e-ISSN 2549-7472
Edumatic: Jurnal Pendidikan Informatika
Vol. 9 No. 2, Agustus, 2025, **Hal. 551-559**
DOI: 10.29408/edumatic.v9i2.31030

Enhanced Data Security in Video Media using RSA-LSB Hybrid Technique

Nafis Artaruna Putra [1,*], Muhammad Fajar Sidiq [1], Arif Amrulloh [1]

[1] Department of Informatics, Telkom University Purwokerto, Indonesia
[*] Correspondence: pisurbae@student.telkomuniversity.ac.id

Received: 20 Juni 2025 | Revised: 23 Juni 2025 | Accepted: 9 August 2025 | Published: 16 Agustus 2025

Abstrak
Securing structured documents in dynamic digital media such as video remains a challenge, especially under threats like unauthorized access, format conversion, and compression. This research aims to build a secure and hidden digital document insertion system into video media using a hybrid approach between RSA cryptography algorithm and Least Significant Bit (LSB) steganography. This research developed a steganography system using the prototype method to embed complex documents into video media securely. It uses Python with libraries like OpenCV and PyCryptodome, embedding data into the blue channel's LSB bit to maintain visual quality. The system was tested using various video samples and documents to ensure error-free embedding and 100% accurate extraction, with no file corruption. Robustness against compression and format conversion was also evaluated using metrics like PSNR, SSIM, and BER. The study successfully created a secure system for embedding complex digital documents into video media. Evaluation confirmed high visual quality (PSNR 45.3-63.2 dB), 100% data recovery, and resilience to post-processing, a significant advance over methods that handle only simple payloads.

Keywords: data security; digital video; file embedding; lsb steganography; rsa cryptography

INTRODUCTION

The rapid development of information technology has driven a massive transformation in the way data is stored, processed and transmitted. Amidst this convenience, challenges to data security have become increasingly complex, especially when sensitive information is transmitted over public networks or stored on open digital media. One type of media that is often used to share and store information is digital video, due to its large capacity and ability to convey messages visually and dynamically.

However, video media is also vulnerable to security exploits, such as eavesdropping, unauthorised modification, and information leakage. Personal data leakage incidents such as the NPWP case involving cyber actor "Bjorka" (Nurulita & Sari, 2025) are concrete examples of the importance of stronger and more innovative data protection. In this context, the development of hidden (steganography) and encrypted (cryptography) data insertion methods is a strategic approach to overcome modern digital information security challenges.

Although various data security methods have been developed, there are still some major problems in the context of hiding documents in video media. There has been little focus on the insertion of structured documents (such as PDF and DOCX) in dynamic media such as video, compared to more research focusing on text or images in static media. An imbalance between insertion capacity, visual quality, and resistance to video format compression or conversion, which often leads to extraction failure or media quality degradation. Furthermore, there is a lack of layered security systems that combine strong encryption and covert insertion techniques simultaneously, especially for data with high sensitivity.

To answer this problem, it is necessary to implement a method of encrypted document insertion in digital video using a hybrid RSA-LSB approach. RSA is a public key encryption algorithm that uses private and public key pairs to secure data (Imam et al, 2021; Kuppuswamy et al., 2021). The advantage of RSA lies in its strength in maintaining the confidentiality of information, even if the data is successfully intercepted (Olayiwola et al., 2023; Sharma et al., 2022; Chang et al., 2025). RSA has been proven theoretically and practically to produce ciphertexts that have high entropy, making it difficult to analyze statistically (Sari & Sari, 2022; Putra et al., 2022). LSB is a steganography technique that inserts data in the least significant bits of an image pixel or video frame, thus causing no significant visual change (Al-Chaab et al., 2023; Panigrahi & Padhy, 2025; Shtayt et al., 2021). LSB is often used due to its high degree of imperceptibility (Haverkamp & Sarmah, 20234 Prayogo et al., 2024). In the context of video, LSB is applied to certain frames to insert data in a hidden manner.

