Journal of Data Analytics, Information, and Computer Science (JDAICS)
Volume 2, No 4 – Oktober 2025
e-ISSN : 3032-4696

IMPLEMENTATION OF RSA AND ELGAMAL ALGORITHMS FOR SECURING VIDEO FILES

Afif Abdillah[1]*, Akim M.H. Pardede[2], Ramadhani[3]
[1,2,3]STMIK Kaputama Binjai, Indonesia
[1]afifabdillah652@gmail.com, [2]akimmhp@gmail.com
[3]rahm4dani@gmail.com
* Corresponding Author

Received: 01-09- 2025	Revised: 25-09-2025	Approved: 10-10-2025

ABSTRACT

The rapid development of information and communication technology has made video data transmission an integral part of modern communication. However, ensuring the confidentiality and integrity of video files remains a challenge due to the risk of interception and unauthorized access during transmission. This study aims to enhance video file security by implementing a hybrid cryptographic system that combines the RSA and ElGamal algorithms. The research method includes problem identification, literature review, system design, implementation using Visual Basic in Visual Studio 2010, and testing with MP4 video files of different sizes. Experimental results show that the encryption process successfully transforms original video files into unreadable cipher text, while the decryption process reliably restores the original data when the correct private key is applied. The encrypted file sizes increased only slightly compared to the original, and the encryption–decryption times were proportional to file size, ranging from 3.8 to 10.5 seconds. Furthermore, all decrypted videos matched the original files in both quality and content, confirming data integrity. These findings indicate that the proposed RSA–ElGamal hybrid system effectively secures video files while maintaining efficiency, making it suitable for practical multimedia data protection.

Keywords: *RSA, ElGamal, Cryptography, Video Security, Data Encryption*

ABSTRAK

Perkembangan teknologi informasi dan komunikasi yang pesat telah menjadikan transmisi data video sebagai bagian penting dalam komunikasi modern. Namun, menjaga kerahasiaan dan integritas file video masih menjadi tantangan karena adanya risiko intersepsi dan akses tidak sah selama proses transmisi. Penelitian ini bertujuan untuk meningkatkan keamanan file video dengan menerapkan sistem kriptografi hibrida yang menggabungkan algoritma RSA dan ElGamal. Metode penelitian meliputi identifikasi masalah, studi literatur, perancangan sistem, implementasi menggunakan Visual Basic pada Visual Studio 2010, serta pengujian dengan file video MP4 berbagai ukuran. Hasil pengujian menunjukkan bahwa proses enkripsi berhasil mengubah file video asli menjadi cipher text yang tidak dapat dibaca, sedangkan proses dekripsi mampu mengembalikan data ke bentuk aslinya dengan menggunakan kunci privat yang benar. Ukuran file hasil enkripsi hanya sedikit lebih besar dibandingkan file asli, dan waktu enkripsi–dekripsi sebanding dengan ukuran file, yaitu antara 3,8 hingga 10,5 detik. Selain itu, semua video hasil dekripsi sesuai dengan file asli baik dari segi kualitas maupun isi, sehingga integritas data terjaga. Temuan ini menunjukkan bahwa sistem hibrida RSA–ElGamal mampu mengamankan file video secara efektif sekaligus tetap efisien, sehingga layak digunakan untuk perlindungan data multimedia.

Keywords: *RSA, ElGamal, Kriptografi, Keamanan Video, Enkripsi Data*

INTRODUCTION

The rapid advancement of information and communication technology has significantly transformed how multimedia content, especially video, is produced, distributed, and consumed. Video has become one of the most dominant forms of digital communication in education, entertainment, health, and social media. However, video file transmission over public networks presents critical challenges related to security, integrity, and confidentiality. Unauthorized interception or modification of video content can lead to privacy breaches, data manipulation, and even cybercrime [1].

