

Secure Text embedding using hybrid encryption algorithms

Kauthar Kabir

Department of Computer Software Engineering, Katsina State Institute of Technology and Management,
Katsina-Nigeria, PMB 2101. kautharkabir1@gmail.com

Abstract—Data and information Security in this modern world of digital communication are dominant looking at the rapid growing priority and dependency for interchanging confidential information across data networks. This paper emphasized to look into this and come up with an enhancement of image Steganography approach known as Most Significant Bit (MSB) using Secure Text embedding (STE). This research comprises of advance encryption System and Blow-fish algorithm to protect cover image and embed encryption Keys within Stego-image as Key images to improves the security of encrypted data by applying a robust pixel random function. In this respect a greater complexity is introduced without impacting the execution time significantly. The results of experiment indicate that this method's security is far better compared to other steganographic techniques, good distortion measurement computed having Mean Square error of 0.00043 and Peak Signal to noise ratio of 90.27 values guaranteeing excellent quality of image, very short Run time of 0.52ms for encryption and 0.90ms for decryption, which is correlated to security. Additional evaluations indicate the robustness of the proposed method making it the right solution for protected information concealment in digital images.

Keywords: Image steganography, Most Significant Bit, Secure Text, information concealment and communication

I. INTRODUCTION

The progressive need for protected communication system leads to effective advancement in information hiding approaches. The paper presented in AICITTRA 2024 conference titled “Information hiding in digital images using protected hiding scheme (PTHS)” focuses on embedding secret text message bits over cover image which are encrypted using Blowfish algorithm only to enhance security. In contrast, the proposed study under this title “protected concealment technique in digital images using secure text embedding (STE) focuses on embedding secret text message bits over cover image firstly by encrypting the secret message bits using Blowfish and AES algorithm to further addresses the emerging security, efficiency and robustness challenges. while the other work priorities to encrypt the secret text with Blowfish algorithm only, the enhanced approach introduce an advancement of combining blowfish algorithm with AES algorithm

aimed at bolstering integrity of data, confidentiality and resistance to malicious attacks.

To refine and extend the latitude of the earlier work, this new research targets to address the existing practical applications and theoretical foundations, thereby providing more comprehensive digital image steganography security solution. The dissimilarity between the two works lies in the issue of depth with the former presenting a base model and then offering a robust and optimized forward looking approach.

Malicious and illegal cyber-attacks targeting to attack private firms, Government organizations and manufacturing industries has led to continuous need for robust measures to secure confidential information. To this extent researchers and developers are looking for all possible technical way outs to guide the confidentiality of secret information [1]. Information and data security has reached a peak due to change from local area to wide area networks. To improve the security of cryptanalysis algorithms used for encryption have undergone significant advancements to improve their complexity there by preventing attackers from compromising encrypted data [2]. Steganography is defined as method of concealing secret message over cover media which is originated from the word “secret writing”. Steganography mainly aims at concealing the very presence of the message inside the cover medium [3].

There are many steganography techniques used to conceal secret information on cover media. Recent techniques take advantage of concealing secret information over images, audio, video and so on. The recent techniques of steganography attempt to take advantage of video files, digital media images, audio files, etc. Steganography can combine hiding and encryption mechanisms. This makes finding the data hidden in the object much more complicated since the data are unreadable, and any attacking techniques see the results as un expectable and confusing [4]. Moreover, steganalysis is the science and art of presenting messages hidden through steganography, identical to cryptanalysis utilized in cryptography [5]. The objectives of steganalys is to identify suspicious attacks, find out whether there is a payload that is encoded into the packages and retrieve that payload. Therefore, the main challenges of efficient steganography are as follows: Many researchers have been working on

steganography algorithms to make it difficult to detect/extract secret data by steganalysis and to make it difficult for the Human Visual System (HVS) to find a slight difference that happens on cover data such as audio, image, and video after the hiding process. In addition, the use of hybrid steganography has been increasing in recent years [6].

