Available online at www.qu.edu.iq/journalcm
JOURNAL OF AL-QADISIYAH FOR COMPUTER SCIENCE AND MATHEMATICS
ISSN:2521-3504(online) ISSN:2074-0204(print)

Review on various image protection methods

Ekhlas Ghaleb Abdulkadhim [a] ***, Sanaa Hammad Dhahi*** [b] ***, Meeras Salman Al-Shemarry*** [c]

[a]*College of Tourism Science , University of Kerbala, Kerbala 5006, Iraq.Email:ekhlas.g@uokerbala.edu.iq*
[b]*College of Tourism Science , University of Kerbala, Kerbala 5006, Iraq.Email: sanaa.h@uokerbala.edu.iq*
[c]*College of Computer Science and Information Technology, University of Kerbala, Kerbala 5006, Iraq.Email:Meeras.s@uokerbala.edu.iq*

ARTICLE INFO

Article history:
Received: 12 /10/2023
Rrevised form: 19 /12/2023
Accepted : 27 /12/2023
Available online: 30 /12/2023

Keywords:

Steganography
Cryptography
Information Hiding
Data Protection
Hiding Techniques

ABSTRACT

The security of information exchange over email and other web-based means is rather low, and there is the risk of interception when it comes to confidential information (e.g., credit card info). Therefore, online users should be ensured of the security and privacy of their web interactions. Despite the remarkable benefits of the Internet in the modern era and its contribution to digital communication, the information security of open networks has become an important issue due to its heavy costs. Several approaches have been used to address this issue, particularly through information hiding and encryption in system security strategies. Cryptography is the process of information encryption, and steganography refers to information hiding. These methods have proven quite effective in maintaining information security. Cryptography involves making changes to confidential information, which prevents their readability by eavesdroppers, which could also be considered a technique of original text to cipher text. On the other hand, steganography entirely hides confidential information from unauthorized users using multiple carrier formats, including audio, video, protocol, and images. Given the availability of digital images, they are often employed as carrier files online. Other approaches to image steganography are also common and have specific limitations and advantages. The present study aimed to review different methods of image cryptography and steganography and compare the studies in this regard so as to determine which the best, specific and accurate methods of information security.

MSC..

https://doi.org/ *10.29304/jqcsm.2023.15.41364*

1. Introduction

Information security on the internet could be supported by various methods, and the most common approaches in this regard are cryptography and steganography [1]. In steganography, confidential messages could be concealed via digital media, which prevents the detection of the information. As a result, the exchange of confidential messages would be possible by images without changing the structure of the delivered data; this is because the data are concealed within a media and have become invisible. On the other hand, cryptography involves hiding secret messages from unauthorized users by altering their connotation [2]. Data encoding systems and their confidentiality are the backbone of steganography as the steganography system could only be recognized and tracked when the encoding system is confirmed. Steganography allows incognito communication exchange via digital media, which is not visible by the sender or the receiver of the messages. As for cryptography, information integrity becomes incomprehensible, so that no other user than the receiver and sender could be understand the meaning of this information. In terms of Cryptography, this mathematical method addresses data authenticity,

∗Corresponding author Ekhlas Ghaleb Abdulkadhim

Email addresses: ekhlas.g@uokerbala.edu.iq

Communicated by 'sub etitor'

data integrity, and entity authenticity [4]. To benefit from the combined form of the mentioned methods, further investigation is required so as to determine their advantages and limitations.

NOMENCLATURE

Aradius of
Bposition of
Cfurther nomenclature continues down the page inside the text box

1.1. Steganography

Steganography was first denoted in a message sent by Herodotus to the Greek nation. In addition, steganography was used as a means of communication security by USSR and US in the Cold War. Today, confidentiality is ensured by using multiple algorithms and media carriers. Basically, steganography embeds confidential data to be visible only by the sender and the receiver, and the contents of the message are concealed in a stego object file, which is delivered to the receiver who subsequently extracts the algorithm to retrieve the hidden information (Figure 1) [5]. Figure 1 depicts the general process of steganography.