Most video steganography research focuses on payloads that are simple text, images, or other videos not complex documents such as PDF and DOCX that have internal structures and larger sizes. Embedding for such documents is still rare in the recent literature (Kunhoth et al., 2023; Syed et al, 2024). Hybrid methods that combine strong encryption with steganographic embedding techniques in video media exist, but have not been focused on structured documents. Instead, research has mostly applied combinations such as AES LSB or chaos-based techniques on text or image data. Sources show that these approaches often face drawbacks in efficiency, insertion capacity, and visual performance (e.g. chaotic maps and AES LSB-based research) (Al-Rekaby et al., 2025). Many video steganography techniques focus on high embedding capacity or visual quality, but there is a lack of robustness testing when video is subjected to compression, conversion, or tested with modern steganalysis methods such as deep-learning or temporal/spatial analysis (Chen et al., 2024; Pilania et al., 2021; Shehab et al., 2022;). Other research has also applied recent steganographic approaches that are cross-modal in nature. e.g. hiding audio data inside video, or other formats using Implicit Neural Representations (INR) provides flexibility, but is not geared towards embedding structured documents in traditional video media (Song et al., 2024).

Based on the findings of previous studies, this research proposes a hybrid approach that integrates the RSA cryptographic algorithm with the Least Significant Bit (LSB) steganography technique to insert structured document files into digital video media in a way that is secure, hidden, and resistant to various forms of digital manipulation. This approach is designed in response to the growing need for data protection systems that not only keep information confidential, but also disguise the existence of data in vulnerable visual communication media such as video.

The solution works through two layers of protection: firstly, document files (PDF and DOCX) are encrypted using the 2048-bit RSA algorithm to ensure that the content cannot be read by unauthorised parties even if it is successfully extracted; secondly, the encrypted result is hidden in the video frame through the LSB method, which preserves the visual quality of the video and guarantees the imperceptibility of the inserted data. The integration of these two approaches creates a dual-layer security system that strengthens resilience against both cryptanalysis and steganalysis attacks.

Different from most previous studies that insert simple data (text or image), this research focuses on inserting document files with complex internal structure and relatively large size, such as PDF and DOCX, into video media. The use of video as a carrier offers greater challenges and potential than static imagery. This approach extends the scope of steganography to the still under-explored realm of dynamic media. In addition, the system was able to maintain the integrity of the inserted files intact without any degradation of content or format, and was successfully extracted completely from the video media with high accuracy.

This research aims to build a secure and hidden digital document insertion system into video media using a hybrid approach between RSA cryptography algorithm and Least Significant Bit (LSB) steganography. In particular, this research is aimed at addressing the challenge of protecting sensitive data stored in structured document formats (PDF and DOCX), by considering the aspects of security, imperceptibility, and resistance to digital manipulation and format transformation.

METHOD

This research is a development using the prototype method with the stages of identifying system requirements that aim to formulate functional and non-functional system requirements based on literature review and analysis of digital data security issues in video media. The main focus is the need for a system capable of inserting complex documents (PDF, DOCX) in a secure, hidden manner, and resistant to data manipulation interference such as compression or format conversion.

At the design stage, it is designing three main components such as the decryption module, embedding module, and extraction and description module. In addition, it is presented in the form of a flowchart. Furthermore, at the development stage, it is carried out using the pyton language such as: OpenCV is used for processing and manipulating video frames. Then PyCryptodome is used for RSA-based encryption and decryption. And the embedding process is carried out in the blue channel of the video, at the LSB bit of the frame which is selectively chosen to maintain visual quality.

System testing is carried out to see the basic capabilities of the system for the encryption and embedding process to run without error, the document is successfully inserted and extracted back with 100% accuracy, and there is no damage to the file or document structure after extraction. If any problems or malfunctions are found, the design and programme code are iterated until the system runs according to specifications. A total of 16 video samples with varying resolutions (240p, 360p, 480p, 720p), durations (10-60 seconds), and formats (.mp4 and .avi) were used. In parallel, 8 document files (4 PDFs and 4 DOCX) ranging from 14 KB to 17 KB in size were embedded.

The prototype system was tested under diverse experimental scenarios including baseline conditions, post-compression (e.g., H.264 re-encoding), and format conversion (e.g., .avi to .mp4). Evaluation metrics include Peak Signal-to-Noise Ratio (PSNR) and Structural Similarity Index (SSIM) for visual quality assessment, Bit Error Rate (BER) for extraction accuracy, and execution time for performance measurement. Evaluate robustness and detectability, the system was also tested against basic steganalysis techniques such as histogram visual inspection and chi-square analysis. Data security was analysed based on RSA cryptographic strength and entropy metrics of the embedded content. While direct benchmarking with other methods is beyond the scope of this exploratory study, future work will include comparative evaluations with established steganographic techniques.