With rapid advancements in Information and communication (ICT), mostly information is stored as an Electronic-format. The information security has unavoidably resulted to a fundamental means of guarding modern right for digital broadcasting such as Text, audio, video, and images. In this respect, Steganography is applied to hide the existence of secret message specifically text, by which the message is concealed in digital broadcasting. This paper projected, protected concealment technique in digital images using secure text embedding (STE) that is based on Most Significant Bit (MSB) technique in hiding text in an image. The scheme improved the technique of MSB by embedding message bits at a random manner in to the image to come up with more secured scheme. Firstly the proposed algorithm encrypt the message bit by means of Blowfish and AES algorithms then embeds the secret message bits at random within original image attached with stego Keys applied. For message embedding and extraction of secret message the projected scheme offers what is known as a stego-key. Today's modern global information transmission needs efficient and protected or secured means of guiding information from illegal attacks.

The main contributions of the research paper are summarized as follows:

1. Development of an effective and efficient data hiding approach by means of secure text hiding steganography: These paper projected an approach that embed message bits at a random manner in to the image to come up with more secured scheme. The goal is to make the message hidden inside a cover medium undetectable to attackers.
2. Improvement in security of stego image: The projected approach aims to enhanced the security of the stego image by minimizing any visual differences between the cover image and the stego image. This helps to prevent presence of hidden data due visual attacks using Steganography evaluation metrics to testify this.
3. Application of Blowfish and AES algorithms for encryption: The paper utilizes Blowfish and AES algorithms used for encryption of the secret message and embedded in the cover image during the embedding process. The encryption key is derived from the stego value, ensuring that any alterations to the image are capable of

preventing successful key extraction and message decryption.

The remaining parts of this paper is organized as follows: Section 2 addresses the related works, Section 3 presents Design and Section 4 presents the results and discussion, and, and 5 recommendations for future direction.

II. LITERATURE REVIEW

The internet is offers a lot of merits to humans, especially to interchange information, teaching, learning, research, and so on. Confidentiality of data and security are the challenges of the internet. Many techniques were utilized to provide security including digital signatures, steganography, cryptography, and watermarking [7]. [8] conducted brief analysis and comparison of different spatial domain image steganography techniques. The author concluded that the modern secure image steganography presented a challenging task of transferring the embedded information to the destination without being detected. Steganography refers to covered writing. In relation to may Authors reports, Steganography is the skill and science of hiding delicate info in means that prevent revealing. The purpose of steganography is to deliver a message in such a way that not one person apart from the sender and projected recipient suspects the presence of the message [9].

In recent times, numerous ways to transmit coded messages is established to conceal the message in dissimilar application particularly broadcasting media like image, audio, or video. The method of Image steganography is classified into two categories based on the working domain: Spatial domain where the pixel value is directly modified for data hiding. Images in this domain are represented as a rectangular grid of pixels or points of color where the human perception does not observe the image as a grid. LSB and MSB known as Least significant bit and most significant bit respectively -based hiding strategies are most commonly used in this approach.

Frequency domain where the images that are in the domain of transform space are more robust in terms of some image processing manipulation and lossy and less prone to attacks Discrete cosine transform-based steganography and Discrete wavelet transform-based steganography are most commonly used in this approach. compression and less prone to attacks Discrete cosine transform-based steganography and Discrete wavelet transform-based steganography are most commonly used in this approach. Two valid reasons lead to the rapid growth and development in the interest of steganography as follows [10]:

- (i) Publication and broadcasting manufactures have interest of coming up with techniques to hide encoded

exclusive rights information and barcode numbers in advanced digital movies, audio soundtracks, paperwork and hypermedia products.

- (ii) Governments effort to restrict the obtainability of encryption services have encouraged people to study approaches by which private messages can be embedded in seemingly innocuous cover messages.

The approach of symmetric encryption is among the most famous methods of maintaining and protecting data security; a text or several random characters can be regarded as the secret key. The secret key is employed by a text message to change its content [11]. The encryption approach used in this technique is to convert each character to several alphabetic characters when the sender and recipient know the keys of all parties and then use the secret key to encrypt and decrypt the message. Blowfish is a technique of encryption, a block cipher more specifically. It is most frequently referred to as a cipher. Blow fish has a 64-bit block size and uses keys ranging from 3 to 2448 bits and. Its creator, Bruce Schneier, claims that it is free to use, open source, and royalty free. Although Blowfish is utilized in several cipher suites and encryption methods, AES is often employed. Blowfish is secure since no cryptanalysis attempt has succeeded [12,13].

