RESEARCH ARTICLE OPEN ACCESS

Cryptography and Steganography Based Hiding Technique for Efficient Data Protection

Muhammad Lamir Isah[1],Adamu Muhammad Tukur[2], Hamza Audi Giade[3]; Monday Simon[4]
[1]Department of Computer Science. Abubakar Tatari Ali Polytechnic, Bauchi,Bauchi State Nigeria.
E-mail: muhammadlamir75@gmail.com
[2]Department of Computer Science. Abubakar Tatari Ali Polytechnic, Bauchi,Bauchi State Nigeria.
E-mail: babaadamu6644@gmail.com
[3]Department of Computer Science. Abubakar Tatari Ali Polytechnic, Bauchi,Bauchi State Nigeria.
E-mail: gidadohenz@gmail.com
[4]Department of Mathematical Science. Abubakar Tafawa BalewaI University Bauchi, Bauchi State Nigeria.
E-mail: simonmonday3386@gmail.com

----------**********----------

Abstract:

A more reliable technique for protecting data transfer has in fact been required due to the rise in attacks that have been documented during electronic information exchange between the source and the intended destination. Two well-known and often used methods for manipulating data to encrypt or conceal its presence are cryptography and steganography. These two methods aim to prevent unwanted access to information while maintaining its availability, confidentiality, and integrity. However, attackers now have an easier time hiding concealed data because to the advancements in steganalysis and image processing techniques. Researchers have suggested a number of countermeasures to address this problem, such as combining encryption with steganography. The Least Significant Bit (LSB) method, the Rivest–Shamir–Adleman (RSA) asymmetric key encryption scheme, and the Advanced Encryption Standard (AES) symmetric key encryption scheme—which uses the Diffie–Hellman key exchange algorithm—are all used in this research to implement the steganography technique. Next, the effectiveness of these two approaches is assessed in terms of how well they can protect and hide sensitive information as well as how quickly it can be hidden. The created method, which combines the Diffie-Hellman key exchange algorithm with AES, outperforms RSA as the encryption algorithm in terms of speed and data concealing capacity, according to the results.

Keywords **—Least Significant Bit, Rivest–Shamir–Adleman, Advanced Encryption Standard**

----------**********----------

I. INTRODUCTION

This document is a template. An electronic copy can bedownloaded from the conference website.

In the modern world, secure data transfer is essential. Text, picture, audio, and video data may now be sent and received with ease thanks to the development of the Internet. Data privacy and confidentiality are among the issues with data transfer (Santoso et al., 2018). Certain data is seen to be more private than others. Data hiding and encryption are two appropriate data security approaches that must be used to safeguard this kind of data. Steganography, a data concealment technique, is one of the approaches that may be applied (Sahu&Sahu, 2020). According to Bandekar and Suguna (2018), steganography is the process of concealing data, including text, images, audio, and video, behind another piece of data known as a cover picture. Three components typically make up this method: the data, the data carrier, and the secret key. Steganography differs from encryption in that it conceals the existence of processed data, whereas encryption does not (Fayyad-Kazan et al., 2021). Steganography is

therefore more attractive for data that has to be hidden in order to be meaningful. Steganography finds its use across a wide range of fields, including e-commerce, finance, the military, and the Internet of Things (IoT). The use of audio steganography for government and military covert communication has been suggested by Xin et al. (2018). Liashenko et al. (2018) investigate the use of steganography for remote biometric authentication. Several network-based steganography techniques are assessed in the study. Douglas et al. have also carried out a more thorough analysis of steganography uses in biometric data (2017). Next, Khari et al. (2020) used the Matrix XOR encoding to enable steganography on the Internet of Things. Malware like Zbot, Adgholas, and Cerber are also created using steganography (Cameron, 2018). These uses have demonstrated the widespread usage of steganography in data security and security attack techniques.

Steganalysis is the process of identifying whether steganography is present. The steganalysis methods have been enhanced by the development of modern technologies (Fayyad-Kazan et al., 2021). To prevent the data from being seen by current steganalysis tools, this study combines encryption methods with steganography that uses the LSB approach. The simplest type of steganography approach is called the Least Significant Bit (LSB) method, in which the concealed data is substituted for the least significant bit of the picture. Text encryption may be accomplished with the help of the lightweight RSA encryption method. A public key cryptography method called the RSA algorithm was first presented in 1977. There are three steps of RSA, which are key generation, message encryption, and message decryption. Another encryption scheme method that is AES will be paired with Diffie–Hellman algorithm which is used for the key exchanging process. All these algorithms are well-known and secure enough for text encryption.

