

Hide Text within a Video Using Data Encryption Standard (DES) Technology

Abbas Ali Hassan Al-Agaili ¹, Huda Hamdan Ali ¹, Hayder A. Naser ¹

¹ Department of CTE, Imam Al-Kadhumi College, Baghdad, Iraq

Abstract – It is possible to encode a message using one of the encryption algorithms and embed the text within a selected frame from the video, as this is considered a more secure method for handling confidential information. The concealment is deemed unbreakable because the message is encrypted in a manner that prevents decryption, making it challenging to retrieve the hidden text. In this study, Data Encryption Standard (DES) technology was employed to embed the last bits of the chosen video frame using a software-based approach. The frames, decoders, PSNR, and encrypted messages are illustrated in various videos. The results demonstrated minimal impact on the video's accuracy, as concealment occurs in the least significant bits (LSB), preserving the overall precision of the video.

Keywords – Data Encryption Standard, DES, least significant bits, LSB, steganography.

1. Introduction

The practice of concealing text within images has a rich history depicted across various pictures. However, the act of embedding written content within images traces its origins back to the 15th century with the use of a technique known as "steganography."

DOI: 10.18421/SAR71-04

<https://doi.org/10.18421/SAR71-04>

Corresponding author: Hayder A. Naser ,
Department of CTE, Imam Al-Kadhumi College, Baghdad,
Iraq


Email: hayder.a.naser@gmail.com

Received: 14 February 2024.

Revised: 15 March 2024.

Accepted: 21 March 2024.

Published: 27 March 2024.

 © 2024 Abbas Ali Hassan Al-Agaili, Huda Hamdan Ali & Hayder A. Naser; published by UIKTEN. This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivs 4.0 License.

The article is published with Open Access at <https://www.sarjournal.com/>

During this period, individuals employed steganography to covertly embed confidential messages within small images, which were then portrayed on maps or other items. With the development of technology following the world wars, computers were employed to conceal information within images. Consequently, text concealment techniques have become more widespread and accessible to a larger audience. Messages are hidden using steganographic techniques so that only the envisioned receiver can see them [1]. Steganography involves concealing confidential text or messages within various media files, such as images, texts, audios, or videos [2]. This strategy aims to safeguard the secrecy of the message by evading detection [3]. Broadly, steganography techniques can be categorized into physical microdots and digital methods [4]. Image steganography techniques for embedding can further be classified into two classes based on the hosting place and the nature of the image [5]. Video steganography refers to the concealment of information using video as the carrier. This method excels at concealing substantial amounts of data, leveraging the fact that a video comprises frames or images containing a significant number of redundant bits [6]. Different formats are available for varying video transmission and storage capacities. The choice of physical interface and signal protocol depends on the physical format of the data storage device or transmission medium [7]. In recent years, self-destructing or disappearing texts have gained traction and become more accessible to many users. The size and sensitivity of data transferred across the Internet continue to grow, emphasizing the increasing importance of network security [8]. The Data Encryption Standard (DES) encryption technique has its origins in the LUCIFER Feistel block cipher, developed in 1971 by IBM cryptography expert Horst Feistel [9]. Each round in DES utilizes a unique key, and the Feistel construction is employed with 16 rounds. DES uses a 56-bit key for encryption. The DES algorithm can be cracked by machines. It takes a 64-bit plaintext block and a defined key, and uses them to create a 64-bit encoded text blocks.

Demonstrating its high competence [10], the DES algorithm operates through multiple rounds, with each round constituting a distinct step in the process. Iterations are calculated based on the size of the key; for instance, a 128-bit key requires 10 iterations, while a 192-bit key requires 12 iterations, and so on. Besides being competent, unnoticeable, and robust, the least significant bit (LSB) steganography is among the most reliable methods for image steganography. It has been widely employed to conceal text behind images in various fields, including encryption, anti-hacking, and secure online data sharing [11], [12]. In the initial phase of this investigation, a video file was read and converted into frames. Subsequently, we developed new tools and platforms to enhance the safety and efficiency of this process. With ongoing technological advancements, there is a continual emergence of new tools and platforms aimed at improving safety and efficiency. Employing the DES algorithm and LSB steganography, we chose one of the generated frames to conceal a previously encoded message.

2. Materials and Methods

The DES process is divided into several parts, denoted as rounds in Figure 1. The size of the key being utilized determines how many rounds are required. For instance, 10 rounds are needed for a 128-bit key, 12 rounds are needed for a 192-bit key, and so forth [4].