The authors in [14] proposed image steganography method using LSB approach combined with Hybrid encryption algorithm but the security of LSB is very weak and the work requires graphical interface enhancement and takes long during encoding because LSB is normally the last bit, the algorithm have pass across all bits until it reach to the last. The means (AES) was chosen because it meets the paper objectives. A powerful encryption mechanism without the complication of sharing multiple keys as asymmetric encryption, especially when demanding to send the parameter required for extracting the data on a secure tunnel. AES is a symmetric block encryption that uses a 128-bit encryption key, which is very hard to break.

Also, the block encryption mechanism makes it possible to predict the encryption data using their language characteristic since it replaces the same data block with different coding types and sizes each time, Text steganography principles can be applied to a standard text file by hiding the message in the header information of the file. Using it this way helps maintain the original text file and jeep it the same without any change in the content itself; on the other hand, this mechanism increases the size of the file. Another mechanism replaces bits of the text file content and changes the original text, but it is not widely used since it makes the text unreadable. The AES solved the issue of short key use by 3DES and other symmetric encryption, which is the best choice

of the proposed algorithm technically [15]. Text steganography can also be applied to PDF documents or other text standards [16]. The most significant bit (also called the high-order bit) is the bit position in a binary number having the greatest value [17].

In [18] presented a work on image steganography using protected hiding scheme, which encrypts the secret text message bits using blow fish algorithm randomly within the cover image which is not secured enough and still needs improvement. MSB Steganography is highest bit in a series of numbers in binary. e.g in the binary number: 11001100, the most significant bit is far left 1. In the MSB technique the secret message is embedded in the most significant bit of the pixel of the image. The MSB is sometimes referred to as the left-most bit due to the convention in positional notation of writing more significant digits further to the left. Therefore, the research combined MSB with AES and Blow fish which developed a hybrid approach, and enhanced hiding Capacity, image quality, run time and Security of the aforementioned approaches specifically the work of kauthar kabir presented in AICITTRA Conference 2024 as lead paper for improvement.

III. METHODOLOGY

A. Secure Text Embedding (STE)

Cover images are used as means of concealing classified multimedia information from illegal attackers. In this approach, the hiding capacity of the cover image is divided with 50% of the storage are allocated for the stego file. Within this allocation, 30% is utilized for inserting the secret message, while the remaining 20% is dedicated to storing decoy data, which is used to test credibility. The key for encryption/decryption of stego value, obtained from the image during the upload function serves as a basis for a specific algorithm. Blowfish and AES techniques are used for encryption of the secret message and embedded in the cover image during the embedding process. The encryption key is derived from the stego value, ensuring that any alterations to the image are capable of preventing successful key extraction and message decryption. The length of the encryption and decryption keys varies depending on the size of the cover image, as it is derived from them as k value obtained from the image.

The secret message is divided into multiple parts to counter visual and statistical attacks, and strategically inserted into different segments of the cover image. Image Compression is performed to minimize noise and maintain the integrity of the embedded message. The process involves calculating the message and image size and determining the segment number and split used

within the image. Python 3.6 on VScode IDE utilising a web page is used to implement the embedding and extracting algorithms and applied to colored (5040 x 4032) pixels rose.jpg and (750 x 1125) pixels giraffe.png images. Many secret texts messages were embedded to evaluate the capability of the embedding process on the images.

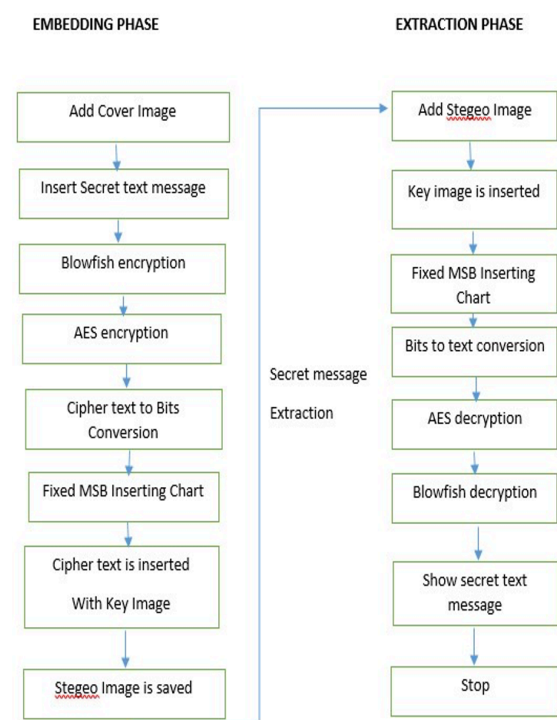


Fig 1: secured Text Embedding ((STE) encryption and decryption process

B. Key Steps in Secure Text Embedding (STE)

Embedding Stage

Step 1: Original image Pre-processing: Before embedding, the image has to be pre-processed which involves modifying brightness or contrast so as information hidden in MSB does not significantly affect quality of image.