In general, a steganography model is composed of the following:

1. Media carrier, also known as the cover image/cover object, which contains the confidential information in the form of a message.
2. Secret data, which refers to the hidden message (e.g., data, file, image).
3. Secret key, which encodes or decodes the hidden message.
4. Stego media (Y), also known as the stego object, which is developed by embedding the confidential information (i.e., message).

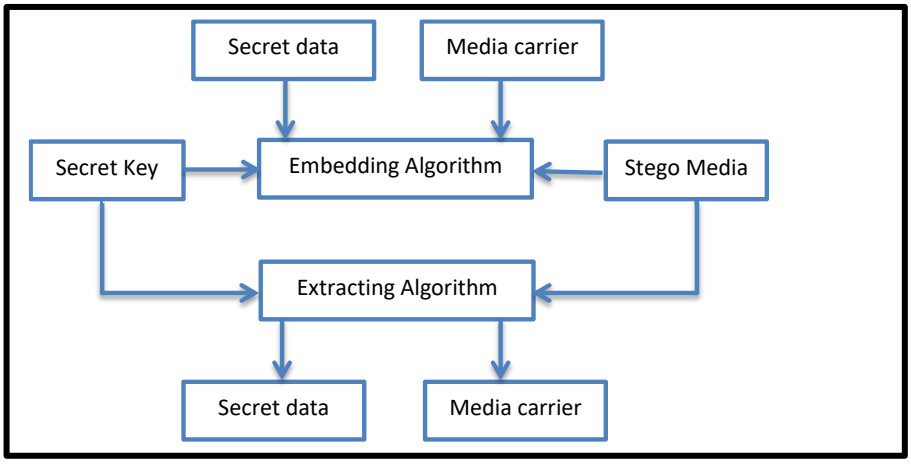

Fig. 1. Block diagram of Steganography Process

1.1.1. Different Types of Steganography

Steganography has no limitation when it comes to digital file formats, while the highest efficiency has been reported with digital images given their high availability. In general, four file formats are applicable to steganography (Figure 2), which have been discussed below:

1. Image steganography: The cover object used in steganography is mainly selected from digital images. The digital image containing the embedded message is formed based on an algorithm using a secret key, which generates the stego image. In addition, the confidential information is concealed by pixel intensities [6].

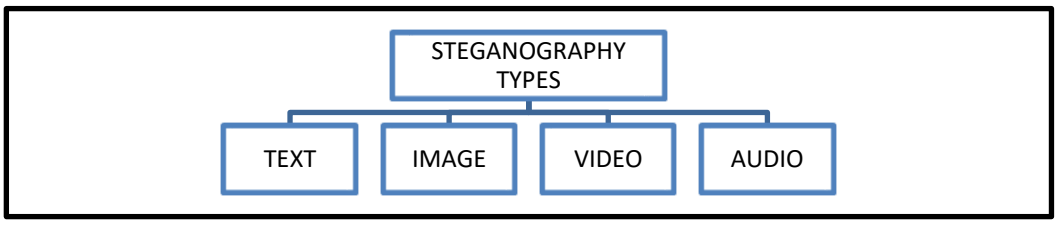

Fig. 2. Steganography types

2. Video steganography: In this technique, a confidential message is embedded into a video file, which contains a set of images and audio. Notably, images and audio are implementable onto video files. Video steganography is preferable over other multimedia files owing to its capacity to contain large volumes of data, which could be inserted and concealed within a video and remain unnoticed by users due to the continuous information flow. Several video files are applicable for video steganography, including H.264, Mp4, MPEG, and AVI[7].
3. Text steganography: In this technique, confidential data are stored into a text file. Some of the advantages of this method are that only limited storage is required for the message, and the method allows for the use of numerous formats. Message hiding is performed by tabs capital letters and the number of white spaces. However, text files containing large volumes of extra information could not be incorporated into text steganography [8].
4. Protocol steganography: TCP, UDP, ICMP, and IP network protocols are utilized to embed confidential data in this method, while the protocol acts as the carrier as well. The main components of the network packet are user data, packet headers, and packet trailers, which allow for the use of some network model layers in the steganography process, which is overall referred to as protocol steganography [9].

1.1.2. Steganographic Techniques

In general, steganographic image embedding could be performed by two approaches, which are selected based on the type of the image and hosting space [10]. These approaches are transform domain techniques and spatial domain techniques (Figure 3).

