*.

***Abstract*—In the era of rapid digital transformation, securing sensitive information from unauthorized access has become a critical challenge. Cryptographic techniques play a vital role in protecting data against potential cyber threats. This research presents a *Hybrid Cryptosystem* that combines the strengths of two classical encryption methods—the Vigenère cipher and the Polybius cipher—to create a robust, dual-layered encryption framework. The system employs unique dual keys for each cipher, supporting extended ASCII characters to ensure compatibility with modern data formats. The hybrid approach enhances cryptographic strength by combining polyalphabetic substitution and coordinate-based transposition, making it resilient against common cryptanalysis techniques like frequency analysis and brute force attacks. The research contributes to advancing cryptographic techniques by showcasing the innovative integration of classical encryption methods with modern technology.**

***Index Terms*—Polybius, Vigenère, cryptosystem, encryption, decryption**

I. INTRODUCTION

In today's digital age, the internet serves as the primary medium for transmitting data worldwide, enabling swift and efficient communication through emails, instant messaging, and other methods. However, this convenience brings significant security risks, including unauthorized access to sensitive information. Ensuring data security has become a critical priority, and cryptography plays a central role in safeguarding information during transmission.

Cryptography is the art and science of transforming plain text into an unreadable format, known as ciphertext, using encryption algorithms and keys. The original data is restored at the recipient's end through decryption. These methods not only protect confidentiality but also ensure data integrity, authentication, and non-repudiation. With technological advancements, the demand for robust encryption techniques has grown exponentially, highlighting the importance of cryptography in secure communication.

Modern cryptography can be classified into two types: symmetric and asymmetric encryption. Symmetric encryption uses a single key for both encryption and decryption, offering simplicity but posing challenges in secure key distribution. Asymmetric encryption, on the other hand, relies on a public-private key pair, where the public key is used for encryption, and the private key is used for decryption. This approach enhances security, as only the private key can unlock the encrypted data.

To address evolving security needs, this research integrates two classical cryptographic methods—the Vigenère cipher and the Polybius cipher—into a hybrid cryptosystem. The Vigenère cipher uses polyalphabetic substitution to resist frequency analysis, while the Polybius cipher encodes data through coordinate-based transposition. Together, they form a dual-layered encryption system that enhances security and supports diverse data formats.

In addition to encryption, this project incorporates multimedia encoding. The hybrid cryptosystem converts encrypted data into visual formats like images and GIFs, improving usability and portability. This innovative approach demonstrates the relevance of classical cryptography in addressing modern data security challenges while expanding its application to contemporary data formats.

II. METHODOLOGY

A. Extended Polybius Cipher:

The *Extended Polybius Cipher* is an enhanced version of the classical Polybius cipher, tailored to address the

limitations of its traditional counterpart by supporting modern encryption needs. While the original Polybius cipher operates on a 5x5 grid to encode 25 alphabetic characters, it falls short in handling the extended ASCII set, which includes alphanumeric characters, special symbols, and other data representations. The extended version expands the grid to a 16x16 matrix, accommodating all 256 characters in the extended ASCII table. This adaptation ensures compatibility with contemporary data formats, including text, binary files, and multimedia content, thus making it a versatile encryption tool.

Unlike the traditional cipher, which is limited to a fixed character mapping, the extended Polybius cipher employs a dynamic grid generation process. The grid's configuration is determined by a user-provided key, which introduces an element of randomness and uniqueness. Each character in the extended ASCII set is assigned a pair of coordinates based on its position in the grid, creating a unique mapping for every encryption session. For instance, the character 'A' might correspond to the coordinates (0,1), while a special symbol like '@' could be encoded as (3,5). This coordinate-based substitution technique ensures that the cipher is both secure and efficient.

The encryption process begins by converting plaintext characters into their corresponding coordinates in the grid. These coordinate pairs are then concatenated to form the ciphertext. Decryption reverses the process, using the same key-based grid to map the coordinates back to their original characters. The reliance on a key ensures that the encryption is highly secure, as unauthorized users cannot reconstruct the grid without access to the key. Moreover, the extended Polybius cipher's support for all ASCII characters enables it to encrypt a wide range of data types, including multilingual text and binary data, making it suitable for modern communication and storage requirements.

One of the key advantages of the extended Polybius cipher is its adaptability. The expanded grid size allows it to scale for even larger character sets, such as Unicode, by increasing the matrix dimensions. Furthermore, the use of a dual-key mechanism for grid generation adds an additional layer of security, making the cipher resistant to brute force and frequency analysis attacks. Its simplicity in design and computational efficiency makes it a practical choice for resource-constrained environments, while its ability to encode non-textual data extends its application to domains such as secure file storage and multimedia encryption.