Data confidentiality is a crucial aspect of security, and text is the most common form of data. Sensitive data, such as passwords or secret messages, necessitates the use of appropriate data security measures to ensure its protection. Steganography is a technique that conceals both the data and its existence from parties other than the sender and recipient. The primary considerations for securing text data using this technique are cover image quality, which helps to conceal the data from attackers, and data hiding speed, which ensures that the text data remains secure from the sender to the receiver. Attackers are unlikely to target data whose existence is unknown to them. Steganography is a versatile data concealment technique. However, using steganography alone to protect text data can be risky, as new steganalysis tools can detect traditional steganographic techniques as well as advancements in image processing and steganalysis tools have made it easier for attackers to uncover hidden data. To address this issue, researchers have proposed combining steganography with encryption. To this effect, we proposed a text data hiding system that combines the Least Significant Bit (LSB) steganography technique in conjunction with modified Advanced Encryption Standard (AES) symmetric encryption algorithm using Diffie-Hellman key exchange algorithm for efficient text data hiding as a complement to existing systems.

The objective of this research are to improve cover image quality for text data security in steganography using AES data encryption technique integrated with Diffie-Hellman Key Exchange Algorithm and LSB data hiding technique and to also evaluate the systems for performance using processing speed.

II. REVIEW OF RELATED LITERATURE

An easy way to comply with the conference paper formatting requirements is to use this document as a template and simply type your text into it.

The volume of data that is exchanged on a daily basis has data owners worried about security. Tawalbeh&Saldamli (2019) examined the problems with data privacy in big data and offered solutions. Sensors, networks, and back-end systems are among the IoT's system components that are identified as the primary sources of security concerns (Babu et al., 2018). Other areas that deal with data security issues include banking, social networking, e-business, healthcare, and governance

(Rath& Kumar, 2021). Cryptography and data concealing techniques are the two primary data security strategies, according to study by Sahu&Sahu (2020). Watermarking and steganography are the two primary techniques that fall under the category of data concealment methods. Steganography, according to Hussain et al. (2018), preserves the method's intricacy while enabling the concealment of both the data and the transmission.Steganography comes in two flavors: text and visual (Ali Khodher&AldeenKhairi, 2020). Spatial domain, spread spectrum, and distortion approach are image steganography techniques. Pixel Value Differencing (PVD), Least Significant Bit (LSB), and replacement algorithms are available in the spatial domain. In terms of performance, LSB offers high capacity, medium resilience, and high accuracy, according to a comparison of different approaches in the same research.

A. Steganography in Data Security

Steganography research comes in a variety of forms. Research on LSB and DWT-based steganography for picture and audio has been done by Ramya et al. (2018). Position Value (MPV) is the foundation of a picture steganography approach developed by Mukherjee et al. (2018). Arnold's transformation is used to jumble the cover picture before the concealed message is embedded. In a subsequent study, the picture compression approach is employed in conjunction with the LSB method after the concealment of the secret message.. On the data receiver side, this secret message will next be decompressed before being decrypted (Pandey et al., 2021).The majority of current research focuses on combining encryption methods with steganography techniques. This is done in an effort to increase the suggested method's complexity. Modified RSA steganography was first introduced by Majumder&Rahman (2019). Some disadvantages of this approach are said to exist, including the fact that it can only be used with grayscale images, that a high-resolution image is needed, and that both the original image and the image containing secret data must follow the same transmission protocol. In a different study, the steganography methods of Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DCT) or Dual RSA were merged (Vinothkanna, 2019). Cryptography Incorporated Steganography (CICS) is the name given to this combination. Before the data is hidden inside a.bmp picture file, the secret text is encrypted using the RSA technique (NassifJassim et al., 2019). Al Saffar (2019) has also created a steganography method to conceal the plain text in the cover picture, which is based on RSA and steganography. Al Saffar has proposed in this study that using the current method in conjunction with the Diffie-Hellman algorithm might enhance the intricacy of the data is hidden. The aforementioned study has demonstrated that the RSA algorithm works well in conjunction with steganography..It has been noted that the Advanced Encryption Standard (AES) algorithm is used in some steganography combinations with encryption techniques. Additionally, it has been revealed that AES performs more complexly and securely than RSA (Hindi et al., 2019). An image watermarking method called MarkToLock (Cirineo et al., 2017) is presented. It is based on the LSB approach and the AES algorithm. In this study, an additional picture is concealed within the cover image. The average file size of the majority of the resultant image has grown by 56.208%. Steganography and AES have been used by Siddalingesh&Manjunatha (2019) to conceal text and images in audio. The procedures are carried out using the DCT coefficient. Next, Hattim&Taha (2019) used the LSB approach in conjunction with AES. The.png file exhibits good Peak Signal to Noise Ratio (PSNR) values according to this research. The steganography-encrypted picture and the original cover image plotted histograms are almost identical.