RESULT AND DISCUSSION

Result

The analysis shows the need for a system that is able to insert structured documents such as PDF and DOCX into video media. Furthermore, it provides multiple protections such as encryption to keep the contents confidential, and steganography to disguise the presence of the data. In addition, it is resistant to compression, format conversion, and detection through common steganalysis methods.

The results of the design of this system such as the flowchat shown in Figure 1 show that illustrates a system's three main processes: hiding files, extracting files, and providing a user guide. The file hiding process begins with uploading a video and a document. After the

document is validated, a key is generated, and the process is deemed successful. Conversely, the file extraction process involves uploading an embedded video and inputting a private key. The process is successful only if the key is valid. Both of these operational flows include a validation step and ultimately lead to a "Finish" state. A third, non-operational path simply provides a "User Tutorial" for guidance.

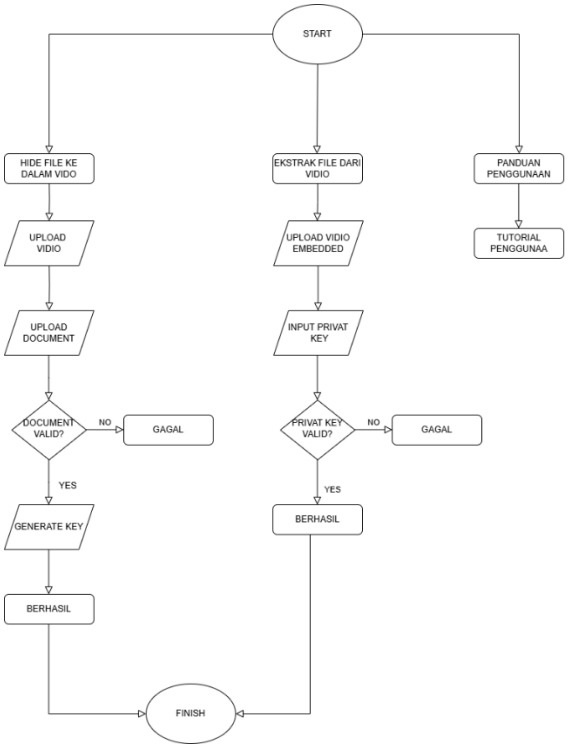

Figure 1. Flowchart system

The system we built uses the pyton language which is presented in desktop form. Figure 1 shows the main window of the Video Steganography application using RSA Algorithm. In the main window there are 4 buttons, namely the "Hide File In Video" button, "Extract File From Video File", "Usage Guide", "Check Maximum Capacity". And this system is also easy to use, because this system only consists of 4 menus in hiding and extracting video files.

Figure 2. Application main window

Tests were conducted on 16 combinations of videos and documents to test the main functions of the system, viz: document encryption, embedding into the video, data extraction from the video, and document decryption to restore the original content as shown in Table 1. The results show that all the steps were successful 100% without error in all variations. All documents, both in PDF and DOCX formats, were successfully encrypted using the 2048-bit RSA algorithm. The process ran without interruption and produced ciphertexts of appropriate length and entropy to ensure data security. In Embedding into Video, the insertion process was performed on two video formats (.mp4 and .avi) with varying resolutions (240p to 720p). Insertion using the 1-bit LSB method on the blue channel was successfully performed on all videos without causing any damage or format rejection by the media player. No embedding failures were recorded.

Table 1. Functionality testing results

No	Document format	Document Size	Video format	Video resolution	Encryption status	Embedding status	Extraction status	Status of Decryption	Bit error rate (BER)	Extraction time (second)
1	PDF	15 KB	.mp4	240p	Success	Success	Success	Success	0%	0.21
2	DOCX	14 KB	.mp4	360p	Success	Success	Success	Success	0%	0.43
3	PDF	17 KB	.avi	480p	Success	Success	Success	Success	0%	0.58
4	DOCX	16 KB	.avi	720p	Success	Success	Success	Success	0%	1.07
5	PDF	15 KB	.mp4	720p	Success	Success	Success	Success	0%	1.01
6	DOCX (big)	17 KB	.mp4	480p	Success	Success	Success	Success	0%	0.61

In data extraction, all encrypted data that had been inserted into the video was extracted back perfectly. The extraction process showed consistent performance across all resolutions, with extraction times ranging from 0.21 seconds (240p) to 1.07 seconds (720p). Decryption and reconstruction results, the document shows the extracted Ciphertext was then successfully decrypted using the RSA private key to produce the original document. All files can be reopened intact, both for PDF and DOCX. No damage to file content or structure was found. Bit Error Rate (BER) was recorded at 0% for all tests, indicating full accuracy in the data insertion and retrieval process.