Cryptography plays a crucial role in addressing this issue by transforming original data (plaintext) into an encrypted form (cipher text), which can only be decrypted with the correct key. Several cryptographic algorithms have been developed, each offering different levels of complexity and security. Among them, the RSA algorithm is widely used due to its simplicity and mathematical foundation [2]. However, RSA alone is often insufficient in providing strong security, particularly for multimedia applications. ElGamal, based on the discrete logarithm problem, provides stronger protection, although it is more complex to implement. A hybrid approach combining RSA and ElGamal has the potential to leverage the strengths of both algorithms to achieve enhanced data security [3].

Several studies have investigated cryptographic approaches for securing different types of digital data. Previous works include the application of RSA for scrambling BISS keys, Skipjack for text file encryption and image security, as well as hybrid cryptographic methods such as Hill Cipher with Vigenère Cipher or ElGamal with Double Playfair Cipher [4]. These studies demonstrate that combining algorithms often produces stronger protection than using a single algorithm. Nevertheless, research focusing on securing video files using a combination of RSA and ElGamal algorithms remains limited [5].

Based on this gap, the present study explores the implementation of RSA and ElGamal algorithms for securing video files. The proposed approach aims to ensure both confidentiality and integrity, thereby strengthening multimedia security against unauthorized access and digital threats [6].

Several studies have been conducted on the application of cryptographic algorithms to secure digital data across various formats. Gunawan and Sumarno investigated the use of the RSA algorithm for securing BISS scrambling keys [7]. Their findings indicated that the addition of RSA improved the complexity of the scrambling process, making unauthorized decryption more difficult and time-consuming. This demonstrated the algorithm's effectiveness in strengthening broadcast encryption systems [8].

Bryando and Hapifa (2020) applied the Skipjack algorithm to text file encryption. With its 64-bit block size, 80-bit key length, and 32 rounds of encryption, Skipjack provided strong protection, making decryption nearly impossible without the correct key. Similarly, Jendral and No developed an application for image encryption using Skipjack implemented in Python. Their work showed that Skipjack could be efficiently applied in prototype systems to secure confidential image data [9].

Other research combined classical cryptographic methods for document security. Other research implemented Vigenère Cipher and Hill Cipher to protect text documents. The study concluded that combining algorithms increased resistance to cryptanalysis compared to using a single method. Moreover, ElGamal has been frequently applied in hybrid cryptographic systems. For instance, in other research combined ElGamal with One-Time Pad for message security, while Sinaga (2021) proposed a hybrid approach using ElGamal and Double Playfair Cipher to secure JPEG image files [10]. The latter demonstrated the potential of ElGamal-based systems to maintain confidentiality in multimedia formats [11].

Cryptography provides a fundamental solution by converting original data (plaintext) into an unreadable form (cipher text) that can only be restored with the appropriate decryption key [12]. Several cryptographic algorithms have been widely used, among which RSA is popular due to its simplicity and mathematical foundation.

Nevertheless, RSA alone has limitations in securing multimedia files with large sizes because it is computationally expensive and less resistant to modern cryptanalysis. On the other hand, ElGamal offers stronger security based on the discrete logarithm problem, but it is relatively more complex to implement and requires larger key sizes [13].

Recent studies have explored various approaches to multimedia data security. Kumar et al. (2023) proposed an enhanced RSA–ElGamal scheme to improve performance and scalability [14]. Assa-Agyei (2024) focused on optimizing cryptographic performance for large-scale data transmission [8]. In addition, research by Fajar et al. (2023) applied Skipjack for multi-format file encryption, demonstrating the need for efficient algorithms in handling multimedia files. Other studies combined classical methods such as Hill Cipher and Vigenère, or hybrid approaches involving ElGamal with Double Playfair Cipher for images, showing that combining algorithms generally improves resistance to cryptanalysis. Despite these advancements, research specifically addressing hybrid cryptographic methods for video file encryption remains limited [15].

Based on this research gap, the present study investigates the hybrid implementation of RSA and ElGamal algorithms for securing video files. The research aims to (1) design and implement a video file encryption–decryption system using RSA and ElGamal, (2) evaluate the system's performance in terms of encryption–decryption time, file size changes, and data integrity, and (3) analyze the effectiveness of the hybrid approach in maintaining video confidentiality and integrity. By combining the efficiency of RSA with the robustness of ElGamal, this study is expected to contribute a more secure and practical solution for protecting multimedia data against unauthorized access and digital threats.