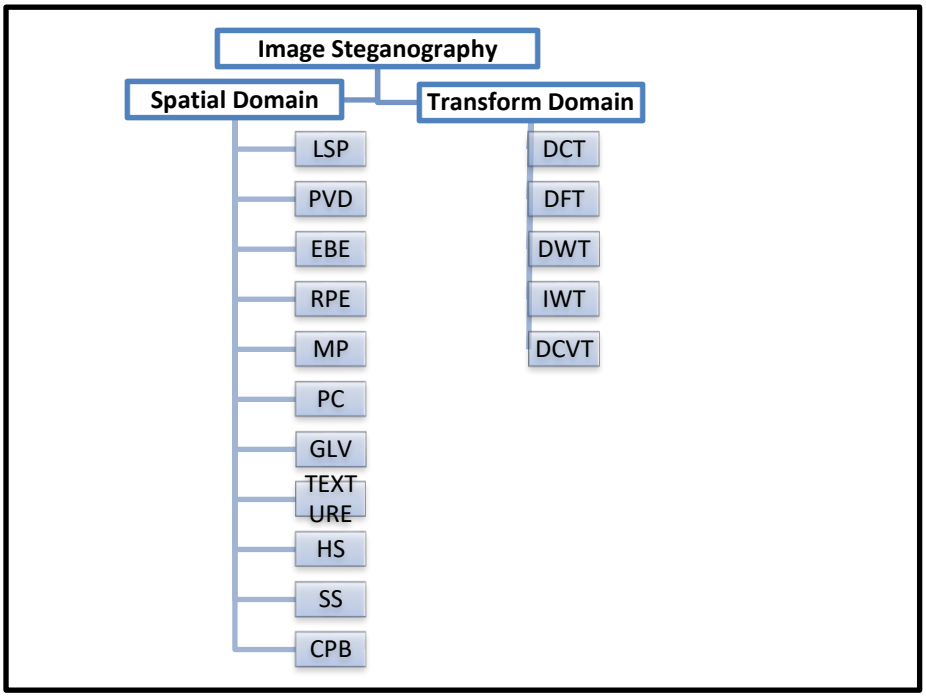

Fig. 3. Classification of Image Steganography Techniques

1.2. Cryptography

In cryptography, confidential messages are made in writing, and the encoded message is extracted by encryption and deciphering. This method is most effective in case of communication should occur over a medium with poor security, which is prone to eavesdropping (Figure 4). According to Gollmann , cryptography is a set of wide-ranging methods, which are implemented within decryption and encryption frameworks, and the secondary frameworks are digital signature and integrity check function. The encryption framework is used when the secret information should be converted into an illegible format for unauthorized users. As for the decryption framework, an authorized user would be allowed to decode the hidden message. The integrity check function provides the cryptographic hash function [11], which mathematically detects small data volumes for the specific identification of large digital objects. These objects have varied hash function values, and no object could be with the same hash value in terms of computation . The integrity of messages after delivery could be determined based on hash functions. Furthermore, message authentication codes are used for integrity check function. These codes are obtained from two inputs, which are the cryptographic secret key and transmitted message. In addition, message authentication codes could check post-transmission message integrity. Digital signature algorithms could be applied to detect the changes in messages that have been made by invaders in interactions, and the principles are similar to those of asymmetric encryption [12].

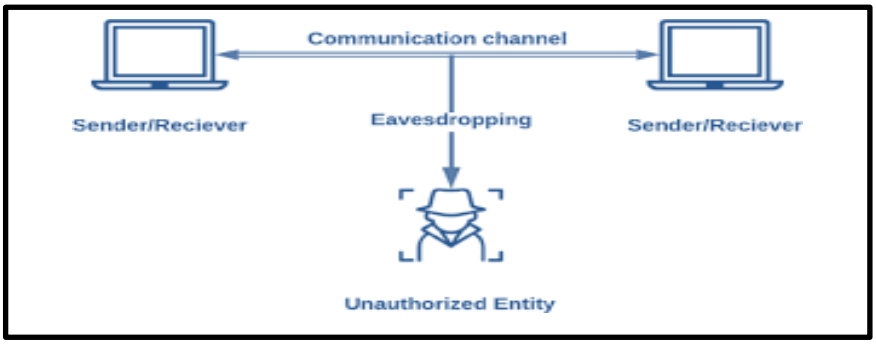

Fig 4. A basic pictorial of the encryption system

1.2.1. Cryptography Applications

The main application of cryptographic encryption is to protect confidential data against unwanted changes through encrypting the stored data to increase communication security [13]. If an eavesdropper manages to intercept an encrypted message, the attacker will not benefit as the message cannot be decrypted even in case of authorization.