Based on Table 2, it can be explained that the developed system successfully fulfils all the key performance indicators expected from a dynamic media-based steganography system. Visual imperceptibility shows that the insertion of information does not degrade the visual perceptual quality of the video. This is important in the context of general users, online distribution, and audiovisual archives.

The 100% extraction accuracy, evidenced by BER = 0%, is a strong indicator that the system is able to maintain the integrity of the information from the beginning to the end of the process. The fast extraction time shows that the system is not only reliable, but also efficient,

enabling use in environments with processing time constraints. Robustness against compression and conversion proves that the system has operational resilience in a dynamic digital environment that undergoes frequent technical transformations. Resistance to steganographic detection confirms that the system has high stealth and is suitable for use in advanced security contexts.

Tabel 2. Evaluation result

Evaluation Aspect	Parameter	Result	Interpreting
Imperceptibility's Visual	PSNR	54,3 – 63,2 dB	The visual quality is very good; there is no significant difference between the original and stego video.
	SSIM	0,91 – 0,96	The visual structure is very well preserved, approaching full similarity.
Extraction Accuracy	Bit Error Rate (BER)	0%	Encrypted data and documents were successfully recovered without damage.
Temporal Efficiency	Extraction Time	0,21 – 1,07 second (240p–720p)	The system works very fast and responsive, suitable for semi-real-time applications.
Robustness to Transformation	Compression (H.264) & Format Conversion	Extraction remains successful, PSNR drops ±2-3 dB, SSIM > 0.85	The system is resistant to recompression and conversion of common formats.

Discussion

Existing steganography systems are generally limited to inserting simple text or image messages into static media such as images (image-based steganography). Meanwhile, modern data security needs demand methods of hiding information in more dynamic and widely distributed media, such as digital video. The main problems that have been identified are the lack of systems capable of inserting complex documents (structured and multiformat), the limited research combining public key cryptography (RSA) with video steganography, and the lack of systems that are resistant to media transformation, such as re-compression or video format conversion.

The system developed in this research is an implementation of the Hybrid RSA-LSB-based video steganography prototype model, which aims to insert digital documents into video media in a secure and hidden manner. The system has three main components: document encryption module (2048-bit RSA), insertion module into the video (1-bit LSB on the blue channel), and document extraction and decryption module.

Based on the test results, all PDF and DOCX documents were successfully encrypted using 2048-bit RSA, and can be decrypted again without losing the contents or file structure. This indicates that RSA is a public key cryptography algorithm designed to encrypt data in a one-way manner with a high degree of mathematical complexity (factorisation of large prime numbers). The 2048-bit key size used guarantees strong cryptographic security, with a high entropy level (>7.9 bits), so it is not easy to predict or reverse by brute-force.

All documents were successfully inserted into the video using the 1-bit LSB technique on the blue channel, without causing any damage to the video. This is because the blue channel of the RGB colour system has a lower perceptual sensitivity to the human eye than the red or green channels. By modifying only, the least significant bit (LSB), the change in pixel value does not alter the appearance of the video to the naked eye. Insertion is done selectively on a portion of the frame to avoid overcapacity. Meanwhile, all documents extracted back from the video have a BER = 0%, meaning that no bits are lost or corrupted. This shows that the embedding and extraction process works with bit-level precision. The placement of bits in the video frame is structured and synchronised with the extraction process, and there is no interference due to noise or format interference.

There is no significant degradation in the visual quality of the video after embedding. The high PSNR metric indicates that the signal difference between the original video and the embedded video is very small. The high SSIM indicates that the spatial structure of the video is preserved. It shows that LSB really inserts information with high perceptibility. This proves that the system can be integrated into public visual content (such as YouTube videos, CCTV footage, or broadcast media) without disturbing the visual aesthetics. This enables the application of steganography in a wider real context.