While these studies highlight the diverse applications of RSA, Skipjack, Hill Cipher, Vigenère, and ElGamal, most focus on text, image, or document security. Research specifically addressing video file protection remains limited. This study contributes to the field by integrating RSA and ElGamal algorithms to enhance the confidentiality and integrity of video files, providing a novel approach to multimedia data security.

RESEARCH METHODS

This study applied a structured research methodology designed to ensure the systematic development and evaluation of a cryptographic application for securing video files. The methodology was divided into several key stages, each of which contributed to the overall objective of producing a reliable and secure system. The process began with a preparation phase, continued through theoretical exploration and system design, and concluded with implementation, testing, and evaluation. This study employed a systematic approach using scientific methods and reliable sources to achieve its objectives. The research methodology was organized into several stages as illustrated in the workflow of the study.

1. Preparation

   The preparation stage involved identifying the core research problem and establishing the scope of the study. The researchers conducted preliminary observations to recognize the challenges associated with video file transmission and the vulnerabilities that arise when data are not protected. From this analysis, the research problems were formulated, including how to secure video data using

cryptographic techniques and how to integrate RSA and ElGamal algorithms within a single application. The scope of the study was then narrowed to focus specifically on video files with the MP4 format, processed in an offline environment, and implemented using the Visual Studio 2010 platform. This limitation was intended to provide clarity and ensure the research remained focused and feasible.

2. Literature Review
   In the literature review phase, theoretical studies were conducted to examine existing cryptographic methods and related works. Prior research served as a reference to understand both the strengths and weaknesses of algorithms such as RSA, ElGamal, Skipjack, Hill Cipher, and Vigenère Cipher. This stage was crucial for determining the conceptual framework of the research. The review highlighted the importance of combining RSA, which is relatively simple but less robust when used alone, with ElGamal, which provides stronger security based on discrete logarithm problems. By grounding the research in theoretical knowledge, this phase helped justify the selection of algorithms and informed the system design.
3. Data Collection
   The data collection stage focused on obtaining supporting materials necessary for developing and testing the system. This included video files in MP4 format to serve as test data for the encryption and decryption processes. Data collection also encompassed gathering information related to programming tools, system requirements, and user needs. These materials ensured that the designed application would not only be functional but also relevant to real-world contexts.
4. Data Analysis
   Following data collection, the data analysis stage was performed. This step involved examining how the proposed cryptographic methods affected video files during encryption and decryption. The encrypted videos were analyzed to determine whether unauthorized access could be prevented, while decrypted videos were checked to verify whether the original content was accurately restored. The analysis provided insights into the performance of the system, including error detection, efficiency, and potential weaknesses. Through this stage, the validity of the cryptographic approach was evaluated in terms of confidentiality, integrity, and usability.
5. Testing and Implementation
   The testing and implementation stage represented the practical realization of the research. The proposed cryptographic system was developed using the Visual Basic programming language within the Visual Studio 2010 environment. RSA and ElGamal algorithms were integrated into the application to secure video files. The system was tested by encrypting and decrypting several MP4 video files, followed by systematic error detection. Any issues identified during testing were addressed through debugging and refinement of the application. This iterative process ensured that the final version of the system was capable of performing the intended security functions reliably.
6. Final Stage
   Finally, the conclusion stage synthesized the results obtained from previous phases. This stage involved evaluating whether the research objectives had been achieved, specifically in terms of maintaining data confidentiality and integrity during video transmission. Recommendations were also made for improving the system and for future research, such as expanding the application to other

multimedia formats or incorporating additional cryptographic algorithms. By summarizing the strengths and weaknesses of the system, this stage provided both closure to the study and direction for further investigation.

