A Project Report on

A CROPPING-RESISTANT APPROACH TO IMAGE STEGANOGRAPHY

By

Rentala Sai Joshika - 21BCE5159

Pulaparthi Penchala Deepthi Sri – 21BCE5464

G. Tanmayi - 21BCE5976

Ambati Bala Venkata Naga Sri Sai - 21BCE6062

A Project Report submitted to

Dr. Balasaraswathi V R

SCHOOL OF COMPUTER SCIENCE AND ENGINEERING

In partial fulfillment of the requirements of the course of

BCSE309L – Cryptography & Network Security

in

B.tech COMPUTER SCIENCE & ENGINEERING

Vandalur – Kelambakkam Road

Chennai – 600127

APRIL – 2024

ACKNOWLEDGEMENT

We wish to express our sincere thanks and deep sense of gratitude to our project guide, Dr. Balasarawathi V R , Professor Higher Academic Grade, School of Computer Science Engineering, for her consistent encouragement and valuable guidance offered to us in a pleasant manner throughout the course of the project work.

We also take this opportunity to thank all the faculty and staff of the school for their support and their wisdom imparted to us throughout the course.

We thank our parents, family, and friends for bearing with us throughout the course of our project and for the opportunity they provided us in undergoing this course in such a prestigious institution.

TABLE OF CONTENTS

S.NO	TITLE	PAGE.NO.
1	ACKNOWLEDGEMENT	2
2	ABSTRACT	4
3	INTRODUCTION	5
4	LITERATURE SURVEY	6 - 13
5	MODULE DESCRIPTION	14 - 15
6	IMPLEMENTATION	16 - 18
7	RESULT	19 - 20
8	IMPLEMENTATION(Details)	21 - 23
	8. i) LSB	21
	8. ii) CEPP	22
9	PROPOSED SOLUTION	24
10	DISCUSSION	25 - 26
11	CONCLUSION	27
12	REFERENCES	28

ABSTRACT

Image steganography is a covert communication technique that involves concealing secret information within digital images. This project explores various steganographic methods, their implementations, and their applications. A comprehensive literature survey provides insights into recent advancements in image steganography, including techniques such as LSB insertion, randomization, hybrid methods, and deep learning-based approaches.

The project comprises several modules, including encoding, decoding, stego□key management, steganalysis (optional), and security countermeasures. Each module serves a specific purpose in the process of hiding and retrieving hidden messages from images while ensuring security and robustness against detection.

The implementation section presents a Python-based approach for hiding and retrieving messages within images using LSB insertion. This method involves modifying the least significant bit of pixel values to embed binary data, achieving a balance between imperceptibility and data capacity.

Overall, this project aims to contribute to the understanding and practical application of image steganography, highlighting its importance in secure communication and exploring avenues for further research and development.

Keywords:
Steganography, Stego-key management, Steganalysis, Imperceptibility

INTRODUCTION

Image steganography is a fascinating field that involves the concealment of secret information within digital images. It is a technique that has been employed for centuries, evolving from ancient methods of hiding messages in plain sight to the modern digital era. Steganography provides a covert means of communication by embedding information within the pixels of an image, making it imperceptible to the human eye.

In today's interconnected world, where the transmission and sharing of digital media are ubiquitous, image steganography plays a crucial role in ensuring the privacy and security of sensitive information. By exploiting the redundancy and complexity of image data, steganographic techniques enable the seamless integration of hidden messages, files, or even entire documents into seemingly innocent images.

This project aims to explore the principles, algorithms, and applications of image steganography. By delving into various steganographic methods and analysing their strengths and weaknesses, we can gain a deeper understanding of this intriguing discipline. Furthermore, we will examine the challenges posed by steganalysis—the process of detecting hidden messages—and explore countermeasures to enhance the security of steganographic systems.

In this project, we will uncover the secrets hidden within images and unveil the intricacies of image steganography, unlocking its potential in the realm of secure communication.

LITERATURE SURVEY

1)LSB Insertion with Secret Key for Steganography in Images:

This approach discusses a steganographic technique called Least Significant Bit (LSB) insertion for hiding data within an image. The technique involves overlaying binary bits of hidden information onto the LSB of the pixels in the cover image. The quality of the resulting stego image is measured using the Peak Signal-to-Noise Ratio (PSNR), which quantifies the distortion or loss of quality between the cover and stego images.

The proposed method in the paper introduces a secret key to protect the hidden information. The key is converted into a one-dimensional circular array bit stream, and the LSBs of each byte in the cover image are overwritten with the hidden information and secret key.

The review emphasizes that a larger PSNR value indicates better image quality and a lower likelihood of visual detection by the human eye. The conclusion drawn is that the proposed method successfully embeds hidden information into the cover image, providing a stego image that appears visually similar to the original cover image while containing the concealed data.

S. M. Masud Karim, Md. Saifur Rahman, Md. Ismail Hossain Computer Science and Engineering Discipline Khulna University, Khulna 9208, Bangladesh.

2) A Secure Keyless Image Steganography Approach for Lossless RGB Images

A heuristic approach for information hiding in the form of multimedia objects or text using steganography is proposed in keeping in mind – size and degree of security. A robust image steganography technique based on LSB insertion and RSA encryption technique is proposed in. The approach increases the quality of an image by assigning a rank dependent on how much of LSB bits need to change, but this approach cannot hide a large amount of information. Also, this approach requires a huge collection of images to get a better rank. In the least significant bit (LSB) of each pixel is modified sequentially in the scan lines across the image in raw image format with the binary data. In the authors have proposed a steganographic technique by mixing with it cryptography to increase the security layer. The problem here is that both the cover image and stego image needs to be sent to retrieve the message, which might compromise security.