Step 2: Secret message Encryption: The secret text message is embedded firmly over cover image at several films by means of the two Hybrid encryption algorithms (Blow fish and AES) and compression.

Step 3: Encrypted Text Embedding: The encrypted text is then embedded into the MSB of selected pixels using a robust pixel random function for security enhancement.

Step 4: Key Embedding: The cover image combines a secret message and an image created using a dynamic transfer model which acclimatises the key image method for calculating a cipher key and lead to many data-hiding techniques for security enhancement. The output is a stego image which difficult to detect secret message over it and ensure

robust and effective security. The stego image remain with a key as an idea for idea decryption.

Extraction Stage

To extract the hidden data, the reverse of the embedding process is performed:

Step 1: Add modified image. The image is uploaded, and the same sequence of pixels used for embedding is accessed.

Step 2: MSB Extraction. The MSBs of the selected pixels are extracted to reconstruct the binary data (the encrypted text).

Step 3: Key Decryption. In order to extract original secret text hidden, the extracted binary data is decrypted using the decryption key.

Step 4: Output. As the image is successfully uploaded, that's beginning of decryption phase, and decoding process followed, revealing the hidden secret message. An integrity checks guarantees that any alterations to the image, like an attack, did not change the value of the mask and compromised the decryption Key. This enables exactness and safety of the recovered secret message.

C. STE approach algorithm

```

# Main STE function
def ste_algorithm():
    # Load image
    image = Image.open('input_image.png').convert('L') # Convert to grayscale for simplicity
    # Input text and key for encryption
    text_to_hide = "Secret text message"
    key = os.urandom(32) # Blowfish key (32 bytes for Blowfish-256)
    key = os.urandom(32) # AES key (32 bytes for AES-256)

    # Encrypt the text
    encrypted_text = encrypt_text(text_to_hide, key)
    encrypted_text_length = len(encrypted_text)
    # Embed encrypted text into the image
    stego_image = embed_text_in_image(image, encrypted_text)
    stego_image.save('stego_image.png')
    print("Text successfully hidden in the image!")
    # Extract the encrypted text from the image
    extracted_encrypted_text = extract_text_from_image(stego_image, encrypted_text_length)
    # Decrypt the extracted text
    decrypted_text = decrypt_text(extracted_encrypted_text, key)
    print("Extracted and decrypted text:", decrypted_text)
    # Run the STE algorithm
    ste_algorithm()
  
```

D. PTHS algorithm explanation

1. Encryption: The 'encrypt_text' function encrypts the text using the Blowfish and AES algorithms with a random initialization vector (IV) in CBC mode which is prepended to the ciphertext for use during decryption. Text is padded to ensure it is a multiple of the Blowfish block size.
2. Embedding: The 'embed_text_in_image' function takes an image and the encrypted text and hides the text in the most significant bit (MSB) of each pixel's value. The text is converted to its binary representation, and the MSB of each pixel is replaced with bits of the encrypted text.
3. Extraction: The 'extract_text_from_image' function extracts the MSB from the pixels to reconstruct the encrypted text. The length of the extracted text is controlled based on the length of the original encrypted text.
4. Decryption: The 'decrypt_text' function decrypts the extracted encrypted text using the same Blow-fish and AES Key that were used for encryption.

The proposed work is tested based on the parameters of secret text message invisibility, Security and time taken to encode secret text message by means of three evaluation metrics which include Mean square error, Peak Signal to noise ratio and encoding time to test the proposed method efficiency and limitation of the proposed approach. Table 1 show thee jpg png and Gif images used for comparison.