1.2.2. Encryption Algorithms and the Cryptographic Key

In 1883, Auguste Kerckhoff proposed the primary standards of cryptographic engineering for the first time . These standards dictate that although encryption could be disclosed publicly, message decryption is only possible through using the cryptographic key . The cryptographic key is equally important in encryption and decryption since these processes would not be effective without the key despite the recognition of the encryption algorithm. Based on the algorithm key, symmetric encryption algorithms (SEAs) and asymmetric encryption algorithms are considered to be the two main categories of modern encryption frameworks. Secret key encryption (SKE) is another term used to refer to SEAs[14]. For SKE to function properly in encryption and decryption, the sender and receiver of the message must have access to a shared secret key (Figure 5).

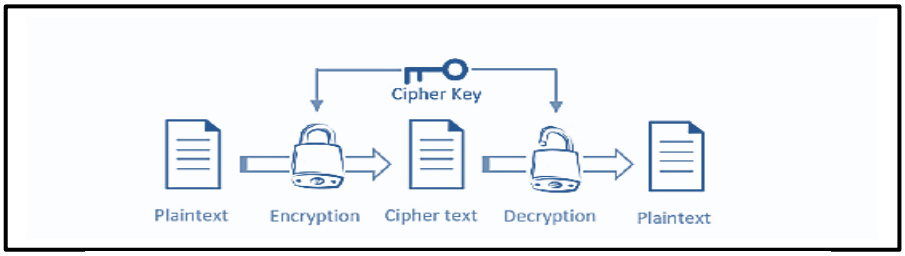

Fig. 5. A simple symmetric encryption framework

Figure 5 depicts a simple symmetric encryption framework. Asymmetric encryption algorithms (AES) are also known as public key encryption. In AES, two keys should be accessible to the sender and receiver of the message, one of which is public and the other is private (Figure 6). As such, information security could be guaranteed in case unsafe communication occurs via unreliable media [15].

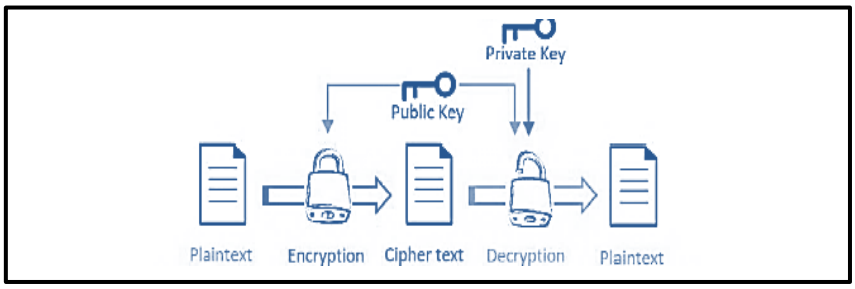

Fig. 6. Basic pictorial of symmetric encryption

Cryptographic techniques must primarily ensure message confidentiality so as to be efficient as a means of communication security, which requires encryption algorithms. Data security is often achieved by private keys in AES and SEA [15]. The length of these secret keys plays a pivotal role in ensuring information security. After sending a message, the receiver and sender should employ cryptographic hash functions to confirm the integrity of the message while it is being delivered as the message might be changed purposefully or accidentally during the delivery process. Furthermore, digital signature schemes could be applied to guarantee message authenticity or nonrepudiation support [15]. AES and digital encryption schemes have common rules as they require a private key for message encryption, while the encrypted message is the signature as only a specific private key could decrypt the message. According to ISO 7498-2, the main security services provided by cryptography are data integrity, confidentiality, non-repudiation, authentication, and identification. There is ongoing research regarding cryptography since the issue associated with this technology should be partly addressed by comparative measures.