Sankar Roy, Ranjan Parekh; School of Education Technology Jadavpur University Kolkata, India

3) Secure RGB Image Steganography Based on Randomization

Triple-A concealment technique is introduced as a new method to hide digital data inside image-based medium. The algorithm adds more randomization by using two different seeds generated from a user-chosen key in order to select the component(s) used to hide the secret bits as well as the number of the bits used inside the RGB image component. This randomization adds more security especially if an active encryption technique is used such as AES. The capacity ratio is increased above SCC and pixel indicator scheme. Triple-A has a capacity ratio of 14% and can be increased if a greater number of bits is used inside the component(s). As a final note, we can say that SCC algorithm is a special case of Triple-A algorithm if the number of bit used is fixed and equal 1 and Seed2 is restricted to [0,2] with circular effect.

Adnan Gutub, Mahmoud Ankeer, Muhammad Abu-Ghalioun, Abdulrahman Shaheen, and Aleem Alvi, "Pixel Indicator high capacity Technique for RGB image Based Steganography", WoSPA 2008 – 5th IEEE International Workshop on Signal Processing and its Applications, University of Sharjah, Sharjah, U.A.E. 18 – 20 March 2008.

4) Hybrid image steganography method using Lempel Ziv Welch and genetic algorithms for hiding confidential data

This paper presents a hybrid steganography method that combines Haar Discrete Wavelet Transform, Lempel Ziv Welch algorithm, Genetic Algorithm, and the Optimal Pixel Adjustment Process. The aim of the method is to enhance the quality and security of stego images while increasing the capacity for hidden data.

By utilizing the Haar Discrete Wavelet Transform, the stego image is made more robust against attacks. The Lempel Ziv Welch algorithm ensures efficient compression and encoding of the secret message, enhancing both capacity and security. The Genetic Algorithm optimizes the mapping function for each block in the image, further improving the quality and effectiveness of the steganographic process.

Experimental evaluations using standard images and different types of secret messages demonstrate that the proposed method outperforms existing techniques in terms of visual quality and capacity for embedded data. The information-hiding capacity reached 50% with a high Peak Signal-to-Noise Ratio (PSNR) of 52.83 dB.

Overall, the hybrid image steganography method presented in this paper offers a promising approach for achieving high-quality stego images with increased data hiding capacity and security, surpassing the capabilities of current state-of-the-art methods.

A.H.M. Almawgani, Ayman Taher Hindi, Waled Hussein Al-Arashi, A. Y. Al-Ashwal Multidimensional Systems and Signal ProcessingVolume 33Issue 2Jun 2022pp 561–578https://doi.org/10.1007/s11045-021-00793-w

5) Blockchain-based secure data sharing scheme using image steganography and encryption techniques for telemedicine applications

Telemedicine is an alternate way to the conventional delivery of healthcare services. Timely communication of the patient records in a secure and private way is essential for telemedicine services, where the poor secrecy affects the quality of the services to a certain extent. Presently, the advent of Blockchain technologies has attracted several researchers to achieve secure data sharing. In this way, this chapter designs a new Blockchain-based secure data-sharing scheme (BBSDSS) using image steganography and encryption techniques for telemedicine applications. The BBSDSS model involves three stage processes namely image steganography, encryption, and secure data sharing. Initially, glowworm swarm optimization algorithm is applied for the image steganography process. The presented model includes signcryption technique for encrypting the stego image. Finally, the Blockchain technique is applied to enable secure sharing of the patient details. Extensive experimental analysis was taken place and the results are examined in terms of distinct aspects. The simulation values denoted that the presented algorithm has resulted in a higher peak signal to noise ratio (PSNR) of 51.75dB, 51.75dB, 51.75dB, and 51.75dB on the applied images 1–4, respectively.

Irina V. Pustokhina, Denis A. Pustokhin, K. Shankar Department of Entrepreneurship and Logistics, Plekhanov Russian University of Economics, Moscow, Russia Department of Logistics, State University of Management, Moscow, Russia Federal University of Piauí, Teresina, Brazil.

6) 3-Level security based spread spectrum image steganography with enhanced peak signal to noise ratio

This research elucidates a method of enhancing peak signal to noise ratio and minimizing mean square error through spread spectrum image steganography. The centre of focus is more onto security, for that three levels of security have been designed which are as follows: First level indicates security of hidden text inside cover media by RSA Encryption with Diffie-Hellman Key exchange

algorithm, second level of security is maintained by compressing the data to be hidden using Run-length Encoding (a lossless compression). Further the communication is kept more secured by spreading the message all over the pixels of cover media using pseudo random generator that generates random locations of pixels in an image and embedding message with Least Significant Bit algorithm to make it highly indiscernible. With this technique PSNR of 71.347 dB and MSE of 0.0048 achieved with compression ratio 0.5 and BER of 0.0171.

P. Yadav and M. Dutta, "3-Level security based spread spectrum image steganography with enhanced peak signal to noise ratio," 2017 Fourth International Conference on Image Information Processing (ICIIP), Shimla, India, 2017, pp. 1-5, doi: 10.1109/ICIIP.2017.8313696.

7) An embedding approach using orthogonal matrices of the singular value decomposition for image steganography

This paper aims to reduce the embedding errors, maintain the image fidelity, and reduce the errors, when detecting the embedded messages in images. An embedding approach is proposed that depends on using the orthogonal matrices of the Singular Value Decomposition (SVD) as a vessel for embedding information instead of embedding in the singular values of the images. Three ways are suggested to reduce the embedding errors and maintain the image fidelity, when detecting the embedded message. These ways are increasing the number of columns protected without embedding, choosing the suitable block size to embed in and adjusting the singular values in order to give a high quality of the stego image. Results show that utilization of the orthogonal matrices of the SVD for information hiding can be as effective as using transform-based techniques, and it gives better results than those obtained with the Least Significant Bit (LSB) technique.

Abdallah, H.A., Amoon, M., Hadhoud, M.M. et al. An embedding approach using orthogonal matrices of the singular value decomposition for image steganography.