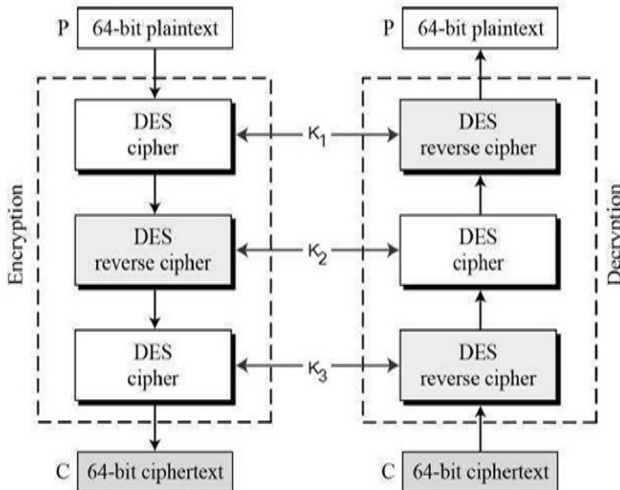


Figure 1. The procedure of DES

The code snippet is displayed in Figure 2. The plain text is organized into 64-bit chunks. The Initial Permutation (IP), which involves a transposition process, is carried out before to the first round.

This phase substitutes the first bit with the 58th bit, and the another bit with the 50th bit, and so on. Following this, the 64-bit text is divided into two equal segments, each containing 32 bits. These segments are referred to as Left Plain Text (LPT) and Right Plain Text (RPT) [13].

- Step 1: Transform Key Elements (Compression Permutation)

The DES procedure utilizes a 56-bit key, created by eliminating bits at every 8th place in a 64-bit key, resulting in the production of a 56-bit key. Afterward, the 56-bit key is divided into two identical parts, and the bits undergo a rounded leftward modification based on the amount of rounds [14]. This shift rearranges all key bits, eliminating certain bits in the process and ultimately resulting in a 48-bit key.

- Step 2: Permutation of Expansions

For an RPT with a size of 32 bits formed during the IP stage, it is stretched from 32 bits to 48 bits in this phase. The 32-bit RPT is segmented into 8 chunks, each consisting of 4 bits, with an additional two bits appended to each portion. Following this, the bits undergo permutation among themselves, yielding a 48-bit dataset. Subsequently, the 48-bit key that was attained in step 1 and the extended 48-bit RPT are subjected to an XOR function.

```
function varargout = hidden(varargin)
% HIDDEN MATLAB code for hidden.fig
%   HIDDEN, by itself,
%   creates a new HIDDEN or raises
%   the existing
%   singleton*.
```

Figure 2. A section of the programming code for the intended project

The procedure for this task is outlined in Figure 3. When executing the code, the initial interface appears, allowing us to implement the required instructions. Next, we can load the video and convert it into frames using the "Convert Video" button. Subsequently, we enter text and press the "Encrypt" button to encrypt the entered text. Afterward, we click on the "Hide" button to conceal the cipher text. Finally, we press the "Decrypt" button to revert the hidden encrypted text to its original form.