B. Review of Related Work

It looks at how the anchor paper by Al Saffar (2019) uses the idea of RSA. According to Fouad et al. (2021), RSA is a symmetric key encryption that relies on a complex number for a certain oddinteger (e) and the rigidity of the analysis of many compounds. There is an integer pair that makes up the RSA public key. RSA is a well-liked encryption technique with several applications (Al Saffar, 2019).The least significant bit of each byte of pixels that make up the cover picture is where the secret message bits are sequentially inserted into order to

create a basic data concealing method called LSB (Mahdi, 2019). LSB replacement (LSBR) and LSB matching (LSBM) are the two different forms of LSB methods (Fateh et al., 2021).The improved approach used in this study entails building on top of the current LSB data concealing methodology by applying the Diffie-Hellman key exchange and AES encryption algorithm. The sender and the recipient share a public key using the Diffie-Hellman key exchange method. The secret key that may be used to both encrypt and decode the secret message is then calculated using this public key. This procedure involves the computation of modulus and inverse (Gupta & Reddy, 2022).The symmetric cryptography block cipher technique known as Advanced Encryption Standard (AES) uses the AES key schedule method to generate round keys from the cipher key. AES performs a number of operations, including bit-shifting, substitution, and XOR operations (Patgiri, 2021).

III. RESEARCH METHODOLOGY

This section outlines the process for studying the research on steganography and cryptography as effective methods for concealing text data. Keywords and search strategy are described. The method outlined in the computer science systematic literature review was applied in this review. Our systematic literature review is conducted using the work as a guide as well (Jauro et al., 2020).

C. Least Significant Bit

The LSB (Least Significant Bit) strategy, which swaps the least significant bit in some cover file bytes to conceal a series of bytes carrying the concealed data, is reportedly a highly well-liked methodology (Abikoye O. et al., 2012). The simplest method for embedding data into a digital audio file is called least significant bit (LSB) coding, which involves replacing each sample point's least significant bit with a binary message. When calculating, the bit position in a binary integer that indicates the value of the unit—that is, whether the number is even or odd—is known as the least significant bit, or LSB. Because Least significant digits are often written further to the right in positional notation, the LSB is frequently referred to as the right-most bit. It is comparable to the rightmost digit in a decimal number, which is the least significant digit. It is customary to give a bit number to each bit when referring to individual bits inside a binary number. Usually, these values fall between 0 and 1 fewer than the entire number of bits in the number. One beneficial aspect of the least significant bits is that they change quickly if there is even a tiny change in the number. As an illustration, adding 1 (binary 00000001) to 3 (binary 00000011) yields 4 (binary 00000100), changing three of the least significant bits from 011 to 100. In contrast, the three most important bits (000 to 000) do not change. In checksums generated by pseudorandom number generators, least significant bits are usually used. The following image shows how the LSB technique is used to encode the message "HEY" in a 16-bit CD quality sample (Jayaram, P. et al., 2011).

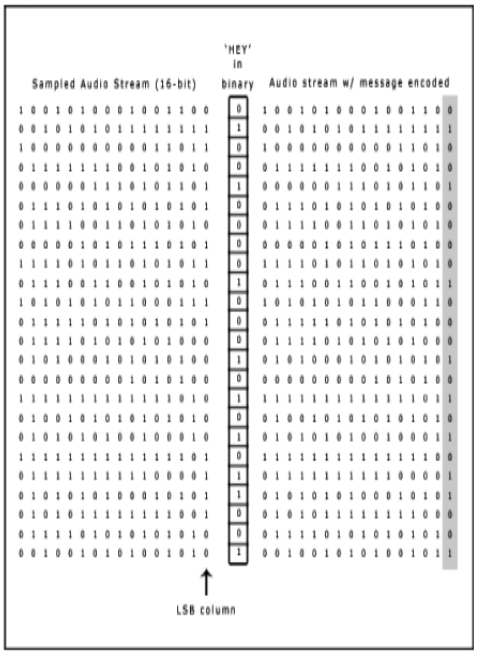

Figure1: Illustration of how the message “HEY” is encoded using LSB method, adapted from (Abikoye O. et al.,2012).

The secret key that may be used to both encrypt and decode the secret message is then calculated using this public key. This procedure involves the computation of modulus and alternative (Gupta & Reddy, 2022). The Advanced Encryption Standard (AES) symmetric cryptography block cipher methodology generates round keys from the cipher key using the AES key scheduling mechanism. AES carries out several operations, such as substitution, XOR, and bit-shifting (Patgiri, 2021).