8) A Novel Approach to Image Steganography Based on the Image Colorization

This paper proposes a novel image steganography algorithm for colour image. Recently, colorization-based image coding technique has been studied. In order to compress the colour image effectively, this technique transform the chrominance image to a vector in a low-dimensional subspace via the colorization matrix. This paper utilizes the colorization-based image coding for steganography algorithm, where the secret data is embedded into the null space of the colorization matrix. Because the null space is high dimension enough, a large

capacity data can be embedded. Numerical examples show that the proposed algorithm embeds large capacity secret data such as grayscale image into colour image effectively.

K. Uruma, K. Konishi, T. Takahashi and T. Furukawa, "A Novel Approach to Image Steganography Based on the Image Colorization," 2019 IEEE Visual Communications and Image Processing (VCIP), Sydney, NSW, Australia, 2019, pp. 1-4, doi: 10.1109/VCIP47243.2019.8965732.

9) An image steganography method based on texture perception

Existing image steganography technology can resist image attacks; however, the quality of generated encoded image is poor and the low-frequency region can be perceived. To improve the quality of the encoded image, an image steganography method based on texture analysis is proposed. In this method, the gray level co-occurrence matrix is used to extract the texture information of the cover image, the information is embedded in the complex position of the image, in and the network structure of the StegaStamp encoder is improved, small convolution layers are added in the down-sampling process to expand the receptive field, and channel attention is used to assign different weights to feature channels to enhance the influence of important features of images. The experimental results show that the proposed method can effectively improve the PSNR and SSIM values of coded image, and the quality is improved without degrading the robustness and embedding capacity.

L. Niu and J. Zhang, "An image steganography method based on texture perception," 2022 IEEE 2nd International Conference on Data Science and Computer Application (ICDSCA), Dalian, China, 2022, pp. 625-628, doi: 10.1109/ICDSCA56264.2022.9988162.

10) Generating Steganographic Images via Adversarial Training

In conclusion, this paper presents a novel application of adversarial training techniques to the discriminative task of learning a steganographic algorithm. The study demonstrates that unsupervised adversarial training can generate robust steganographic techniques that rival state-of-the-art methods. Additionally, a robust steganalysis is developed, which effectively discriminates whether an image contains hidden information.

By defining a game involving three parties (Alice, Bob, and Eve) and representing them with neural networks, the proposed approach achieves competitive performance on two independent image datasets. The results highlight the effectiveness of adversarial training for steganography, expanding its applications beyond generative tasks.

This work offers valuable insights into the potential of adversarial training for steganographic problems, shedding light on the possibility of developing more robust and secure information hiding techniques. Further exploration and refinement of this approach can pave the way for advancements in the field of steganography.

NIPS 2017: Neuíal Infoímation Píocessing Systems 2017, 4-9 Decembeí 2017, Long Beach, Califoínia, USA Volume: 30

11) CNN Auto-Encoder Network Using Dilated Inception for Image Steganography

Numerous studies have used convolutional neural networks (CNNs) in the field of information concealment as well as steganalysis, achieving promising results in terms of capacity and invisibility. In this study, we propose a CNN-based steganographic model to hide a colour image within another colour image. The proposed model consists of two sub-networks: the hiding network is used by the sender to conceal the secret image; and the reveal network is used by the recipient to extract the secret image from the stego image. The architecture of the concealment sub-network is inspired by the U-Net auto-encoder and benefits from the advantages of the dilated comolution. The reveal sub-network is inspired by the auto-encoder architecture.

To ensure the integrity of the hidden secret image, the model is trained end to end: rather than training separately, the two subnetworks are trained simultaneously a pair of networks. The loss function is elaborated in such a way that it favors the quality of the stego image over the secret image as the stego image is the one that comes under steganalysis attacks. To validate the proposed model, we carried out several tests on a range of challenging publicly available image datasets such as ImageNet, Labelled Faces in the Wild (LFW), and PASCAL-VOCI 2. Our results show that the proposed method can dissimulate an image into another one with the same size, reaching an embedding capacity of 24 bit per pixel without generating visual or structural artefacts on the host image. In addition, the proposed model is generic, that is, it does not depend on the image's size or the database source.

IKich, E. B. Ameur, Y. Taouil and A. Benhfid, "Image Steganography Scheme Using Dilated Convolutional Network," 2021 12th International Conference on Information and Communication Systems (ICICS), Valencia, Spain, 2021, pp. 305-309, doi: 10.1109/ICICS52457.2021.9464546.

12) Image Steganography Using Auto Encoder-Decoder Based Deep Learning Method

Image steganography is the process of communicating hidden secret image embedded in a cover image in plain sight without arousing any suspicions. In the recent times, deep learning methods have gained popularity and is widely used in the field of steganography. In this paper, an auto encoder-decoder based deep convolutional neural network is proposed to embed the secret image inside the cover image and to extract the secret image from the generated stego image. Training and testing is done on a subset of the ImageNet dataset. To evaluate the proposed method, Peak Signal-Noise Ratio (PSNR) and Mean Squared Error (MSE) metrics are used. The proposed method has proved to achieve higher invisibility, security and robustness. The capacity of the method is higher when compared to traditional Least Significant Bit substitution methods.

Visions and Concepts for Education 4.0 (pp.520-530); Authors: Nandhini Subramanian, Omar Elharrouss, Somaya Al-ma'adeed, Samir A. El-Seoud

13) Sharing Confidential Images with Abbreviated Shares using Steganography and AES Algorithm

'Steganography' derives from the Greek steganos (= "covered") and graphy (= "writing") so its literal meaning is "covered writing." It is concerned with communication that is 'invisible'. There are many steganographic approaches for hiding vital information in various file formats, some of which are more difficult than others, and each has its own set of strengths and weaknesses. In the Least Significant Bit (LSB) embedding approach, data is embedded in the cover picture's least significant bits in a manner that renders the unaided eye incapable of discerning the image in the cover file. This approach could work in both 24-bit and 8-bit settings. In BPCS steganography, the image is the vessel data, secret info is embedded in the vessel's bit-planes. Without degradation of image quality, we replace with secret data, every "noise-like" region within the bit-planes of the vessel image. This steganography may be called "BPCSSteganography," or Bit-Plane Complexity Segmentation Steganography. In this paper we describe an experimental approach to hide the secret image by using LSB and BPCS steganography and AES algorithm.