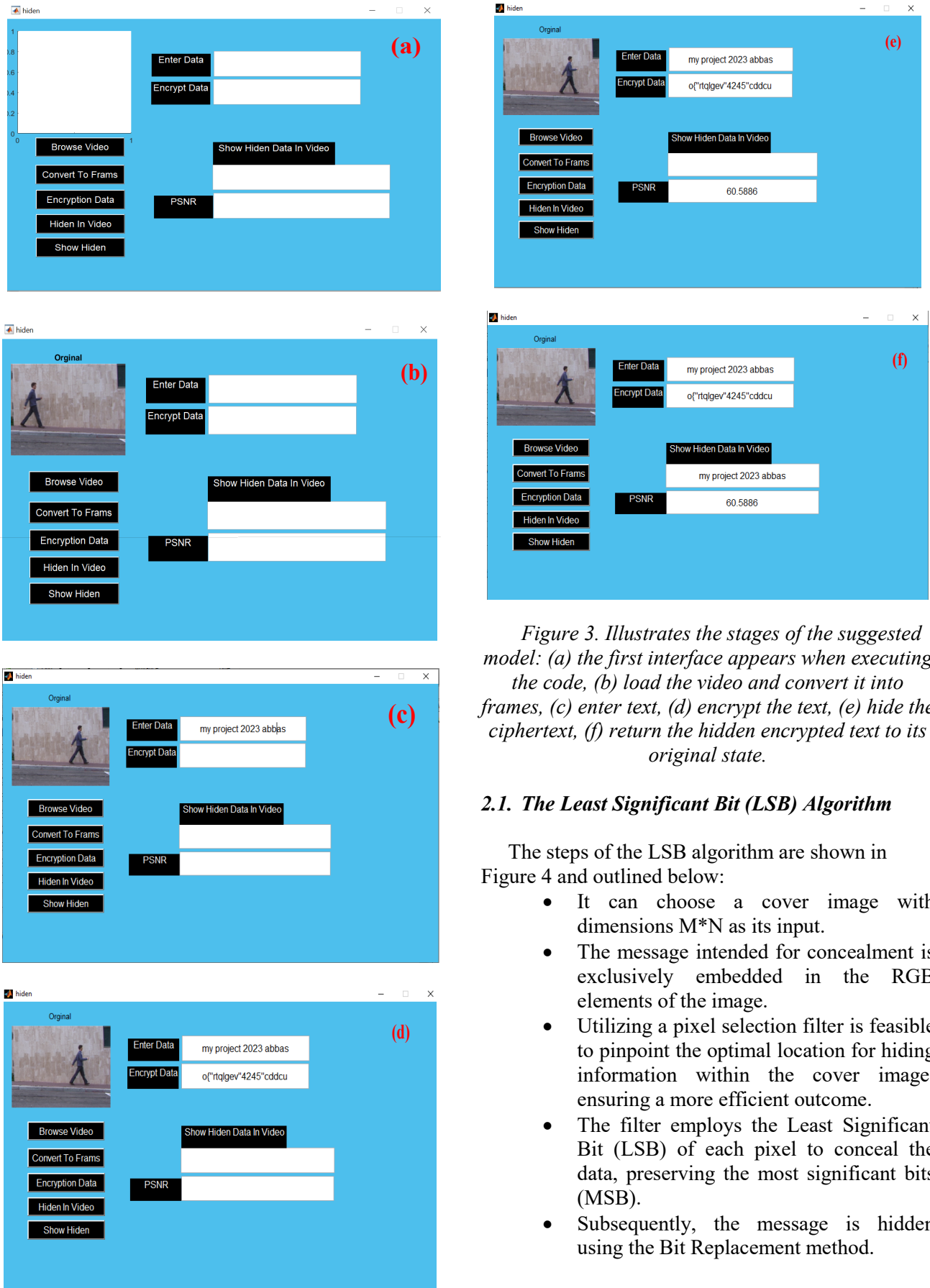


Figure 3. Illustrates the stages of the suggested model: (a) the first interface appears when executing the code, (b) load the video and convert it into frames, (c) enter text, (d) encrypt the text, (e) hide the ciphertext, (f) return the hidden encrypted text to its original state.

2.1. The Least Significant Bit (LSB) Algorithm

The steps of the LSB algorithm are shown in Figure 4 and outlined below:

- It can choose a cover image with dimensions $M \times N$ as its input.
- The message intended for concealment is exclusively embedded in the RGB elements of the image.
- Utilizing a pixel selection filter is feasible to pinpoint the optimal location for hiding information within the cover image, ensuring a more efficient outcome.
- The filter employs the Least Significant Bit (LSB) of each pixel to conceal the data, preserving the most significant bits (MSB).
- Subsequently, the message is hidden using the Bit Replacement method.