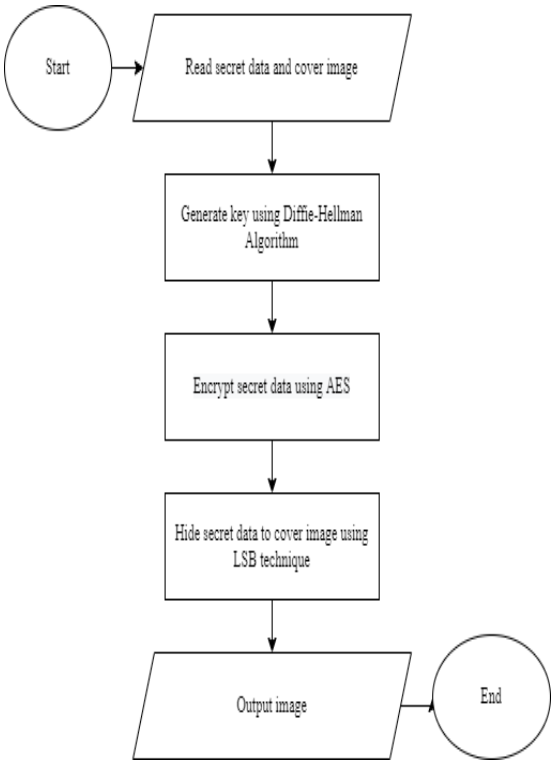

Figure2: Data hiding flowchart for the asymmetric algorithm.

The secret text message will be encrypted using RSA. The steps for the RSA encryption algorithm are shown in Figure 2

The LSB method is used to interlace the encrypted text with the cover picture. The practice of swapping out the image's least important bit for the concealed data bits is known as LSB. The receiver will receive the output of the LSB. The data extraction procedure is completed after the receiver receives the steganography image.The Data Extraction Flowchart is displayed in the following Figure 3.

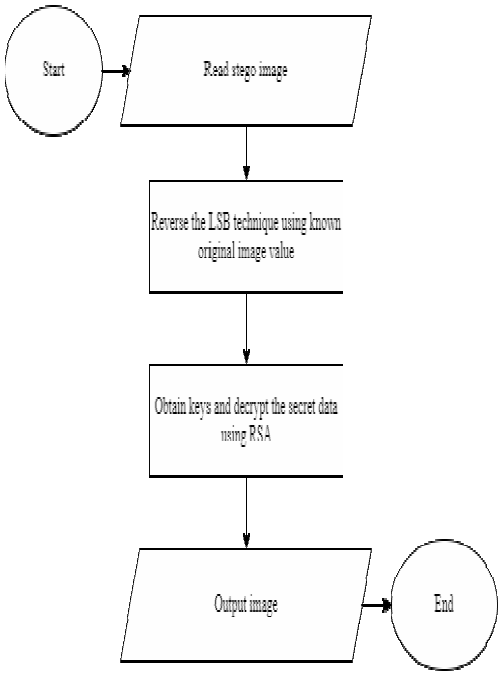

Figure 3: Asymmetric Algorithm Data extraction flowchart

The figure below shows the new suggested symmetric encryption technique that combines the Diffie-Hellman key generation process, AES encryption algorithm, and LSB steganography method.

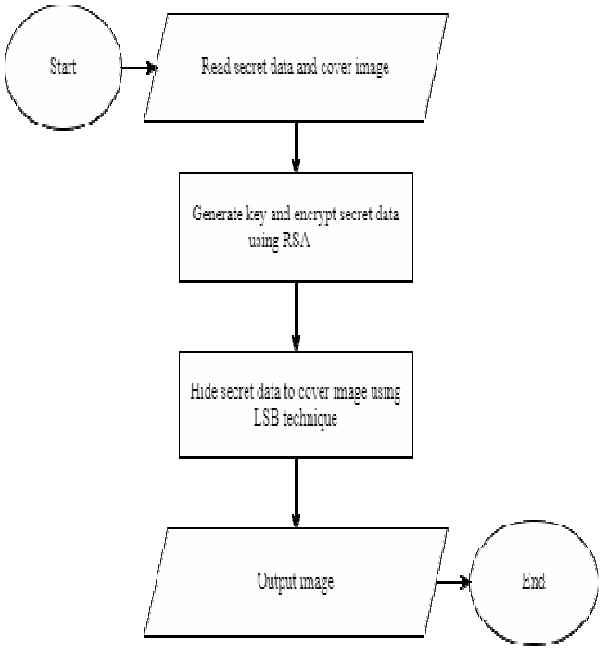

Figure 4: Data hiding flowchart for a symmetric algorithm

The MATLAB library module is used to apply the RSA image encryption procedures.