2. Literature Review

In the method introduced by Subhash Panwar et al. [16], modified LSB and AES algorithms are employed for digital image steganography. According to the authors, better outcomes could be obtained by the AES since despite image detection, the message contents cannot be deciphered. In addition, the modified LSB technique is also highly efficient in the security maintenance of the image contents. Similarly, the steganography method of Aishwarya Pandey et al. [17] is primarily based on the AES and LSB, which is considered to be an innovative approach to concealing confidential data when used in the combined form. In this method, the users choose the quality of the image, and the message length is determined correspondingly. This allows the free choice of wide-ranging image size outputs by the users depending on their needs. Moreover, a new steganography technique has been proposed by Namrata Singh et al. [18], which is employed for high peak signal-to-noise ratio (PSNR)-based image steganography (e.g., DCT, SVD, and LWT). The PSNR and mean square error (MSE) values could enhance the function of this approach as well. Another LSB-based technique has been introduced by Aung Myint Aye et al. [19] for steganography, which also exploits novel extraction and embedding methods. In this approach, confidential data are embedded in a cover image file, and the selection of the embedded pixel occurs simultaneously based on the public shared key of the message receiver and sender. The method described by Ashish et al. [20] is used for data embedding within cryptographic and steganographic frameworks, and message encryption/decryption is achieved by the AES algorithm. In addition, the DWT algorithm is applied for the embedding and extraction of the obtained message via the AES algorithm in the previous stage. Finally, the message is sent to the receiver in the form of a stego image. Another method has been presented by Vikas et al. [21], which is a hybrid approach to text/image steganography based on the LSB and AES algorithms. In this method, security risk could be diminished in the transfer of confidential data on the internet. Another technique of image steganography has been described by Pravin B. Desai et al. [22] based on the LSB algorithm, which is reported to sustain high security and performance. Similarly, the LSB-based method of Naveen Verma et al. [23] is applied for steganography, as a result of which image security improves along with the confidential message. The security is ensured by selecting random keys, which are used for the extraction of the confidential content of the message. Furthermore, the method has been shown to enhance the MSE and PSNR values. An LSB-based hybrid domain has been proposed by K. B. Shiva Kumar et al. [24] for steganography, which has been reported to have a higher PSNR and more efficient security compared to other methods. On the other hand, the cryptography technique introduced by Pooja Rani et al. [25] involves image steganography, which renders secret message contents unclear to unauthorized users. As mentioned earlier, the basis of steganography is to conceal data through their embedding into a different cover medium. Moreover, an MSB-based image steganography technique has been described by Ammad Ul Islam et al. [26], which functions through bit differencing. By

utilizing MSB bits, the technique increases security in case of unauthorized access. Souvik Kumar et al. [27] also introduced a data hiding method based on image steganography, which encompasses DNA sequence arithmetic and LSB insertion to conceal two confidential images within a cover image.

3. Analysis and Discussion

A combination of steganography and cryptography could lead to obtaining an effective stego image with a higher power and security against invasions. Previous studies have mainly evaluated different stenographic methods, particularly image steganography. According to the findings, these methods could all ensure data security through embedding the data. However, some of the incorporated algorithms have an extremely high time complexity and extremely low data storage capability within images. Therefore, further investigations are required to develop steganography or cryptography procedures with higher accuracy and capability through combining the current methods or their upgrade. In the present study, various steganography and cryptographic were reviewed in the previous studies and evaluated in terms of their ability in embedding actual information and their protection against insecure interactions. Although different carrier file types are considered applicable, digital images have proven superior owing to their availability and large number of users over the internet. Numerous stenographic techniques could be employed to conceal confidential data within images, which have varied complexities, strengths, and limitations (Table 1) [28].