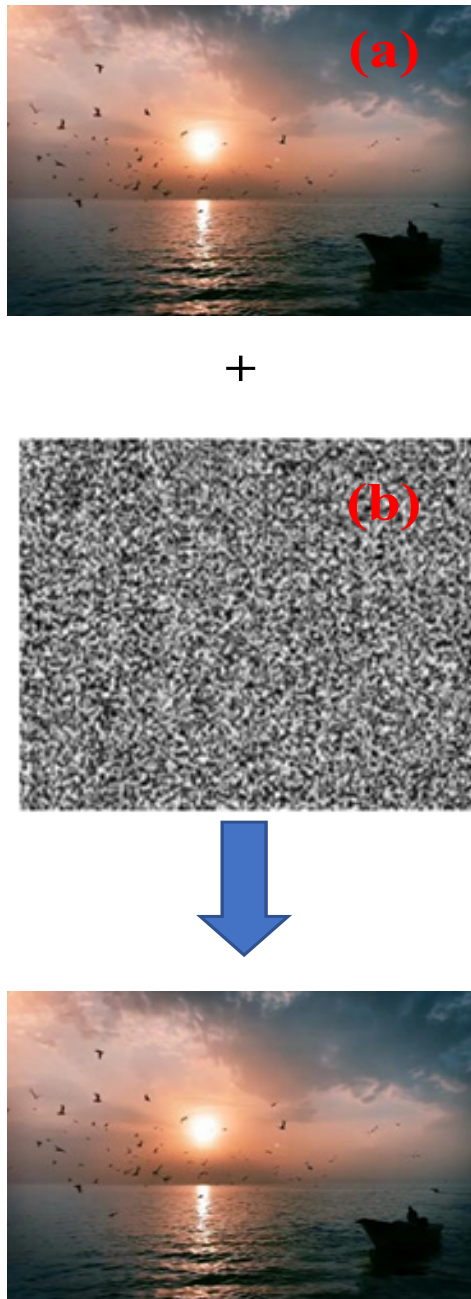


Figure 4. The steps of the LSB algorithm.

GIF pictures can also be steganized with LSB [15], but additional care has to be taken. The challenge with using the color approach for GIF images is that changing a pixel's LSB can significantly affect the image's color because it alters the color palette's index [16].

3. Results and Discussions

The obtained results of applying the projected technique are listed in Table 1. This table includes the original text, its encoding, the percentage of text hidden inside the image, and the image in which the text was concealed, sourced from the video frames. The frames, decoders, PSNR, and encryption messages are displayed with different videos.

Table 1. The results of the present work show text hiding inside the image taken from the video frames. The frames and decoding, PSNR, and encryption messages are displayed with different videos.

No.	Image of the video frame	Frames	Decode	PSNR	Encryption	Message
1		3827	Hide text inside a video with DES technology	72.0379	Jkfg"vgzv"kp ukfg"c"xfqg" ykvj"FGU"vg ejpnqj{	Hide text inside a video with DES technology
3		1006	Hide text inside a video with DES technology	59.3590	Jkfg"vgzv"kp ukfg"c"xfqg" ykvj"FGU"vg ejpnqj{	Hide text inside a video with DES technology
5		464	Hide text inside a video with DES technology	59.9919	Jkfg"vgzv"kp ukfg"c"xfqg" ykvj"FGU"vg ejpnqj{	Hide text inside a video with DES technology
7		1797	Hide text inside a video with DES technology	65.0654	Jkfg"vgzv"kp ukfg"c"xfqg" ykvj"FGU"vg ejpnqj{	Hide text inside a video with DES technology
10		668	my project 2023 abas ali Itenog	63.0690	Jkfg"vgzv"kp ukfg"c"xfqg" ykvj"FGU"vg ejpnqj{	my project 2023 abas ali Itenog
11		755	Hide text inside a video with DES technology	62.2886	Jkfg"vgzv"kp ukfg"c"xfqg" ykvj"FGU"vg ejpnqj{	Hide text inside a video with DES technology
13		998	Hide text inside a video with DES technology	82.6397	Jkfg"vgzv"kp ukfg"c"xfqg" ykvj"FGU"vg ejpnqj{	Hide text inside a video with DES technology
15		741	Hide text inside a video with DES technology	79.2262	Jkfg"vgzv"kp ukfg"c"xfqg" ykvj"FGU"vg ejpnqj{	Hide text inside a video with DES technology
17		3398	Hide text inside a video with DES technology	65.8489	Jkfg"vgzv"kp ukfg"c"xfqg" ykvj"FGU"vg ejpnqj{	Hide text inside a video with DES technology
19		916	Hide text inside a video with DES technology	60.7789	Jkfg"vgzv"kp ukfg"c"xfqg" ykvj"FGU"vg ejpnqj{	Hide text inside a video with DES technology

According to Table 1, the PSNR values range from 59.3590 to 82.6397 for 16-bit data, which are more typical compared to the values in [17]. As a result, when alternate videos are used in this code, the software generates an image that conceals hidden text. Furthermore, the program ensures the replacement of old frames with new ones when alternate videos are employed.

4. Conclusion

In this work, we encrypted essential messages within video clips using Data Encryption Standard (DES) technology. Through this method, we successfully concealed crucial data across a diverse range of file formats, including images, videos, sounds, and other intricate files. To achieve this, the data were integrated into arrays of their components, resulting in an exceptionally effective data concealment system. Favorable results were observed in concealing data, as indicated by the PSNR results ranging from 59.3590 to 82.9310. Further development of the system is recommended to accommodate a variety of texts and files. Additionally, incorporating artificial intelligence into the system is suggested to enhance its security.