In the previous research by Al Saffar (2019), the image size is limited to square images. And in this research, images with aspect ratio other than 1:1 can also be encrypted using the encryption algorithm. However, the image resolution is limited up to 7680 x 4320 pixels.

Alice	Bob
Public Keys available = P, G	Public Keys available = P, G
Private Key Selected = a	Private Key Selected = b
Key generated = $x = G^a mod P$	Key generated = $y = G^b mod P$

Figure 5: Diffie-Hellman key generation process

The encrypted text is interwoven with the cover picture using the LSB approach once the Diffie-Hellman algorithm has finished key creation. The practice of swapping out the image's least important bit for the concealed data bits is known as LSB. The receiver will receive the output of the LSB.

IV. RESULTS AND DISCUSSION

Various key generation and encryption techniques are used before LSB is used to interlace the cover picture and the secret data. Peak Signal-to-Noise Ratio (PSNR), data hiding speed, and histogram analysis are used to measure how well various methods function.

D. Histogram Analysis

In steganography, the histogram plots for the original and stego images must be as comparable as feasible, in contrast to histogram analysis in picture encryption. Attackers or data interceptors might not be able to tell if a picture contains a secret message if the histogram plots are comparable. For this research, 7680 x 4320 image of Lenna is used. The image is converted to greyscale before implementing any other algorithms. The histogram plot consists of two axes, which are the pixel intensity value for x-axis and the pixel count for y-axis.

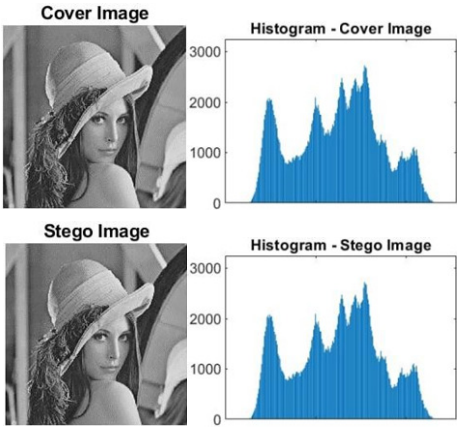

Figure 6: Histogram analysis for cover image and stego image using RSA encryption algorithm and LSB

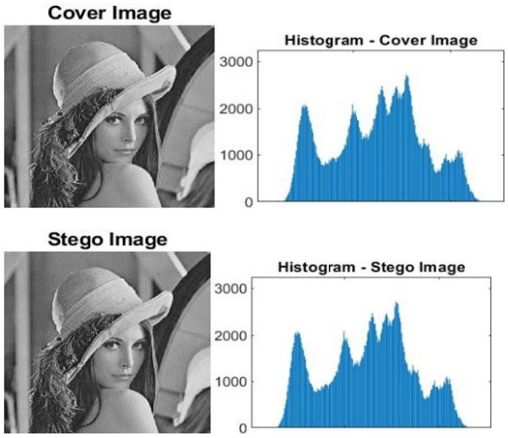

Figure 7: Histogram analysis for cover image and stego image using Diffie-Hellman key exchange algorithm, AES encryption algorithm and LSB

The histogram plots demonstrate that for both techniques, there is no discernible difference in the values for the cover picture and stego image. Given that it is impossible to tell the cover picture from the stego image visually, it follows that both methods are capable of concealing the secret text.

E. Peak Signal to Noise Ratio(PSNR)

PSNR value is a method to measure the quality of the image reconstructed from the steganography image. The higher the PSNR value, the higher the quality of the output image. PSNR value can be

calculated by using the formula below:PSNR = 10 Log10(R2÷MSE).

R is the maximum fluctuation in the input image data and MSE is the mean-square- error value of the image.

TABLE I

PSNR VALUE COMPARISON FOR DIFFERENT STEGANOGRAPHY TECHNIQUES

Algorithm	Image	PSNR (%)
RSA encryption algorithm + LSB steganography	Lenna.png	81.37
Diffie-Hellman key exchange + AES encryption algorithm + LSB steganography	Lenna.png	81.41

The PSNR values for both encryption techniques are high based on the abovementioned results, suggesting that the resulting picture is of good quality. The PSNR number derived from the two techniques shown above differs by just 0.04%. Interestingly, the combination of Diffie-Hellman, AES, and LSB techniques resulted in slightly better PSNR scores compared to using RSA and LSB together.The graphs below illustrate the comparative outcomes of these two methods.