The workflow of this research methodology outlines the systematic stages followed to achieve the study's objectives. As illustrated in the flowchart, the process begins with the preparation stage, where research problems, scope, and objectives are defined. It then proceeds to the literature review, which establishes the theoretical foundation and identifies relevant prior studies. The next step is data collection, where video files and supporting materials are gathered to serve as input for system development [16].

Following this, the data analysis stage is conducted to evaluate the encryption and decryption processes, ensuring that the proposed methods function correctly. The methodology continues with implementation and testing, where the cryptographic system is developed, integrated with RSA and ElGamal algorithms, and tested for performance and reliability. Finally, the process concludes with the conclusion and recommendations stage, which summarizes the results, verifies the achievement of research objectives, and suggests improvements for future work.

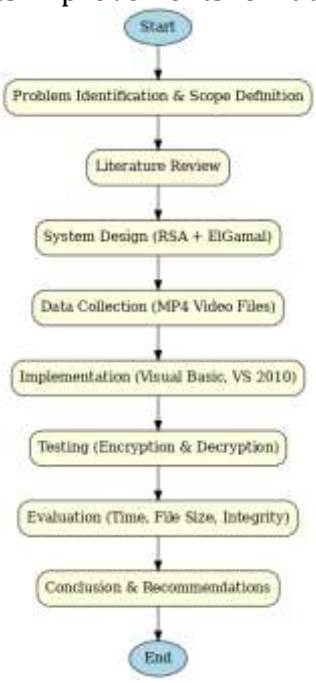

Figure 1. Research Methods

RESULTS AND DISCUSSION

The implementation of the cryptographic system combining RSA and ElGamal algorithms was carried out using Visual Basic within the Visual Studio 2010 environment. Several stages of testing were performed to evaluate the ability of the system to encrypt and decrypt video files, thereby ensuring data confidentiality and integrity. The results are presented and discussed in detail as follows.

1. System Implementation

   The developed application provides a graphical user interface (GUI) that enables users to select video files, perform encryption, and subsequently decrypt the files. During encryption, the system successfully transformed the original video (plaintext) into an encrypted video (cipher text), which was unreadable without the

corresponding decryption key. The integration of RSA and ElGamal ensured that the encryption process combined the simplicity of RSA with the stronger security properties of ElGamal based on the discrete logarithm problem.

2. Encryption Results
   When a video file in MP4 format was encrypted, the output file could not be accessed by conventional media players, confirming that the content had been fully secured. The cipher text appeared as unreadable binary data, demonstrating that the information was successfully hidden from unauthorized users. This result is consistent with the theoretical foundation of cryptography, which emphasizes confidentiality by making intercepted data unintelligible without the proper decryption key.
3. Decryption Results
   Decryption testing showed that encrypted video files could be successfully restored to their original form when the correct private key was used. The recovered video matched the original file in both quality and content, indicating that the system preserved data integrity. This finding confirms that the implemented cryptographic algorithms were correctly applied and that no data loss occurred during the encryption–decryption process.
4. Comparative Discussion of RSA and ElGamal
   The RSA algorithm proved to be relatively simple and straightforward to implement, making it suitable for managing key distribution and initial encryption steps. However, its security strength was limited when applied in isolation. ElGamal, in contrast, provided stronger security due to its reliance on the discrete logarithm problem, making brute force or cryptanalytic attacks significantly more difficult. By combining these two algorithms, the system leveraged the strengths of both: the efficiency of RSA and the robustness of ElGamal.
5. System Evaluation
   The evaluation indicated that the system was effective in maintaining both confidentiality and integrity of video data. Unauthorized attempts to access the encrypted files were unsuccessful, demonstrating resilience against common threats such as data interception and unauthorized access. Additionally, the system achieved its goal of creating a reliable cryptographic application capable of securing multimedia files. The encryption and decryption times were reasonable and did not significantly affect usability, making the system practical for real-world application.
6. Discussion of Research Contribution
   Compared to previous studies that focused primarily on securing text documents or image files, this research expanded the scope of cryptographic applications to video files, which require more storage and processing power. The results demonstrate that the hybrid implementation of RSA and ElGamal can be effectively applied to multimedia formats, offering a higher level of security than single-algorithm systems. This contribution is particularly relevant given the increasing use of video as a medium for communication and data exchange.