The extended Polybius cipher, with its robust and adaptable encryption capabilities, forms a crucial component of the hybrid cryptosystem. Its integration into the system ensures secure and efficient encoding of modern data formats, contributing significantly to the overall resilience and versatility of the proposed encryption framework.

B. Extended Vigenère Cipher:

The *Extended Vigenère Cipher* is an advanced adaptation of the classical Vigenère cipher, designed to address the limitations of the traditional cipher by expanding its functionality to support modern data formats and extended character sets. While the classical Vigenère cipher is a polyalphabetic substitution cipher that operates on the basic English alphabet, the extended version goes beyond this constraint by incorporating the *extended ASCII character set*, which includes symbols, numbers, and special characters. This enhancement makes the cipher suitable for encrypting a wide range of data, including multilingual text, binary files, and multimedia content.

In the extended Vigenère cipher, the encryption process is driven by a user-provided key, which determines the substitution pattern for each character in the plaintext. Unlike the traditional cipher, which cycles through a fixed alphabet, the extended version maps characters using a 256-character table, encompassing the entire extended ASCII set. This table is a shiftable substitution table where each row represents a cyclic permutation of the extended ASCII characters. Each character in the plaintext is matched with a corresponding character from the key, and their ASCII values are combined using modular arithmetic to determine the ciphertext character. This method ensures that the ciphertext is both non-repetitive and resilient to frequency analysis attacks.

The decryption process is the inverse of encryption, where the ciphertext is transformed back into plaintext using the same key. The modular arithmetic operation is reversed to reconstruct the original characters. This reliance on the key ensures that the encryption is highly secure, as the same key is required for both encryption and decryption. Additionally, the extended ASCII compatibility allows the cipher to encrypt and decrypt non-English characters and binary data,

making it a versatile encryption technique for modern data formats.

The extended Vigenère cipher introduces significant enhancements over the classical version, particularly in terms of security and adaptability. The key length, which can be variable and as long as the plaintext, provides a high degree of resistance against brute force and cryptanalysis attacks. By supporting extended ASCII characters, the cipher eliminates the limitation of fixed alphabets and ensures compatibility with diverse data formats. Moreover, the cipher's simplicity in implementation and computational efficiency makes it suitable for practical applications in secure communication and data storage.

When integrated into a hybrid cryptosystem, the extended Vigenère cipher serves as a robust layer of encryption that complements other cryptographic techniques, such as the extended Polybius cipher. Its ability to perform polyalphabetic substitution on a wide range of character sets significantly enhances the overall strength of the encryption framework. This adaptability ensures that the cipher remains relevant in addressing the challenges of modern cryptographic needs, making it a crucial component in securing sensitive information in today's digital landscape.

III. WORKFLOW

This research proposes a hybrid cryptosystem that integrates the Vigenère cipher and Polybius cipher to achieve secure data encryption and encoding. The methodology consists of multiple stages to process, encrypt, encode, decode, and decrypt data. The following steps outline the detailed workflow:

A. Encoding and Encryption Workflow

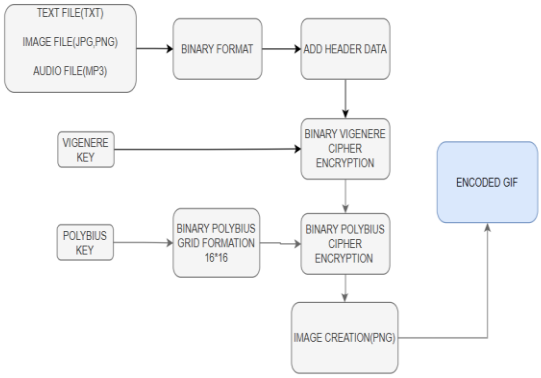

Fig -1: Encoding Workflow

Data Preparation: The system accepts various file formats:

- Text Files: .txt
- Image Files: .jpg, .png
- Audio Files: .mp3

The input file is first converted into its binary format, ensuring a standardized representation for cryptographic processing. This step prepares the data for encryption while maintaining compatibility across different file types.

Header Data Embedding: A header is appended to the binary data to include essential metadata, such as:

- File type
- File size

This metadata is critical for correctly reconstructing the original file during decryption and decoding.