Mean Squared Error (MSE) is calculated mathematically using the following equation which is defined as the measure of error difference between original image and stego image. If MSE is less the image quality is better.

$$MSE = \frac{\sum [(I_1(M, N) - I_2(M, N))^2]}{M * N}$$

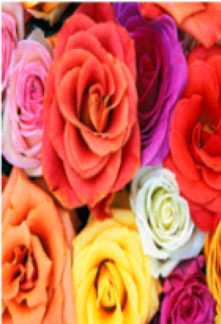
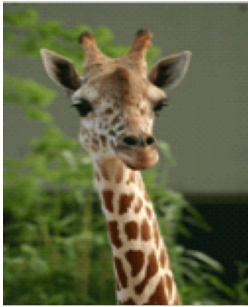
Peak Signal to Noise Ratio (PSNR) is termed as comparison of cover and stego image compression quality expressed mathematically as follows:

$$PSNR = 10 \log_{10} \frac{(255)^2}{MSE}$$

The time taken to embed secret text message in to cover image is known as **encoding time**. If Time T is a variable and Data size D is another variable, then the rate of change of T with respect to D is given by dT/dD.

IV RESULTS AND DISCUSSION

TABLE 1: EVALUATION OF THE PROPOSED METHOD USING TWO COVER IMAGES.

Image1:Rose.jpg	Image2:Giraffe.png	Image3:world.Gif
		

Many secret text messages with different sizes were used in testing the embedding capacity of the proposed approach. The image quality and ability to withstand any operation by image not to display secret message existence was tested using MSE and PSNR. Also the fastness and efficiency of the system was tested using encoding time parameter.

Table 2 show the result of simulation of PSNR, MSE and Encoding time for the proposed approach

by experiment using three images with different image format and dimension with secret text message of 30.4 kilo byte.

TABLE 1: EVALUATION RESULT

Cover Image	Size of the Image	PSNR	MSE	Encoding Time(ms)	
				Encryption	Decryption
Image 1 (Rose.jpg)	5040 x 4032	91.034	0.00040	0.79	0.20
Image 2 (Giraffe.png)	750 x 1125	90.890	0.00050	0.68	0.34
Image 3 (World.Gif)	850 x 1475	88.908	0.00040	0.78	1.01

From Table 2 (secret text message 30.4KB); PSNR values are 90.279, 89.087 and 87.907, MSE values are 0.00040, 0.00050 and 0.00040, in terms of encoding time for encryption the values are 0.79, 0.68 and 0.78, decryption values are 0.20, 0.34 and 1.01 for Images 1, 2 and 3 respectively. In terms of MSE and PSNR values it can be observed that Image 1 have the Highest PSNR and lowest MSE values than Image 2 and 3.

This specifies that Image 1 had the best image quality and the slightest degradation in terms of distortion after the steganographic process was applied compared to the other image. It can be

observed that the MSE values reduces as the PSNR values improved, showing that stego image quality is enhanced by increase in the PSNR values. Efforts should be addressed in future so that all images to have same MSE and PSNR values which will lead to same image quality. For the three images encoding time is ok as it is within the reasonable value.