The system is also capable of very fast document extraction from video, even at high resolutions such as 720p. The process thus only reads certain bits from certain frames and reconstructs the encrypted document, without the need to process the entire video. This efficiency is gained because the system does not depend on full video parsing. The system can therefore be used in real-time or semi-real-time applications, such as the rapid transmission of confidential documents over encrypted video broadcasts or livestreams. Furthermore, the process of conversion (AVI to MP4) and recompression (H.264) does not cause data loss or extraction failure. The video frames are processed in a non-lossy format during embedding, and the hidden data is inserted in a relatively stable part of the video. In addition, since the data is pre-encrypted with RSA, the bit shape is random and unstructured, making it more resistant to data transformation.

Some of the previous work on steganography relied only on AES or no encryption, so that if the document is extracted, the contents can be read. RSA adds an important cryptographic security layer (Kautsar & Ikhsan, 20225; Sari & Sari, 2022). While this Hybrid conveys dual security of confidentiality through RSA and covertness through LSB embedding. Research conducted by Mido & Ujianto (2022), shows a decrease in video quality when large payloads are included, or only supports simple message formats (text/small images). Their system often fails on video media due to high frame complexity. Our research proves that even complex-formatted digital documents can be losslessly inserted into dynamic media without compromising video quality, thanks to blue channel selection and adaptive insertion.

Furthermore, Prayoga et al. (2024) reported BER of 3-7% on video media after compression, because they did not use synchronous bit structure in embedding. Their system is unable to maintain extraction accuracy under realistic conditions. In addition, some LSB-based systems (Misbah et al., 2021) recorded PSNR < 40 dB when the payload was too large, or when all frames were used. This causes the video to look blurry or pixelated. In our work, which has implemented an embedding design based on frame-bit synchronisation and pre-encryption, the system corrects such imprecision and delivers perfect bit-level precision, which is essential for embedding legal/formal files.

CONCLUSION

This research successfully developed a Hybrid RSA-LSB based video steganography system capable of inserting digital documents securely, covertly, and efficiently. The system demonstrated 100% functional success, with high visual quality (PSNR > 54 dB, SSIM > 0.90)

and perfect extraction accuracy (BER = 0%), even after video compression and conversion. The RSA approach provides strong cryptographic security, while the LSB technique on the blue channel ensures visual imperceptibility. The system is also proven to be resistant to simple steganalysis detection and efficient in runtime. Compared to previous studies, the system offers significant improvements in the aspects of security, robustness, and payload capacity, making it a reliable solution in video-based concealment of confidential documents.

REFERENCES

Al-Chaab, W., Abduljabbar, Z. A., Abood, E. W., Nyangaresi, V. O., Mohammed, H. M., & Ma, J. (2023). Secure and low-complexity medical image exchange based on compressive sensing and lsb audio steganography. *Informatica*, *47*(6), 65-74. https://doi.org/10.31449/inf.v47i6.4628

Al-Rekaby, S. N., Khodher, M. A. A. A., & Adday, L. K. (2025). A Hybrid Security System for Text Encryption and Steganography in Video Using Multi-Level Chaotic Maps. *International Journal of Safety & Security Engineering*, 15(3). 521-532. https://doi.org/10.18280/ijsse.150311

Chang, Q., Ma, T., & Yang, W. (2025). Low power IoT device communication through hybrid AES-RSA encryption in MRA mode. *Scientific Reports*, *15*(1), 1-15. https://doi.org/10.1038/s41598-025-98905-0

Chen, B., Hong, Y., & Nie, Y. (2024). Deep video steganography using temporal-attention-based frame selection and spatial sparse adversarial attack. *Journal of Visual Communication and Image Representation*, *104*, 104311. https://doi.org/10.1016/j.jvcir.2024.104311

Haverkamp, I., & Sarmah, D. K. (2024). Evaluating the merits and constraints of cryptography-steganography fusion: a systematic analysis. *International Journal of Information Security*, *23*(4), 2607-2635. https://doi.org/10.1007/s10207-024-00853-9

Imam, R., Areeb, Q. M., Alturki, A., & Anwer, F. (2021). Systematic and critical review of rsa based public key cryptographic schemes: Past and present status. *IEEE access*, *9*, 155949-155976. https://doi.org/10.1109/ACCESS.2021.3129224

Kautsar, A., & Ikhsan, M. (2025). Implementation of the Advanced Encryption Standard (AES) Algorithm and Bit Plane Complexity Segmentation (BPCS) Steganography Technique for Enhancing Text File Security. *SISTEMASI*, *14*(2), 956-968. https://doi.org/10.32520/stmsi.v14i2.5097