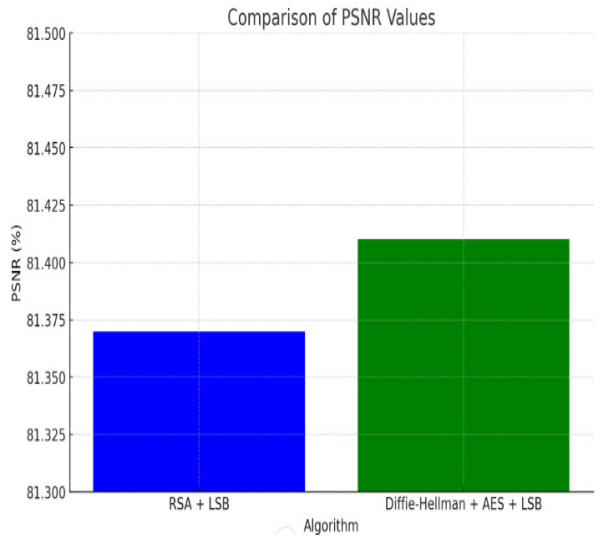

Figure 8: PSNR value comparison

F. Data Hiding Speed

One crucial aspect of steganography for real-time use is speed.In order for a steganography algorithm to be effective, it must not only safeguard the data's confidentiality but also function quickly. An Intel Core i7 8th Gen computer with 16GB RAM is used to execute the task.

TABLE II

TIME TAKEN FOR DIFFERENT STEGANOGRAPHY TECHNIQUES

Algorithm	Image	Time taken (s)
RSA encryption algorithm + LSB steganography	Lenna.png	0.3257
Diffie-Hellman key exchange + AES encryption algorithm + LSB steganography	Lenna.png	0.2104

Combining the Diffie-Hellman, AES, and LSB techniques results in a faster and more efficient process compared to using RSA and LSB techniques together. The graphs below illustrate the comparative outcomes of these two methods.

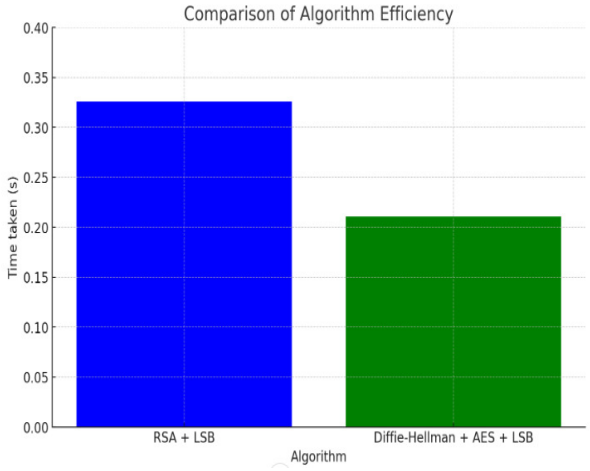

Figure 9: PSNR value comparison

The combination of Diffie-Hellman, AES, and LSB techniques is more sophisticated and produces greater performance than the combination of RSA and LSB, according to the data displayed in this section. While both methods work well when it comes to histogram analysis, the Diffie-Hellman, AES, and LSB combo performs better when it comes to PSNR value and data concealing speed.

V. CONCLUSIONS

In conclusion, enhancing current steganography methods can be achieved by integrating an encryption algorithm with steganography. This study utilizes the Diffie-Hellman key exchange technique to increase the implementation complexity of the encryption method. The results indicate that the combination of Diffie-Hellman, AES, and LSB outperforms the combination of RSA and LSB in terms of processing speed and PSNR value. Specifically, the PSNR value for the Diffie-Hellman and AES combination is 81.41%, compared to 81.37% for RSA. Additionally, the data concealing speed for steganography with RSA encryption is 0.3257 seconds, which is slower than the 0.2104 seconds required for the Diffie-Hellman and AES combination.

Effective steganography methods can enhance data security and maintain data confidentiality. The data remains encrypted even in the unlikely case that the stego picture is cracked. Nonetheless, the steganography method needs to show both high data concealment capability and a quick processing time. The study's findings support the hypothesis that LSB data hiding combined with Diffie-Hellman key exchange and AES encryption can enhance both the speed at which data is hidden and the quality of the cover picture.

G. Future Works

Various encryption algorithms can be integrated with steganography techniques to enhance the complexity of data hiding. Additionally, different types of secret data, such as images and videos, can be concealed within an image using steganography.