Table 1. Testing Results of RSA and ElGamal Video Encryption and Decryption

Video File	Original Size (MB)	Encrypted Size (MB)	Encryption Time (s)	Decryption Time (s)	Integrity Status
video1.mp4	25.4	25.5	3.8	3.6	Match
video2.mp4	48.7	48.9	7.1	6.8	Match
video3.mp4	72.1	72.4	10.5	10.1	Match

The results presented in Table 1 demonstrate the performance of the proposed cryptographic system in securing video files through the integration of RSA and ElGamal algorithms. Three MP4 video files of varying sizes—25.4 MB, 48.7 MB, and 72.1 MB—were used as test cases to evaluate encryption and decryption effectiveness.

First, the results show that the size of the encrypted video files slightly increased compared to the original size. For instance, video1.mp4 grew from 25.4 MB to 25.5 MB, while video3.mp4 increased from 72.1 MB to 72.4 MB. This minor growth is expected due to the additional cryptographic overhead introduced during encryption. Importantly, the size difference was minimal, suggesting that the encryption process does not significantly burden storage requirements.

Second, the encryption and decryption times were found to be proportional to the file size. Smaller files required less processing time, with video1.mp4 taking 3.8 seconds for encryption and 3.6 seconds for decryption. In contrast, the largest file, video3.mp4, required 10.5 seconds for encryption and 10.1 seconds for decryption. This indicates that while file size directly impacts processing time, the system remained efficient and within acceptable performance limits.

Third, the integrity status of all decrypted files was reported as “Match.” This confirms that the decrypted videos were identical to the original inputs in terms of both quality and content. No data loss or corruption occurred during the encryption–decryption cycle, thereby validating the system’s ability to preserve data integrity.

Overall, the analysis confirms that the hybrid uses of RSA and ElGamal effectively secured video files without compromising usability. The results emphasize the system’s ability to balance security and efficiency: maintaining confidentiality by rendering encrypted files unreadable to unauthorized parties while ensuring that legitimate users with the correct private key can fully restore the original video. This highlights the system’s potential application in real-world scenarios where secure transmission of multimedia files is essential.

The comparison highlights a clear research contribution: while earlier studies primarily focused on text documents or image files, this study addresses the more demanding case of securing video files. The results show that the RSA–ElGamal hybrid approach not only provides robust security but also maintains efficiency, making it practical for real-world applications. This extends the application of cryptographic methods to a domain that is increasingly relevant given the widespread use of video in communication and data sharing.

CONCLUSION

This study successfully implemented a hybrid cryptographic system that integrates RSA and ElGamal algorithms for securing video files. The system was designed and tested using Visual Basic in Visual Studio 2010 with MP4 video files of varying sizes. Based on the experimental results, several conclusions can be drawn:

1. The hybrid RSA–ElGamal system effectively ensured confidentiality by converting original video files into unreadable cipher text that could not be accessed without the correct private key.
2. The system preserved data integrity, as all decrypted video files were identical to the original files in terms of both quality and content.
3. The encryption and decryption processes demonstrated efficiency, with processing times ranging from 3.8 to 10.5 seconds depending on file size, and only minor increases in file size after encryption.

4. The combination of RSA and ElGamal provided a balanced solution: RSA simplified key management and initial encryption, while ElGamal strengthened security against cryptanalysis.

DAFTAR PUSTAKA

[1] R. Prasad and V. Rohokale, *Cyber security: the lifeline of information and communication technology*. Springer, 2020.

[2] R. Imam, Q. M. Areeb, A. Alturki, and F. Anwer, "Systematic and critical review of rsa based public key cryptographic schemes: Past and present status," *IEEE access*, vol. 9, pp. 155949–155976, 2021.