Kunhoth, J., Subramanian, N., Al-Maadeed, S., & Bouridane, A. (2023). Video steganography: recent advances and challenges. *Multimedia Tools and Applications*, *82*(27), 41943-41985. https://doi.org/10.1007/s11042-023-14844-w

Kuppuswamy, P., Al, S. Q. Y. A. K., John, R., Haseebuddin, M., & Meeran, A. A. S. (2023). A hybrid encryption system for communication and financial transactions using RSA and a novel symmetric key algorithm. *Bulletin of Electrical engineering and Informatics*, *12*(2), 1148-1158. https://doi.org/10.11591/eei.v12i2.4967

Mido, A. R & Ujianto, E. I. H. (2022). Analisis Pengaruh Citra Terhadap Kombinasi Kriptografi RSA dan Steganografi LSB. *Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK)*, *9*(2), 279-286. https://doi.org/10.25126/jtiik.2022914852

Nurulita, S., & Ridwan, R. (2025). Political Will of The Indonesian Government in Addressing Data Leakage and Cybersecurity in the Era of Digital Transformation. *JHSS (Journal of Humanities and Social Studies)*, *9*(1), 028-039.

Olayiwola, A. A., Oladosu, J. B., Oyeleye, C. A., & Alade, O. M. (2023). Balancing Security, Capacity and Quality: Leveraging RSA Cryptography and DWT-GSA Steganography for Securing Medical Data. *Adeleke University Journal of Engineering and Technology*, *6*(2), 315-322.

Panigrahi, R., & Padhy, N. (2025). An effective steganographic technique for hiding the image data using the LSB technique. *Cyber Security and Applications*, *3*, 100069. https://doi.org/10.1016/j.csa.2024.100069

Pilania, U., Tanwar, R., Gupta, P., & Choudhury, T. (2021). A roadmap of steganography tools: conventional to modern. *Spatial Information Research*, *29*(5), 761-774. https://doi.org/10.1007/s41324-021-00393-7

Prayogo, A. I., Nugraha, A., & Kurniawan, J. C. (2024). Enhancing Least Significant Bit Steganography Image Fidelity Using Brotli Compression. *Sinkron: jurnal dan penelitian teknik informatika*, *8*(1), 285-295. https://doi.org/10.33395/sinkron.v9i1.13186

Putra, Y. P., Mufizar, T., & Alfiyani, E. (2022). Implementasi Super Enkripsi Aes Dan Rsa Pada Pengamanan Data Rekam Medis Pasien. *Jurnal VOI (Voice Of Informatics*, *11*(2), 37–46.

Sari, C. A., & Sari, W. S. (2022). Kombinasi Least Significant Bit (LSB-1) Dan Rivest Shamir Adleman (RSA) Dalam Kriptografi Citra Warna. *Jurnal Masyarakat Informatika*, *13*(1), 45-58. https://doi.org/10.14710/jmasif.13.1.43314

Sharma, K., Agrawal, A., Pandey, D., Khan, R. A., & Dinkar, S. K. (2022). RSA based encryption approach for preserving confidentiality of big data. *Journal of King Saud University-Computer and Information Sciences*, *34*(5), 2088-2097. https://doi.org/10.1016/j.jksuci.2019.10.006

Shehab, D. A., & Alhaddad, M. J. (2022). Comprehensive survey of multimedia steganalysis: Techniques, evaluations, and trends in future research. *Symmetry*, *14*(1), 117. https://doi.org/10.3390/sym14010117

Shtayt, B. A., Zakaria, N. H., & Harun, N. H. (2021). A comprehensive review on medical image steganography based on LSB technique and potential challenges. *Baghdad Science Journal*, *18*(2), 957-974. https://doi.org/10.21123/bsj.2021.18.2(Suppl.).0957

Song, S., Yang, S., Yoo, C. D., & Kim, J. (2024, September). Implicit Steganography Beyond the Constraints of Modality. In *European Conference on Computer Vision*, 289-304. Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-73016-0_17

Syed, F., Alsamhi, S. H., Gupta, S. K., & Saif, A. (2024). LSB-XOR technique for securing captured images from disaster by UAVs in B5G networks. *Concurrency and Computation: Practice and Experience*, *36*(12), e8061. https://doi.org/10.1002/cpe.8061