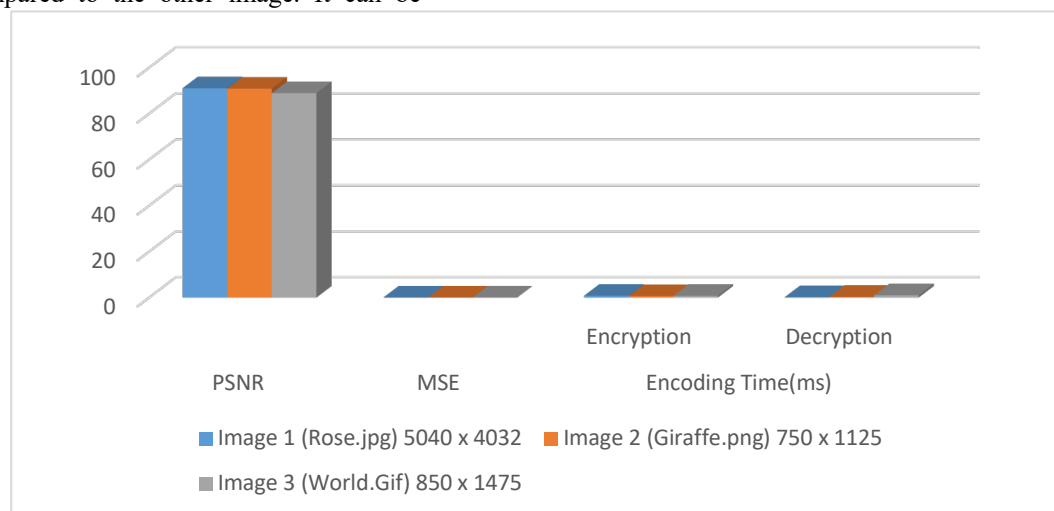


Fig 2: Proposed approach PSNR, MSE and Encoding time values

TABLE 3: PROPOSED AND EXISTING APPROACH PSNR COMPARISON

Proposed approach (PSNR values)		Existing approach (PSNR values)		Proposed algorithm (average running time)		Kabir [18](average running time)	
Image 1	91.034	Image 1	90.279	Encryption	Decryption	Encryption	Decryption
Image 2	90.890	Image 2	89.987	0.70	0.68	0.73	0.69
Image 3	88.908	Image 3	87.907	0.71	0.70	0.73	0.71

In Table 3 Proposed method is compared with existing approach based on PSNR values. The work of the proposed approach was evaluated and compared to Image Steganography Using PTHS that is the work of Kauthar Kabir (2024) in terms of Peak Signal-to-Noise Ratio (PSNR) and encoding time of cover images. The result revealed that

Proposed method have the highest PSNR indicating the one with best stego image quality observed in image 1, 2 and 3 where PSNR values reached 91.034, 90.890 and 88.908 respectively where as the existing approach PSNR is lower than that of the proposed with values from 87 to 90.

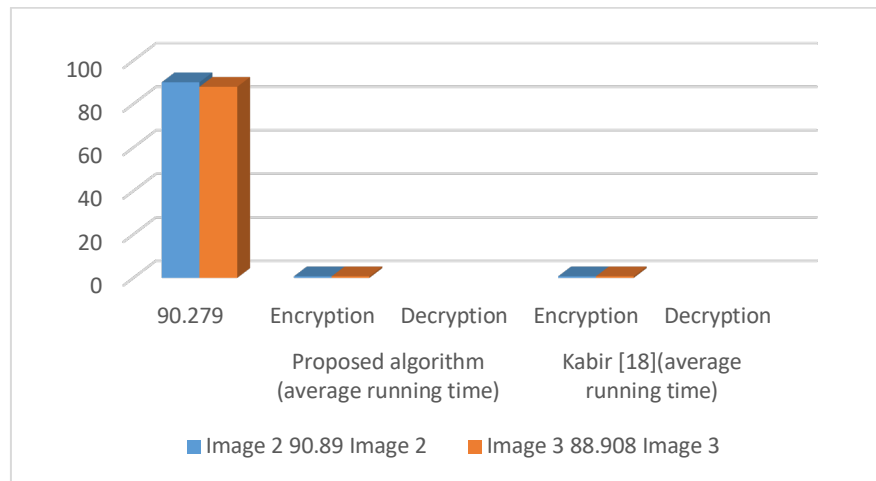


Fig 3: Comparison of the Proposed and existing approaches

Proposed approach security extent. This paper presented another image steganography approach for secret data hiding specifically text based on MSB using two encryption algorithms (Blowfish and AES). The security weakness of data hiding based on MSB approach using Blowfish algorithm only was addressed which was solved by using a random

V. CONCLUSION

This research work presented a novel Image steganography technique based on MSB (Most Significant Bit) using AES and Blow fish encryption algorithms termed as H-MSB because it combined the use of AES and Blowfish. The proposed approach hide secret text message within the MSB bits of cover image, there by addressing weakness of MSB algorithm based on Blowfish algorithm only by means of applying Random function in selecting image pixels thereby utilizing a mask as password decryption Key. Future directions should look in to integrating machine learning and Artificial intelligence to enhance the security against Steganalysis and robust attacks.

REFERENCES

[1] Saini, R.; Joshi, K.; Punyani, K.; Yadav, R.; Nandal, R.; Kumari, D. Interpolated Implicit Pixel-based Novel Hybrid Recent Patents Electronics Electron. Eng., 16, 851–871, 2023.

[2] Anthoniraj, S.; Karthikeyan, P.; Vivek, V. Weed Detection Model Using the Generative Adversarial Network and Deep Convolutional Neural Network. J. Mob. Multimedia, 18, 275–292, 2022).