REFERENCES

[1] Al Saffar, N. F. H. (2019). Steganography Algorithm Based RSA Cryptosystem. Journal of Engineering and Applied Sciences, 14(7), 2240–2243. https://doi.org/10.36478/jeasci.2019.2240.2243

[2] Ali Khodher, M. A., &AldeenKhairi, T. W. (2020). Review: A comparison Steganography Between Texts and Images. Journal of Physics: Conference Series, 1591(1), 012024. https://doi.org/10.1088/1742-6596/1591/1/012024

[3] Bandekar, P. P., &Suguna, G. C. (2018). LSB Based Text and Image Steganography Using AES Algorithm. 2018 3rd International Conference on Communication and Electronics Systems (ICCES). https://doi.org/10.1109/cesys.2018.8724069

[4] Cameron, L. M. (2018, November 16). Computer Magazine | Flagship magazine of the IEEE Computer Society. Retrieved January 1, 2022, from Computer Magazine | Flagship magazine of the IEEE Computer Society website: https://publications.computer.org/computer-magazine/2018/11/15/how- steganography-works/

[5] Cirineo, C. C., Escaro, R. Q., Silerio, C. D. Y., Teotico, J. B. B., &Acula, D. D. (2017). MarkToLock: An image masking security application via insertion of invisible watermark using steganography and Advanced Encryption Standard (AES) algorithm. 2017 International Conference on Applied System Innovation (ICASI). https://doi.org/10.1109/icasi.2017.7988620

[6] Douglas, M., Bailey, K., Leeney, M., & Curran, K. (2017). An overview of steganography techniques applied to the protection of biometric data.

[7] E. Suresh Babu, D., Bhargav Raj, V., Manogna Devi, M., &Kirthana, K. (2018).A Review on Security Issues and Challenges of IoT.International Journal of Engineering & Technology, 7(2.32), 341. https://doi.org/10.14419/ijet.v7i2.32.15708

[8] Fateh, M., Rezvani, M., &Irani, Y. (2021). A New Method of Coding for Steganography Based on LSB Matching Revisited. Security and Communication Networks, 2021, 1–15. https://doi.org/10.1155/2021/6610678 Fayyad-Kazan, H., Saba, E., Hejase, H. J., El Dirani, A., &Rkein, H. (2021). JPEG Steganography: Hiding in Plain Sight. International Journal of Forensic Sciences (IJFSC), 6(1). https://doi.org/10.23880/ijfsc-16000223

[9] Gupta, C., &Subba Reddy, N. V. (2022).Enhancement of Security of Diffie-Hellman Key Exchange Protocol using RSA Cryptography. Journal of Physics: Conference Series, 2161(1), 012014. https://doi.org/10.1088/1742- 6596/2161/1/012014

[10] Hattim, M., &Taha, Z. (2019). Secure and Hidden Text Using AES Cryptography And LSB Steganography. https://doi.org/10.13140/RG.2.2.29786.80321

[11] Hindi, A. Y., Dwairi, M. O., &AlQadi, Z. A. (2019).A Novel Technique for Data Steganography. Engineering, Technology & Applied Science Research, 9(6), 4942–4945. https://doi.org/10.48084/etasr.2955

[12] Hussain, M., Wahab, A. W. A., Idris, Y. I. B., Ho, A. T. S., & Jung, K.-H. (2018).

[13] Image steganography in spatial domain: A survey. Signal Processing: Image Communication, 65, 46–66. https://doi.org/10.1016/j.image.2018.03.012.

[14] Implementation of Diffie-Hellman Algorithm - GeeksforGeeks. (2017, June 24). Retrieved January 1, 2022, from GeeksforGeeks website: https://www.geeksforgeeks.org/implementation-diffie-hellman-algorithm/

[15] Khari, M., Garg, A. K., Gandomi, A. H., Gupta, R., Patan, R., &Balusamy, B. (2020).Securing Data in Internet of Things (IoT) Using Cryptography and Steganography Techniques. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 50(1), 73–80. https://doi.org/10.1109/tsmc.2019.2903785

[16] Liashenko, G., Astrakhantsev, A., &Chernikova, V. (2018).Network steganography application for remote biometrie user authentication.2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT). https://doi.org/10.1109/dessert.2018.8409153

[17] Mahdi, M. H., Abdulrazzaq, A. A., Mohd Rahim, M. S., Taha, M. S., Khalid, H. N., &Lafta, S. A. (2019). Improvement of Image Steganography Scheme Based on LSB Value with Two Control Random Parameters and Multi-level Encryption. IOP Conference Series: Materials Science and Engineering, 518(5), 052002. https://doi.org/10.1088/1757-899x/518/5/052002

[18] Majumder, S., &Rahman, Md. M. (2019). Implementation of Security Enhanced Image Steganography with the Incorporation of Modified RSA Algorithm. 2019 International Conference on Electrical, Computer and Communication Engineering (ECCE). https://doi.org/10.1109/ecace.2019.8679147

[19] Mukherjee, S., Roy, S., &Sanyal, G. (2018). Image Steganography Using Mid Position Value Technique.Procedia Computer Science, 132, 461–468. https://doi.org/10.1016/j.procs.2018.05.160.