A.N, A. V. K and N. R, "Sharing Confidential Images with Abbreviated Shares using Steganography and AES Algorithm," 2022 2nd International Conference on Intelligent Technologies (CONIT), Hubli, India, 2022, pp. 1-5, doi: 10.1109/CONIT55038.2022.9847932.

14) Image Steganography Using Steg with AES and LSB

Nowadays mobile phone becoming one of the most popular communication systems. Information shared through this medium is a very sensitive to the users. Hence it is highly needed to secure the message from the intruders. This paper proposed an android based secured system named Steg! developed by combining the cryptography and steganography. Here the algorithm used for cryptography is Advanced Encryption Standard (AES) and Least Significant Bit is used for the steganography. This hybrid approach increases the level of secretion of information from unauthorized the access by encrypting the message and hiding into the image. The application helps the user to hide/unhide the text to/from the image. The proposed system above is proven to be powerful and robust than those system which implements cryptography and steganography alone.

L. Negi and L. Negi, "Image Steganography Using Steg with AES and LSB," 2021 IEEE 7th International Conference on Computing, Engineering and Design (ICCED), Sukabumi, Indonesia, 2021, pp. 1-6, doi: 10.1109/ICCED53389.2021.9664834.

15) Image Steganography Based on Iterative Adversarial Perturbations onto a Synchronized-Directions Sub-Image

Nowadays a steganography has to face challenges to both feature based steganalysis and convolutional neural network (CNN) based steganalysis. In this paper, we present a novel steganographic scheme to incorporate synchronizing modification directions and iterative adversarial perturbations to enhance steganographic performance. Firstly, an existing steganographic function is employed to compute initial costs. Then the secret message bits are embedded following clustering modification directions profile. If the target CNN classifier discriminates the resulting stego image as the correct class, we change costs in adversarial manners, and then choose a sub-image to re-embed message with changed costs. Adversarial intensity will be iteratively increased until the adversarial stego image can deceive the target CNN classifier, which guarantees that applied adversarial perturbations are minimal and it is unnecessary to search the optimal adversarial intensity. Experiments demonstrate that the proposed method effectively enhances security to counter both feature-based classifiers and CNN classifiers, no matter they are targeted or non-targeted.

X. Qin, S. Tan, W. Tang, B. Li and J. Huang, "Image Steganography Based on Iterative Adversarial Perturbations onto a Synchronized-Directions Sub-Image," ICASSP 2021 - 2021 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Toronto, ON, Canada, 2021, pp. 2705-2709, doi: 10.1109/ICASSP39728.2021.9414055.

MODULE DESCRIPTION

Encoding:

- This module is responsible for taking the secret message and embedding it within the chosen image.
- It utilizes various techniques like:
- Spatial domain techniques: Directly modifying pixel values (Least Significant Bit insertion, Pixel Value Differencing).
- Frequency domain techniques: Transforming the image to another domain (DCT, Discrete Wavelet Transform) and hiding data in coefficients.
- Spread spectrum techniques: Distributing the data across the entire image for increased robustness.
- This module needs to consider factors like embedding capacity, imperceptibility (maintaining image quality), and robustness against noise and compression.

Decoding:

- This module retrieves the hidden message from the stego-image (image containing the hidden data).
- It uses the same technique as the embedding module but in reverse, extracting the information from designated locations or manipulations.
- Security relies on this module being kept secret and not publicly known.

Stego-key Management:

• This module manages any secret keys used for encryption or authentication of the hidden message.

• It ensures only authorized parties can access or extract the hidden message, adding an extra layer of security.

Steganalysis Module (Optional):

• This module, used for security testing or malicious purposes, aims to detect the presence of hidden data in an image.

• It employs statistical analysis, visual clues, and other techniques to uncover anomalies indicative of steganography.

Security and Countermeasures:

• This module focuses on protecting the hidden message from steganalysis and unauthorized access.

• It may involve techniques like stego-image modification, feature selection, and cryptographic integration

IMPLEMENTATION

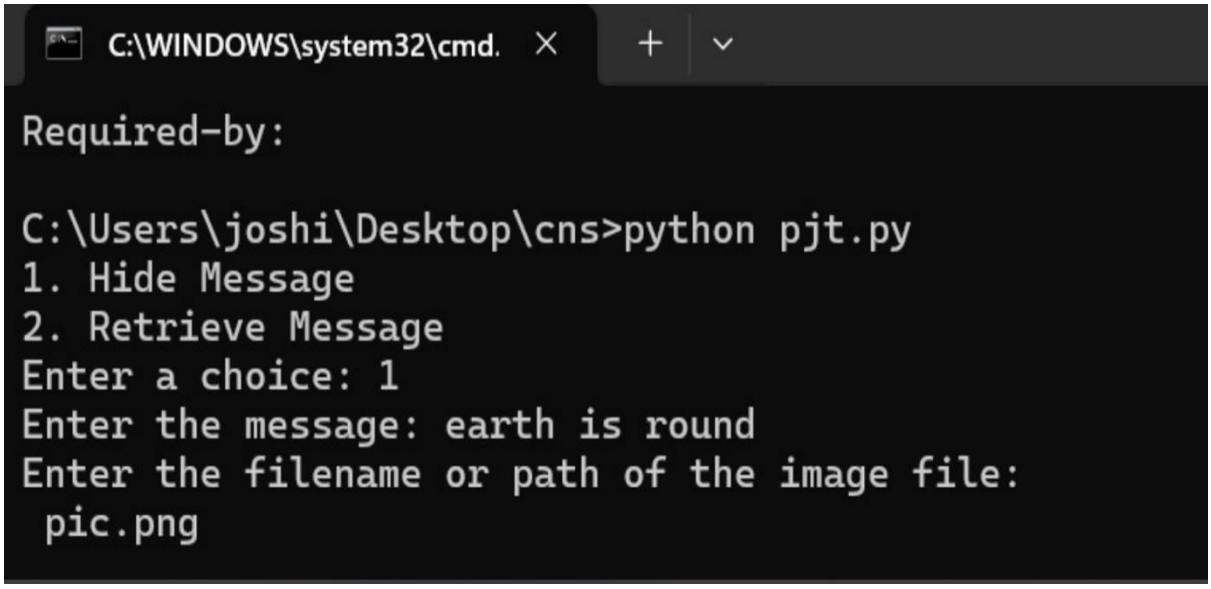
Code:

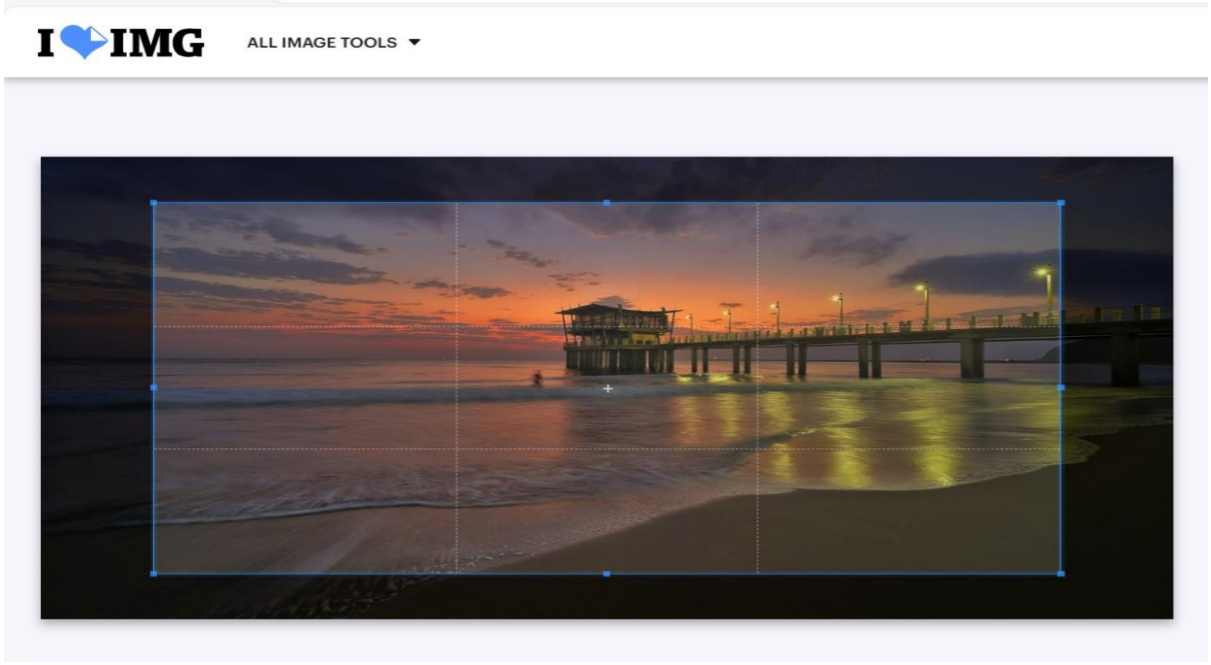
```
from PIL import Image
import bitarray
def hide_message(image_path, message):
# Open the image
image =Image.open(image_path)
width, height = image.size
# Convert the message to binary
ba=bitarray.bitarray()
ba.frombytes (message.encode('utf-8'))
binary_message = ba.to01()
# Calculate the starting position for hiding the message
start_x = width // 2
start_y = height // 2
# Hide the message in the image
index = 0
for y in range(start_y, height):
for x in range(start_x, width):
if index < len(binary_message):
pixel =list(image.getpixel((x, y)))
pixel[0] =pixel[0] & ~1 | int(binary_message[index])
image.putpixel((x, y), tuple(pixel))
index += 1
else:
break
```

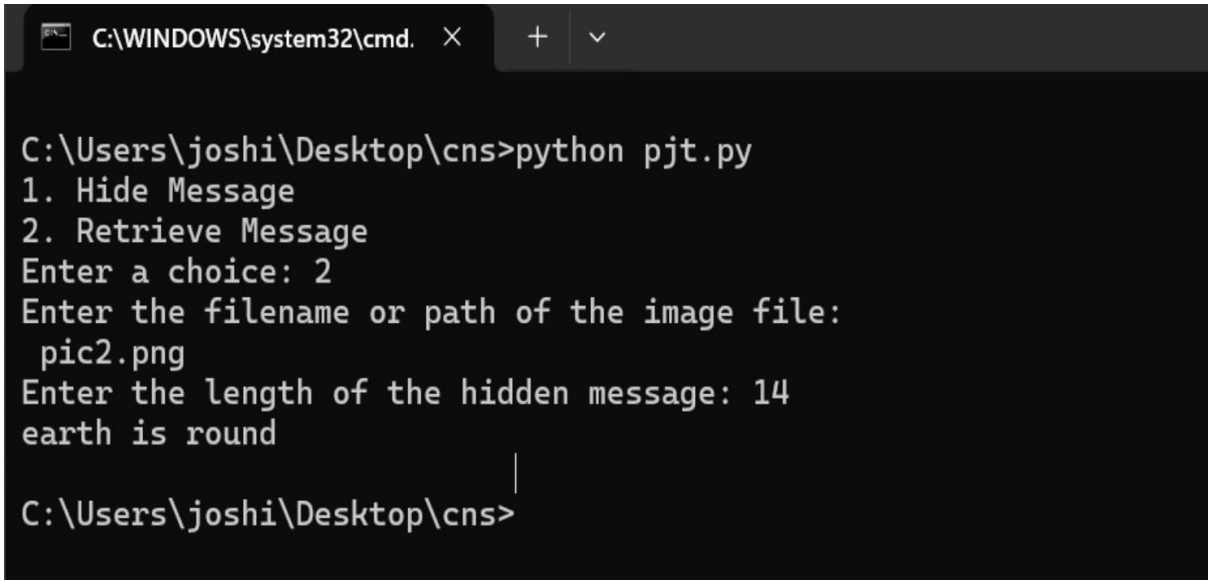
```
# Save the modified image
image.save('hidden_message.png')
def retrieve_message(image_path, message_length):
# Open the image
image = Image.open(image_path)
width, height =image.size
# Calculate the starting position for retrieving the message
start_x = width // 2
start y = height // 2
# Retrieve the message from the image
binary_message=' '
index = 0
for y in range(start_y, height):
for x in range(start_x, width):
if index < message_length * 8:
pixel = list(image.getpixel((x, y)))
binary_message += str(pixel[0] & 1)
index += 1
else:
break
# Convert the binary message to text
ba =bitarray.bitarray(binary_message)
message = ba.tobytes().decode('utf-8')
return message
# Hide a message in an image
print("1. Hide Message")
print("2. Retrieve Message")
```

```
choice =int(input("Enter a choice: "))
if choice == 1:
mess = input("Enter the message: ")
fname = input("Enter the filename or path of the image file: ")
hide_message(fname, mess)
elif choice == 2:
fname = input("Enter the filename or path of the image file: ")
length = int(input("Enter the length of the hidden message: "))
message = retrieve_message(fname, length)
else:
print(message)
print("Invalid choice")
```