Table 1. Comparative Analysis For Various Methods

S.N	Research Name	Domains	Methods	Weakness/strength
1	Digital Image Steganography Using Modified LSB and AES Cryptography[16]	Spatial	LSB and AES Cryptography	High performance PSNR value is Medium
2	Steganography using AES and LSB techniques[17]	Spatial	LSB and AES Cryptography	High Performance PSNR value is High
3	High PSNR based Image Steganography[18]	Transform	DCT	Medium steganography Performance PSNR value is Medium
4	LSB Based steganography for Information Security System[19]	Spatial	LSB steganography	High Performance PSNR value is High
5	Data Imbedding using Image Steganography[20]	Transform	DWT and AES Cryptography	Low steganography Performance PSNR value is Low
6	Hybrid Approach to Text & Image Steganography using AES and LSB techniques[21]	Spatial	LSB and AES Cryptography	High Performance PSNR value is High
7	Image Steganography Using LSB Algorithm[22]	Spatial	LSB Steganography	High performance PSNR value High
8	LSB Based Stegnography to Enhance the Security of an Image[23]	Spatial	LSB Steganography	High performance PSNR value High
9	Hybrid Domain in LSB Steganography[24]	Spatial	LSB and AES Cryptography	High performance PSNR value High
10	Cryptography Using Image Steganography[25]	Spatial	LSB Steganography	High performance PSNR value High
11	An Improved Image Steganography Technique based on MSB using Bit Differencing[26]	Spatial	MSB Steganography	High performance PSNR value High
12	Data Hiding by Image Steganography Applying DNA Sequence Arithmetic & LSB Insertion[27]	Spatial	LSB Steganography	High performance PSNR value High

4. Conclusion

In this study, various methods have been reviewed which are used for image stenography and cryptography. Data hiding covers a wide range of concepts and issues and has currently attracted the attention of researchers. As a result, steganography has become a method of choice for maintaining data confidentiality and information hiding within network interactions. In this article, an overview has been provided of the currently used image steganography methods within the spatial domain, focusing on the strengths and limitations of each technique. While some of these methods are considered superior in terms of image quality, others have shown higher efficiency in their data hiding capacity and information security. Therefore, it is recommended that researchers address the discussed techniques of steganography in the future in more detail and further expand our findings in this regard.