References:

- [1]. Mohsin, S. (2011). Concentration of the specific absorption rate around deep brain stimulation electrodes during MRI. *Progress In Electromagnetics Research*, 121, 469-484.
- [2]. Murhty, G. K., & Kanimozhi, T. (2024). Methodologies in Steganography and Cryptography–Review. *Modern Approaches in Machine Learning and Cognitive Science: A Walkthrough: Volume 4*, 205-214.
- [3]. Guaña-Moya, J., Borja-López, Y., Gutiérrez-Constante, G., Jaramillo-Flores, P., & Basurto-Guerrero, O. (2024). Information Security Vulnerabilities Using Steganography as the Art of Hiding Information. In *International Conference on Information Technology & Systems*, 107-116. Cham: Springer Nature Switzerland.
- [4]. Sachin, Kumar, R., Sakshi, Yadav, R., Reddy, S. G., Yadav, A. K., & Singh, P. (2024, January). Advances in Optical Visual Information Security: A Comprehensive Review. In *Photonics*, 11(1), 99. MDPI.
- [5]. Abdalhussein, E., Ibrahim, N. J., & Ali, Y. H. (2024). Image Steganography Based on Hybrid Salp Swarm Algorithm and Particle Swarm Optimization. *International Journal of Intelligent Engineering & Systems*, 17(1).
- [6]. Muhammad, K., Ahmad, J., Farman, H., & Zubair, M. (2015). A novel image steganographic approach for hiding text in color images using HSI color model. *arXiv preprint arXiv:1503.00388*.
- [7]. Yang, G., Jan, M. A., Rehman, A. U., Babar, M., Aimal, M. M., & Verma, S. (2020). Interoperability and data storage in internet of multimedia things: investigating current trends, research challenges and future directions. *IEEE Access*, 8, 124382-124401.
- [8]. Downing, J. (2023). Social Media, Digital Methods and Critical Security Studies. In *Critical Security Studies in the Digital Age: Social Media and Security*, 71-108. Cham: Springer International Publishing.
- [9]. Bhat, M. I., & Giri, K. J. (2021). Impact of computational power on cryptography. *Multimedia Security: Algorithm Development, Analysis and Applications*, 45-88.
- [10]. Cahya, R., Arief, P., Novriza, A., & Kohei, A. (2018). Noble method for data hiding using steganography discrete wavelet transformation and cryptography triple data encryption standard: DES. *International Journal of Advanced Computer Science and Applications*, 9(11), 261-266.
- [11]. Subramanian, K., Venkatachalam, M., & Saroja, M. (2021, August). Adaptive counter clock gated S-Box transformation based AES algorithm of low power consumption and dissipation in VLSI system design. In *Journal of Physics: Conference Series*, 1979(1), 012066. IOP Publishing.
- [12]. Prokop, K., Polap, D., Srivastava, G., & Lin, J. C. W. (2023). Blockchain-based federated learning with checksums to increase security in internet of things solutions. *Journal of Ambient Intelligence and Humanized Computing*, 14(5), 4685-4694.
- [13]. Chaturvedi, C. M., Singh, V. P., Singh, P., Basu, P., Singaravel, M., Shukla, R. K., ... & Singh, S. (2011). 2.45 GHz (CW) microwave irradiation alters circadian organization, spatial memory, DNA structure in the brain cells and blood cell counts of male mice, *mus musculus*. *Progress In Electromagnetics Research B*, 29, 23-42.
- [14]. Mehndiratta, A. (2015). Data hiding system using cryptography & steganography: a comprehensive modern investigation. *Int. Res. J. Eng. Technol*, 2(01), 397-403.
- [15]. Hassan, M., Murad, A. M. I. N., & Mahdi, S. (2020). Steganalysis Techniques and Comparison of Available Softwares. In *Proceedings of the 1st International Multi-Disciplinary Conference Theme: Sustainable Development and Smart Planning, Proceedings of the 1st International Multi-Disciplinary Conference Theme: Sustainable Development and Smart Planning, IMDC-SDSP 2020, Cyberspace, 28-30 June 202, 248. European Alliance for Innovation*.
- [16]. Watni, D., & Chawla, S. (2023). Impact of various image formats supported by android smartphones on image steganography: a preliminary study. *Multimedia Tools and Applications*, 1-20.
- [17]. Rizqa, I., Safitri, A. N., & Harkespan, I (2022). Kriptostegano Menggunakan Data Encryption Standard dan Least Significant Bit dalam Pengamanan Pesan Gambar. *JURNAL MASYARAKAT INFORMATIKA*, 13(2), 111-120.