RESULT


C:\WINDOWS\system32\cmd.
Required-by:
C:\Users\joshi\Desktop\cns>python pjt.py
1. Hide Message
2. Retrieve Message
Enter a choice: 1
Enter the message: earth is round
Enter the filename or path of the image file:
pic.png

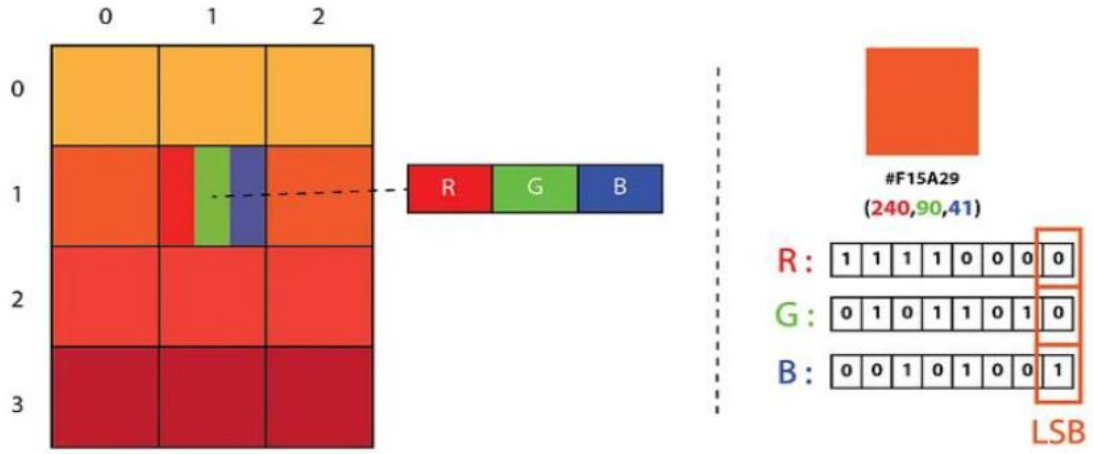

I IMG
ALL IMAGE TOOLS


C:\WINDOWS\system32\cmd.
C:\Users\joshi\Desktop\cns>python pjt.py
1. Hide Message
2. Retrieve Message
Enter a choice: 2
Enter the filename or path of the image file:
pic2.png
Enter the length of the hidden message: 14
earth is round
C:\Users\joshi\Desktop\cns>

IMPLEMENTATION(Details)

LSB Algorithm:

LSB Steganography is an image steganography technique in which messages are hidden inside an image by replacing each pixel's least significant bit with the bits of the message to be hidden. We can convert the message into decimal values and then into binary, by using the ASCII Table. Then, we iterate over the pixel values one by one after converting them to binary, we replace each least significant bit with that message bits in a sequence. To decode an encoded image, we simply reverse the process. Collect and store the last bits of each pixel then split them into groups of 8 and convert it back to ASCII characters to get the hidden message. Here, the message is spread equally across the image so as to avoid detection, but on cropping the image, the secret text is not extractable. So, a solution proposed to this problem is the Centre Embedded Pixel Positioning (CEPP) which is based on Least Significant Bit (LSB) Matching by setting the secret image in the center of the cover image.



Centre Embedded Pixel Positioning (CEPP):
This method involves storing the secret text in the middle of the picture. So, on cropping the image equally on all sides, we can still be able to retrieve the secret text.

Steps to be followed are:
• Take the image and the message as input.
• Convert the message to binary
• Calculate the starting position for hiding the message
• Hide the message in the image using LSB algorithm
• And then save the image.

• To retrieve the secret text from the image, open the image and calculate the starting position for the retrieving the message.
• Once we've extracted it, convert binary to text and display it.

Selection of Secret Message and Cover Image: Like any steganographic technique, CEPP begins with selecting a secret message and a cover image. The secret message is the information that needs to be hidden, while the cover image is the carrier that will contain the secret message.

Binary Conversion of Secret Message: The secret message is converted into binary format. This binary representation is what will be embedded into the pixels of the cover image.