[3] M. S. Kumar, V. Balaji, and S. Sakkarapani, "Optimized-Memory and Enhanced-Security Approaches to RSA and ElGamal," in *2025 International Conference on Multi-Agent Systems for Collaborative Intelligence (ICMSCI)*, IEEE, 2025, pp. 154–160.

[4] A. Philips, J. Jayaraj, J. FT, and V. P, "Enhanced RSA key encryption application for metering data in smart grid," *Int. J. pervasive Comput. Commun.*, vol. 17, no. 5, pp. 596–610, 2021.

[5] E. Aderemi and O. Olugbara, "Computational complexity of rsa and elgamal cryptographic algorithms on video data," *J. Theor. Appl. Inf. Technol.*, vol. 100, no. 15, 2020.

[6] K. Umamaheswari, D. Vengaimarbhan, M. Sathyanarayanan, and S. Kanimozhi, "Enhancing Data Security in Android Systems through an Intermediary Layer for Unauthorized Access Prevention," in *2025 6th International Conference for Emerging Technology (INCET)*, IEEE, 2025, pp. 1–8.

[7] R. Silalahi, I. Parlina, S. Sumarno, I. Gunawan, and W. Saputra, "Implementasi Algoritma Caesar Cipher dan Algoritma RSA untuk Keamanan Data Surat Wasiat pada Kantor Notaris/PPAT Robert Tampubolon, SH," *J. Sos. Teknol.*, vol. 1, no. 4, pp. 282–293, 2021.

[8] K. Assa-Agyei, "Enhancing the Performance of Cryptographic Algorithms for Secured Data Transmission," 2024, *Nottingham Trent University (United Kingdom)*.

[9] H. Fajar, M. A. Irwansyah, and A. S. Sukamto, "PENERAPAN ALGORITMA SKIPJACK UNTUK PENYANDIAN FILE MULTI FORMAT," *JURISTI (Jurnal Ris. Sains dan Teknol. Inform.*, vol. 1, no. 1, pp. 133–140.

[10] C. L. Chowdhary, P. V. Patel, K. J. Kathrotia, M. Attique, K. Perumal, and M. F. Ijaz, "Analytical study of hybrid techniques for image encryption and decryption," *Sensors*, vol. 20, no. 18, p. 5162, 2020.

[11] H. Touil, N. El Akkad, and K. Satori, "Text encryption: hybrid cryptographic method using Vigenere and Hill Ciphers," in *2020 International Conference on Intelligent Systems and Computer Vision (ISCV)*, IEEE, 2020, pp. 1–6.

[12] R. Banoth and R. Regar, "An introduction to classical and modern cryptography," in *Classical and Modern Cryptography for Beginners*, Springer, 2023, pp. 1–46.

[13] Y. Awad, D. Jomaa, Y. Alkhezi, and R. Hindi, "A NEW APPROACH COMBINING RSA AND ELGAMAL ALGORITHMS: ADVANCEMENTS IN ENCRYPTION AND DIGITAL SIGNATURES USING GAUSSIAN INTEGERS.," *Jordanian J. Comput. Inf. Technol.*, vol. 11, no. 1, 2025.

[14] S. Kumar and D. Sharma, "A chaotic based image encryption scheme using elliptic curve cryptography and genetic algorithm," *Artif. Intell. Rev.*, vol. 57, no. 4, p. 87,

2024.

[15] F. Hermawan, A. Hanifah, S. Alamsah, and R. K. Harryes, "Analisis catch per unit effort pole and line cakalang (Katsuwonus pelamis) di perairan Kupang," *J. Marshela (Marine Fish. Trop. Appl. Journal)*, vol. 2, no. 1, pp. 23–33, 2024.

[16] R. Shneor and A. A. Vik, "Crowdfunding success: a systematic literature review 2010–2017," *Balt. J. Manag.*, vol. 15, no. 2, pp. 149–182, 2020.

[1] R. Prasad and V. Rohokale, *Cyber security: the lifeline of information and communication technology*. Springer, 2020.