References

[1] Rakhra, Manik, Rajan Kumar, and Himdweep Walia. "A Review on Data hiding using Steganography and Cryptography." 2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO). IEEE, 2021.
[2] Hureib, Eshraq S., and Adnan A. Gutub. "Enhancing medical data security via combining elliptic curve cryptography and image steganography." Int. J. Comput. Sci. Netw. Secur.(IJCSNS) 20.8 (2020): 1-8.
[3] MAHMOOD, ALI SHAKIR, MOHD RAHIM, and MOHD SHAFRY. "GENERATING AND EXPANDING OF AN ENCRYPTION KEY BASED ON KNIGHT TOUR PROBLEM." Journal of Theoretical & Applied Information Technology 95.7 (2017).
[4] Kumar, Manish, et al. "Enhanced digital image and text data security using hybrid model of LSB steganography and AES cryptography technique." 2022 Second international conference on artificial intelligence and smart energy (ICAIS). IEEE, 2022.
[5] Chavali, Surya Teja, et al. "Comparative Study of Image Encryption and Image Steganography Using Cryptographic Algorithms and Image Evaluation Metrics." Semantic Intelligence: Select Proceedings of ISIC 2022. Singapore: Springer Nature Singapore, 2023. 297-311.
[6] Varsha, Rajender Singh Chhillar, "Data Hiding Using Steganography and Cryptography", International Journal of Computer Science and Mobile Computing, Vol. 4, Issue. 4, pg.802 – 805, April 2015.
[7] Suryawanshi, Govind R., and Suresh N. Mali. "Analysis of Effect of Spatial Domain Steganography Technique on DCT Domain using Statistical Features for Digital Images." International Journal of Applied Engineering Research 13.1 (2018): 634-640.
[8] Rejani, R., D. Murugan, and Deepu V. Krishnan. "Digital data protection using steganography." ICTACT J. Commun. Technol 7.1 (2016): 1245-1254.
[9] Survase, Poonam, and P. Survase. "Qr code based image steganography with enhanced image quality and compression." International Journal for Innovative Research in Science and Technology 2.5 (2015): 104-112.
[10] Dehare, Praneeta, and Padma Bonde. "Hiding image in image by using FMM with LSB substitution in image steganography." International Journal of Advance Research in Computer Science and Management Studies 2.11 (2014): 455-458.
[11] Naoum, Reyadh Shaker. Image Steganography Based on Discrete Wavelet Transform and Enhancing Resilient Backpropogation Neural Network. Diss. Middle East University, 2015.
[12] HASHIM, MOHAMMED MAHDI, MOHD RAHIM, MOHD SHAFRY. "IMAGE STEGANOGRAPHY BASED ON ODD/EVEN PIXELS DISTRIBUTION SCHEME AND TWO PARAMETERS RANDOM FUNCTION." Journal of Theoretical & Applied Information Technology 95.19 (2017).
[13] MAHMOOD, ALI SHAKIR, MOHD RAHIM, and MOHD SHAFRY. "GENERATING AND EXPANDING OF AN ENCRYPTION KEY BASED ON KNIGHT TOUR PROBLEM." Journal of Theoretical & Applied Information Technology 95.7 (2017).
[14] Taha, Mustafa Sabah, et al. "Combination of steganography and cryptography: A short survey." IOP conference series: materials science and engineering. Vol. 518. No. 5. IOP Publishing, 2019.
[15] Raj, UA Solomon, and C. P. Maheswaran. "Secure File Sharing System Using Image Steganography and Cryptography Techniques." 2023 International Conference on Inventive Computation Technologies (ICICT). IEEE, 2023.
[16] Subhash Panwar, Shreenidhi D amani, " Digital Image Steganography Using Modified LSB and AES Cryptography", International Journal of Recent Engineering Research and Development (IJRERD), Volume 03 – Issue 06, Pg. 18-27, June 2018.
[17] Aishwarya Pandey, Jharna Chopra, "Steganography Using AES and LSB Techniques", International Journal of Scientific Research Engineering & Technology (IJSRET), Volume 6, Issue 6, Pg: June 2017620-623.
[18] Namrata Singh, "International Journal of Advanced Engineering Research and Science (IJAERS)", Vol-6, Issue-1,Pg: 109-115 Jan- 2019.
[19] Aung Myint Aye, LSB Based Image Steganography for Information Security System, International Journal of Trend in Scientific Research and Development (IJTSRD), Volume - 3 Issue – 1,PP: 394-400 Nov – Dec 2018.
[20] Ashish S, Manjunath P, K S Prateek, "Data Embedding using Image Steganography", International Research Journal of Engineering and Technology (IRJET), Volume: 06 Issue: 05 ,PP: 1356-1359May 2019. [21] Vikas M, Yashwanth E, " Hybrid Approach to Text & Image Steganography using AES and LSB Technique", International Research Journal of Engineering and Technology (IRJET), Volume: 05 Issue: 04 , Pg:1500-1502 Apr-2018.
[22] Pravin B. Desai, Pradip S. Bhendwade," Image Steganography Using LSB Algorithm", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineerin, Vol. 5, Issue 8, PP: 6883-6890 August 2016.
[23] Naveen Verma, Preeti Sondhi," LSB Based Stegnography to Enhance the Security of an Image", International Journal of Trend in Scientific Research and Development (IJTSRD), Volume: 3, Issue: 4 , PP: 1480-1484 May-Jun 2019.
[24] K B Shiva Kumar, K B Raja, Sabyasachi Pattnaik, "Hybrid Domain in LSB Steganography", International Journal of Computer Applications , Volume 19– No.7, pg: 36-40, April 2011.
[25] Pooja Rani, Preeti Sharma, "Cryptography Using Image Steganography",International Journal of Computer Science and Mobile Computing, Vol. 5, Issue. 7, pg.451 – 456, July 2016.
[26] Ammad Ul Islam, Faiza Khalid, "An Improved Image Steganography Technique based on MSB using Bit Differencing", International conference on innovative computing techninology, Pg: 265-269, 2016.
[27] Souvik Kumar, Kuntal Ghosh, "Data Hiding by Image Steganography Applying DNA Sequence Arithmetic & LSB Insertion", Journal for Research Volume 02, Issue 04 , pg: 49-57,June 2016.
[28] Suresh, Arul, and R. Balasubramanian. "A Systematic Review on Spatial Domain Steganography & Cryptography Techniques." Turkish Online Journal of Qualitative Inquiry 12.6 (2021).