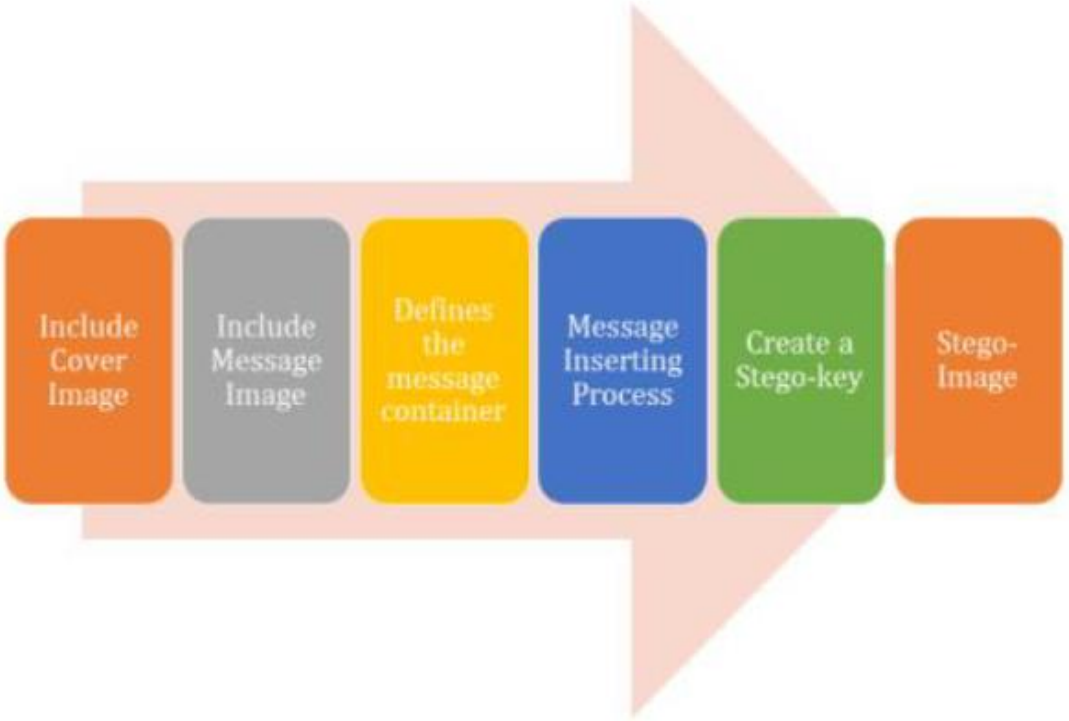
Calculation of Starting Position: CEPP calculates the starting position within the cover image where the embedding of the secret message will begin. This starting position is crucial for ensuring that the message is embedded in a specific location within the image.

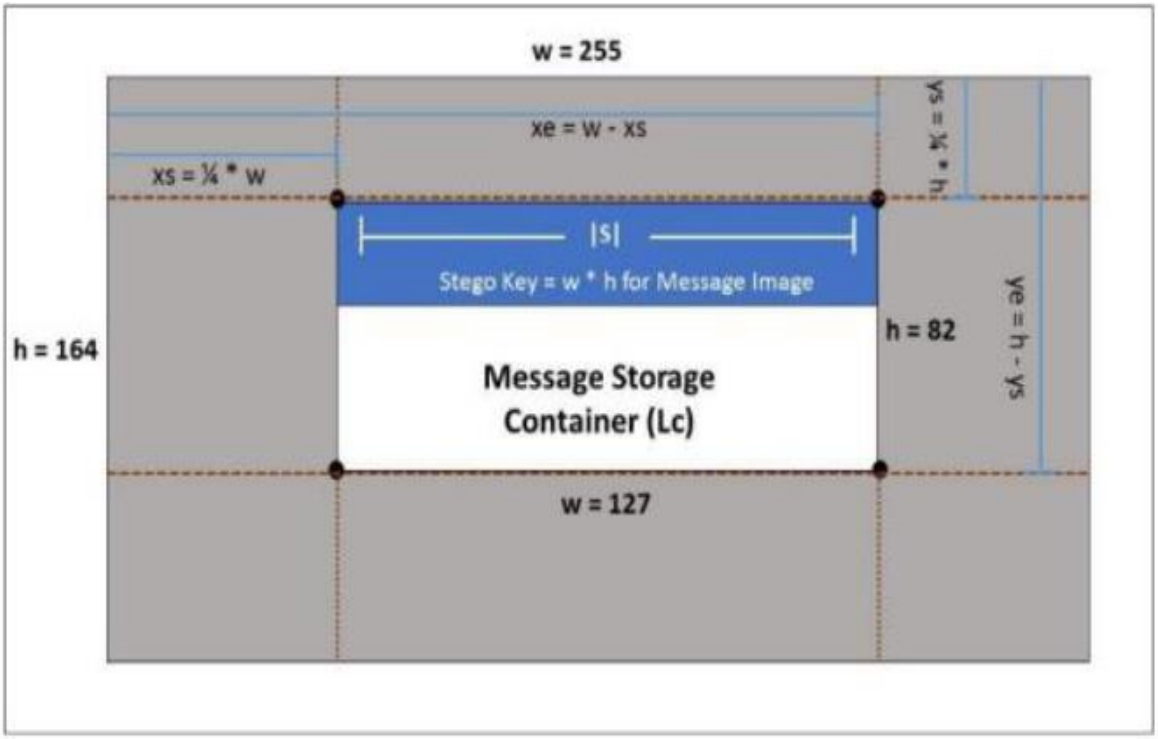
Embedding of Secret Message: The binary representation of the secret message is then embedded into the pixels of the cover image using a steganographic algorithm. In the case of CEPP, the Least Significant Bit (LSB) algorithm is often used for embedding. However, CEPP introduces the concept of positioning the secret message in the centre of the image, which is a key distinguishing feature.

Saving the Modified Image: Once the secret message is embedded, the modified cover image containing the hidden data is saved. This resulting image is referred to as the stego-image.