[20] Multimedia Tools and Applications, 77(13), 17333–17373. https://doi.org/10.1007/s11042-017-5308-3

[21] NassifJassim, K., KhudhurNsaif, A., KuderNseaf, A., Hazidar, A. H., Priambodo, B., Naf'an, E., … Putra, Z. P. (2019). Hybrid cryptography and steganography method to embed encrypted text message within image. Journal of Physics: Conference Series, 1339(1), 012061. https://doi.org/10.1088/1742- 6596/1339/1/012061

[22] Pandey, D., Wairya, S., Al-Mahdawi, R. S., Najim, S. A. M., Khalaf, H. A., Al- Barzinji, S. M., &Obaid, A. J. (2021). Secret data transmission using advance steganography and image compression.Int. J. Nonlinear Anal.Appl, 12, 2008– 6822. https://doi.org/10.22075/ijnaa.2021.5635

[23] Patgiri, R. (2021). privateDH: An Enhanced Diffie-Hellman Key-Exchange Protocol using RSA and AES Algorithm. IACR Cryptol.ePrint Arch., 2021, 647.

[24] Ramya, G., Janarthanan, P. P., &Mohanapriya, D. (2018). Steganography Based Data Hiding for Security Applications. 2018 International Conference on Intelligent Computing and Communication for Smart World (I2C2SW). https://doi.org/10.1109/i2c2sw45816.2018.8997153

[25] Rath, D. K., & Kumar, A. (2021). Information privacy concern at individual, group, organization and societal level - a literature review.Vilakshan - XIMB Journal of Management, ahead-of-print(ahead-of-print). https://doi.org/10.1108/xjm- 08-2020-0096

[26] Sahu, A. K., &Sahu, M. (2020). Digital image steganography and steganalysis: A journey of the past three decades. Open Computer Science, 10(1), 296–342. https://doi.org/10.1515/comp-2020-0136

[27] Santoso, K. A., Fatmawati, &Suprajitno, H. (2018).On Max-Plus Algebra and Its Application on Image Steganography.The Scientific World Journal, 2018, 1– 9. https://doi.org/10.1155/2018/6718653.

[28] Siddalingesh, B., &Manjunatha, R. H. S. (2019).Combined Audio Steganography and AES Encryption to Hide the Text and Image into Audio using DCT.International Journal of Recent Technology and Engineering, 8(3), 1732– 1738. https://doi.org/10.35940/ijrte.c4456.098319

[29] Tawalbeh, L. A., &Saldamli, G. (2019).Reconsidering big data security and privacy in cloud and mobile cloud systems.Journal of King Saud University – Computer and Information Sciences. https://doi.org/10.1016/j.jksuci.2019.05.007

[30] Vinothkanna, R. (2019). A Secure Steganography Creation Algorithm for Multiple File Formats. Journal of Innovative Image Processing, 1(01), 20–30. https://doi.org/10.36548/jiip.2019.1.003

[31] Wahab, O. F. A., Khalaf, A. A. M., Hussein, A. I., &Hamed, H. F. A. (2021).Hiding Data Using Efficient Combination of RSA Cryptography, and Compression Steganography Techniques. IEEE Access, 9, 31805–31815. https://doi.org/10.1109/access.2021.3060317

[32] Xin, G., Liu, Y., Yang, T., & Cao, Y. (2018).An Adaptive Audio Steganography for Covert Wireless Communication. Security and Communication Networks,

[33] Abikoye O. et al.,(2012) International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868Foundation of Computer Science FCS, New York, USAVolume 4– No.11, December 2012 – www.ijais.org

[34] Jauro, F., Chiroma, H., Gital, A. Y., Almutairi, M., Shafi'i, M. A., &Abawajy, J. H. (2020). Deep learning architectures in emerging cloud computing architectures: Recent development, challenges and next research trend. Applied Soft Computing, 96, 106582.

[35] Jayaram, P., Ranganatha, H. R. and Anupama, H. S. 2011.Information Hiding Using Audio Steganography – ASurvey. International Journal of Multimedia and ItsApplication, 3(3), pp. 86-96