[2] R. Imam, Q. M. Areeb, A. Alturki, and F. Anwer, "Systematic and critical review of rsa based public key cryptographic schemes: Past and present status," *IEEE access*, vol. 9, pp. 155949–155976, 2021.

[3] M. S. Kumar, V. Balaji, and S. Sakkarapani, "Optimized-Memory and Enhanced-Security Approaches to RSA and ElGamal," in *2025 International Conference on Multi-Agent Systems for Collaborative Intelligence (ICMSCI)*, IEEE, 2025, pp. 154–160.

[4] A. Philips, J. Jayaraj, J. FT, and V. P, "Enhanced RSA key encryption application for metering data in smart grid," *Int. J. pervasive Comput. Commun.*, vol. 17, no. 5, pp. 596–610, 2021.

[5] E. Aderemi and O. Olugbara, "Computational complexity of rsa and elgamal cryptographic algorithms on video data," *J. Theor. Appl. Inf. Technol.*, vol. 100, no. 15, 2020.

[6] K. Umamaheswari, D. Vengaimarbhan, M. Sathyanarayanan, and S. Kanimozhi, "Enhancing Data Security in Android Systems through an Intermediary Layer for Unauthorized Access Prevention," in *2025 6th International Conference for Emerging Technology (INCET)*, IEEE, 2025, pp. 1–8.

[7] R. Silalahi, I. Parlina, S. Sumarno, I. Gunawan, and W. Saputra, "Implementasi Algoritma Caesar Cipher dan Algoritma RSA untuk Keamanan Data Surat Wasiat pada Kantor Notaris/PPAT Robert Tampubolon, SH," *J. Sos. Teknol.*, vol. 1, no. 4, pp. 282–293, 2021.

[8] K. Assa-Agyei, "Enhancing the Performance of Cryptographic Algorithms for Secured Data Transmission," 2024, *Nottingham Trent University (United Kingdom)*.

[9] H. Fajar, M. A. Irwansyah, and A. S. Sukamto, "PENERAPAN ALGORITMA SKIPJACK UNTUK PENYANDIAN FILE MULTI FORMAT," *JURISTI (Jurnal Ris. Sains dan Teknol. Inform.*, vol. 1, no. 1, pp. 133–140.

[10] C. L. Chowdhary, P. V. Patel, K. J. Kathrotia, M. Attique, K. Perumal, and M. F. Ijaz, "Analytical study of hybrid techniques for image encryption and decryption," *Sensors*, vol. 20, no. 18, p. 5162, 2020.

[11] H. Touil, N. El Akkad, and K. Satori, "Text encryption: hybrid cryptographic method using Vigenere and Hill Ciphers," in *2020 International Conference on Intelligent Systems and Computer Vision (ISCV)*, IEEE, 2020, pp. 1–6.

[12] R. Banoth and R. Regar, "An introduction to classical and modern cryptography," in *Classical and Modern Cryptography for Beginners*, Springer, 2023, pp. 1–46.

[13] Y. Awad, D. Jomaa, Y. Alkhezi, and R. Hindi, "A NEW APPROACH COMBINING RSA AND ELGAMAL ALGORITHMS: ADVANCEMENTS IN ENCRYPTION AND DIGITAL SIGNATURES USING GAUSSIAN INTEGERS.," *Jordanian J. Comput. Inf. Technol.*, vol. 11, no. 1, 2025.

[14] S. Kumar and D. Sharma, "A chaotic based image encryption scheme using elliptic

curve cryptography and genetic algorithm," *Artif. Intell. Rev.*, vol. 57, no. 4, p. 87, 2024.

[15] F. Hermawan, A. Hanifah, S. Alamsah, and R. K. Harryes, "Analisis catch per unit effort pole and line cakalang (Katsuwonus pelamis) di perairan Kupang," *J. Marshela (Marine Fish. Trop. Appl. Journal)*, vol. 2, no. 1, pp. 23–33, 2024.

[16] R. Shneor and A. A. Vik, "Crowdfunding success: a systematic literature review 2010–2017," *Balt. J. Manag.*, vol. 15, no. 2, pp. 149–182, 2020.