Vigenère Cipher Encryption: The binary data is encrypted using the Vigenère cipher, which employs:

- A user-provided Vigenère key.
- Extended ASCII character support for compatibility with diverse data types.

This stage introduces the first layer of encryption, protecting the data from unauthorized access.

Polybius Cipher Encryption: The output from the Vigenère encryption is subjected to Polybius cipher encryption, which uses:

- A custom 16x16 Polybius grid to support extended ASCII characters.
- A user-provided Polybius key to generate the grid.
- This second encryption layer adds an additional level of security, enhancing the system's robustness against cryptanalysis.

Intermediate Image Creation: The doubly encrypted binary data is converted into an image in .png format. This visual representation serves as an intermediate step, making the encrypted data storable and portable.

GIF Encoding: The .png image is encoded into a GIF file, completing the encryption and encoding process. The user can specify the resolution of the GIF (e.g., 4K) based on their requirements. This step ensures the encrypted data is securely encapsulated in a visually storable format.

B. Decoding and Decryption Workflow:

The system provides a reverse workflow to decode and decrypt the data:

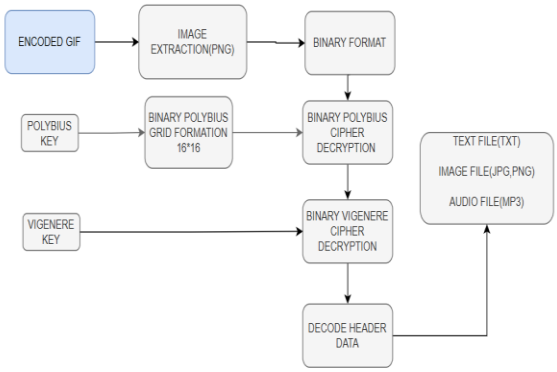

Fig -2: Decoding Workflow

GIF Decoding: The encoded GIF file is processed to extract the embedded .png image. This image contains the doubly encrypted binary data.

Polybius Cipher Decryption: The binary data extracted from the image is decrypted using the Polybius cipher, reconstructing the Vigenère-encrypted binary data. The decryption relies on the user-provided Polybius key.

Vigenère Cipher Decryption: The output from the Polybius decryption is decrypted using the Vigenère cipher, with the Vigenère key provided by the user. This step retrieves the original binary data.

Header Data Decoding: The header data is parsed to extract the metadata, enabling the system to reconstruct the original file in its correct format (.txt, .jpg, .mp3, etc.).

File Reconstruction: The binary data is converted back into the original file, completing the decryption and decoding process. The result is a fully restored version of the input data.

The proposed hybrid encryption system combines the strengths of the Vigenère and Polybius ciphers to create a robust dual-layered encryption mechanism. By leveraging the Vigenère cipher's variable key length and the Polybius cipher's grid-based substitution, the system ensures enhanced data security. Additionally, the system supports extended ASCII characters, making it compatible with a wide range of file formats and character sets. To further enhance usability and portability, the encrypted data is encoded into a GIF format, which not only provides a visually representable medium but also makes the data storable and easily transferable. The inclusion of a dual-key system, requiring independent keys for both Vigenère and Polybius ciphers, adds another layer of security, reducing vulnerabilities to cryptographic attacks. Moreover, the system offers flexibility and scalability by allowing users to specify the resolution of the GIF file, catering to varying storage, quality, and performance requirements. This integration of classical cryptographic methods with modern encoding techniques establishes a secure and versatile framework for data protection.

This methodology demonstrates an innovative approach to secure data transmission by integrating classical encryption methods with modern encoding techniques, ensuring high levels of data security and usability.

IV. RESULTS

After implementing the hybrid cryptosystem combining the Polybius Cipher and Vigenère Cipher for secure data encryption and decryption, the final step was to develop a simple and interactive user interface to facilitate user interaction with the system. A user-friendly web application was built using Streamlit for the frontend, styled with custom CSS, providing a responsive and visually appealing design. The backend was implemented in Python, ensuring smooth integration with the encryption and decryption algorithms, and allowing real-time processing of user inputs.

Fig -3: Image into Encoded Gif

The Figure 3 demonstrates the encoding process of a file into a GIF using the hybrid cryptosystem. The user begins by uploading a file, named "image.png," with a size of 448.8 KB. The application offers an option to

select the resolution of the GIF output, and in this instance, the resolution "4K (3840x2160)" is chosen. To secure the data, the user provides two keys: a Vigenère Cipher key (key890-= [) and a Polybius Cipher key (secret-=#$). After entering these keys, the "Encode" button is clicked to process the file. The system applies the dual-layer encryption using the specified keys and embeds the encrypted data into a high-resolution GIF. This process highlights the application's ability to securely handle and encode diverse file types into multimedia formats with enhanced protection.