[3] Belagali, P.; Udupi, V. Robust Image Steganography Based on Hybrid Edge Detection. Tuijin Jishu/J. Propuls. Technol. 2023, 44, 1509–1521. Appl. Sci. 2023, 13, 11771 19 of

[4] Nasution, R.I.H.; Fauzi, A.; Khair, H. Hybrid Cryptosystem Algorithm Vigenere Cipher and Base64 for Text Message Security Utilizing Least Significant Bit (LSB) Steganography as Insert into Image. J. Artif. Intell. Eng. Appl. (JAIEA) 2023, 2, 89–98

selection of pixels and attach as a password encryption Key and addition AES algorithm. Future directions are recommended to improve this approach by integrating artificial intelligence and machine learning futures for advancement of encryption algorithms.

[5] Velliangiri, S; Manoharn, R; Ramachandran, S.; Venkatesan, K.; Rajasekar, V.; Karthikeyan, P.; Kumar, P.; Kumar, A.; Dhanabalan, S.S. An efficient lightweight privacy- preserving mechanism for industry 4.0 based on elliptic curve cryptography. IEEE Trans. Ind. Inform., 2021, 18, 6494–6502.

[6] Oswal, D.; Parmar, G.; Patidar, H.K.; Badbadwal, K.; Shukla, P. Secure File Using Steganography 2022.

[7] Ron Shmueli, Divya Mishra, Tal Shmueli and Ofer Hadar, A novel technique for image steganography based on maximum energy seam. Multimedia Tools and Applications <https://doi.org/10.1007/s11042-024-18476-6>

[8] Alade O.M, Amusan E.A, Adedeji O.T and Alo O.O: Image steganography using Pixel Value differencing (PVD) based on Firefly Algorithm. Journal Scientific Research & Reports, 2021 27(7): 80- 86

[9] Rejani, Murugan and Deepu Comparative Study of Spatial Domain Image Steganography Techniques. Int. J. Advanced Networking and Application Volume: 07 Issue: 02, 2015.

[10] N. Johnson and S. Jajodia, Steganalysis of images created using current steganography software," 1998. pp. 273-289.

[11] Rajasekar, V.; Premalatha, J.; Dhanaraj, R.K.; Geman, O. Introduction to Classical Cryptography. In Quantum Blockchain: An Emerging Cryptographic Paradigm; John Wiley & Sons, Inc.: Hoboken, NJ, USA, 2022; pp. 1–29.

[12] Aumasson, J.P. Crypto Dictionary: 500 Tasty Tidbits for the Curious Cryptographer; No Starch Press: San Francisco, CA, USA , 2021.

[13] SaadAlmutairi,S.Manimurugan,M.A. Anewsecuretransmissionschemebetween senders and receivers usingHVCHCwithout any loss. EURASIP J. Wirel. Commun. Netw. 2019, 2019, 1–15

- [14] May Alanzy , Razan Alomrani , Bashayer Alqarni and Saad Almutairi. Image Steganography Using LSB and Hybrid Encryption Algorithms. Appl. Sci. 2023, 13, 11771. <https://doi.org/10.3390/app132111771>
- [15] Semenchenko, O.; Iakovenko, O.; Lekakh, A.; Parkhomenko, M.; Podlesny, S.; Karaban, O. The Analysis of the Codes in the Textual Steganography Technologies. In Proceedings of the 2021 IEEE 3rd International Conference on Advanced Trends in Information Theory (ATIT), Kyiv, Ukraine, 15–17 December 2021; pp. 31–35.
- [16] Pandey, D.; Wairya, S.; Al Mahdawi, R.S.; Najim, S.A.D.M.; Khalaf, H.A.; Al Barzinji, S.M.; Obaid, A.J. Secret data transmission using advanced steganography and image compression. Int. J. Nonlinear Anal. Appl. 2021, 12, 1243–1257
- [17] Solomon O.Akinola and Adebanye A.Olatidoye On the image quality and encoding times of lsb, msb and combined lsb-msb steganography algorithms using digital images. International Journal of Computer Science & Information Technology (IJCSIT) Vol 7, No 4, August 2015. PP 79-91.
- [18] kauthar Kabir: Image Steganography method using protected text hiding scheme (PTHS). International Multi-Conference on ICT applications, October 27th to 30th, 2024.