"Encode" button is clicked to process the file. The system applies the dual-layer encryption using the specified keys and embeds the encrypted data into a high-resolution GIF. This process highlights the application's ability to securely handle and encode diverse file types into multimedia formats with enhanced protection.

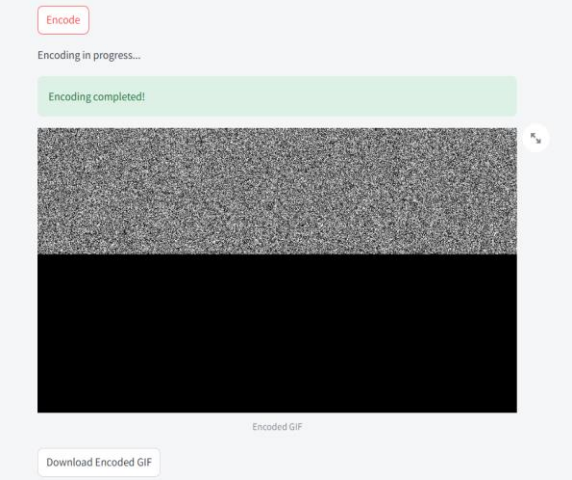

Fig -4 Encoded Gif

The figure 4 illustrates the successful completion of encoding a file into a GIF format using the hybrid cryptosystem. During the encoding process, the progress status is displayed, followed by a confirmation message, "Encoding completed!" The resulting encoded GIF is presented, showcasing a randomized or encrypted pattern that visually represents the embedded and secured data. Below the encoded GIF, the system provides an option to download the file through a "Download Encoded GIF" button. This step confirms the system's ability to securely encode sensitive data into a multimedia format, ensuring its confidentiality and integrity.

V. CONCLUSION

This research presents a robust and innovative hybrid encryption system that integrates the classical Vigenère and Polybius ciphers with modern encoding techniques. By employing a dual-layered encryption approach, the system significantly enhances data security, ensuring confidentiality and integrity. The inclusion of extended ASCII support expands compatibility across diverse file formats and character sets, addressing the challenges posed by modern data environments. Encoding the encrypted output into a GIF format provides a novel, portable, and visually representable medium for storing and transferring data. Furthermore, the dual-key mechanism adds a critical layer of security, making unauthorized decryption highly complex. The system's flexibility and scalability, through user-defined GIF resolutions, cater to varying performance and storage requirements, making it adaptable for a range of applications.

In conclusion, this hybrid cryptosystem demonstrates the potential of combining classical cryptographic methods with contemporary data encoding techniques, paving the way for secure and efficient data protection solutions in today's digital landscape. Future work may explore further optimizations and the inclusion of additional file formats to broaden its applicability.

REFERENCES

[1] Fairouz Mushtaq Sher Ali, Falah Hassan Sarhan, "Enhancing Security of Vigenere Cipher by Stream Cipher. "International Journal of Research in Engineering and Technology, 2013, Vol. 02 Issue 09.

[2] Shivam Vatshayan, Raza Abbas Haidri, Jitendra Kumar Verma, "Development of a hybrid cryptography system combining Vigenère and Polybius ciphers.," 2020 International Conference on Computational Performance Evaluation (ComPE), IEEE.

[3] A. A. Soofi, I. Riaz, and U. Rasheed, "An enhanced Vigenere cipher for data security," Int. J. Sci. Technol. Res, vol. 5, no. 3, pp. 141–145, 2016.4. Michalewicz, Z.: Genetic Algorithms + Data Structures = Evolution Programs. 3rd edn. Springer-Verlag, Berlin Heidelberg New York (1996).

[4] P. Kumar and S. B. Rana, “Design of Hybrid Cryptography System Based on Vigenère Cipher and Polybius Cipher,” Optik, vol. 127, no. 4, pp. 2341–2345, 2016.

[5] Aditi Saraswat, Chahat Khatri, Sudhakara, Prateek Thakrala, Prantik Biswas, “An extended hybridization of vigenere and caesar cipher techniques for secure communication,” Proceedings of the 2nd International Conference on Intelligent Computing, Communication & Convergence (ICCC-2016).