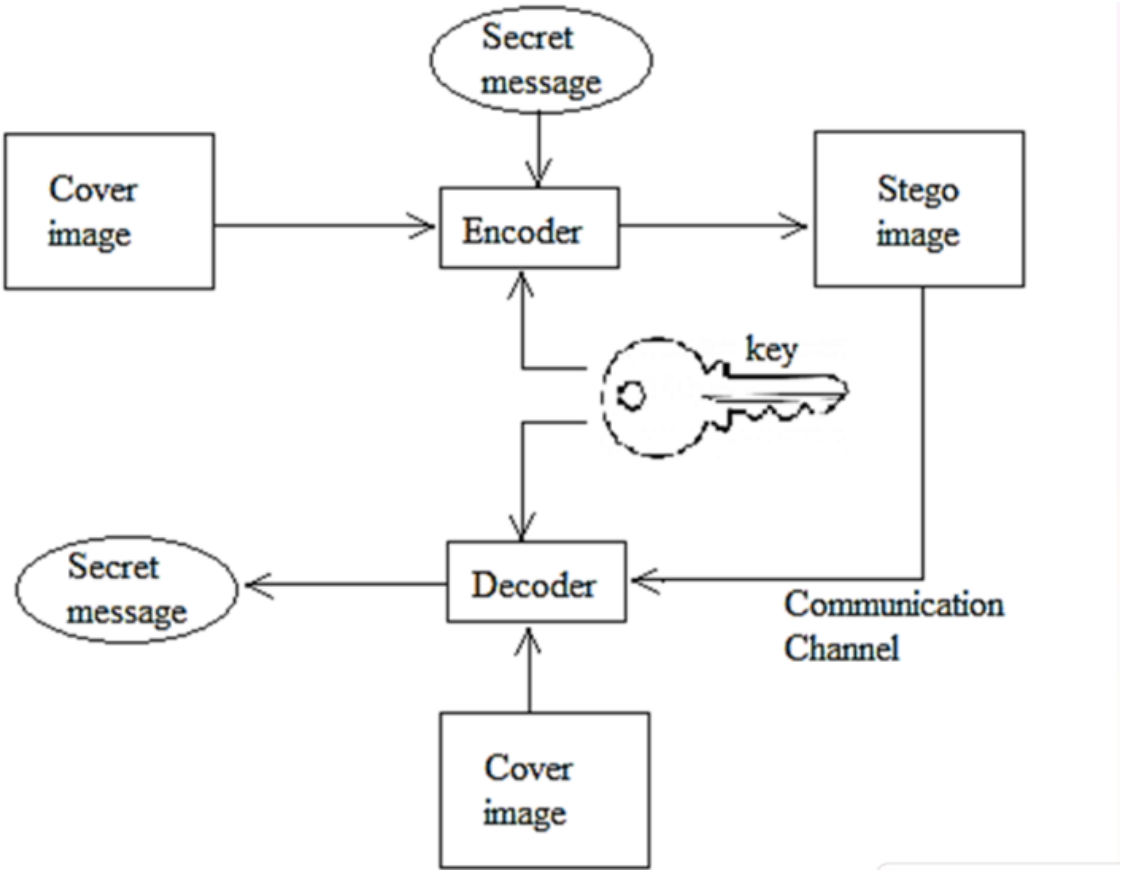
Retrieval of Secret Message: To retrieve the hidden message from the stego-image, the process is reversed. The starting position for extracting the message

is calculated, and then the binary bits are extracted from the pixels of the stego-image. Finally, the binary bits are converted back into the original message format.





PROPOSED SOLUTION



DISCUSSION

Historical Evolution: Start by discussing the historical evolution of steganography, highlighting its roots in ancient methods of concealing messages and its transition into the digital age. Mention notable historical examples, such as invisible ink or microdot technology, to demonstrate the enduring relevance of steganography.

Modern Techniques: Explore the various modern techniques used in image steganography, including LSB (Least Significant Bit) insertion, spread spectrum, and transform domain techniques like DCT (Discrete Cosine Transform) or DWT (Discrete Wavelet Transform). Discuss the principles behind each technique and how they leverage the characteristics of digital images to embed information covertly.

Applications: Highlight the diverse range of applications for image steganography in today's interconnected world. Discuss how steganography is used for covert communication, digital watermarking for copyright protection, and even in forensic investigations to hide information within images.

Security and Privacy: Emphasize the importance of image steganography in ensuring the security and privacy of sensitive information. Discuss how steganographic techniques provide a layer of concealment that complements encryption methods, making it more challenging for adversaries to intercept or decipher hidden messages.

Steganalysis: Acknowledge the existence of steganalysis as the counterpart to steganography, focusing on techniques used to detect hidden messages within images. Discuss the challenges faced by steganalysts in distinguishing between innocuous image data and covertly embedded information.

Challenges and Countermeasures: Explore the challenges inherent in developing secure steganographic systems, including issues such as payload capacity, robustness to attacks, and computational complexity. Discuss potential countermeasures to enhance the security of steganographic techniques, such as adaptive embedding strategies or incorporating cryptographic primitives.

Ethical Considerations: Touch upon the ethical implications of image steganography, including its potential misuse for illicit purposes such as espionage, cybercrime, or terrorism. Highlight the importance of responsible

usage and the need for ethical guidelines to govern the application of steganographic techniques.

Future Directions: Conclude the discussion by speculating on the future directions of image steganography, considering advancements in technology and emerging challenges. Discuss potential areas of research, such as improving the robustness of steganographic methods against detection or exploring novel applications in fields like healthcare or data security.

CONCLUSION

To conclude, image steganography is a powerful technique that allows for the secure and covert embedding of information within images. It offers several advantages, including confidential communication, covert data transfer, digital watermarking, and anti-forensic applications. By leveraging the LSB algorithm or other advanced techniques, sensitive data can be hidden within the least significant bits of image pixels. Based on the discussion, the CEPP algorithm shows a remarkable result in image steganography, proved by its success in the embedding and message extraction processes.

However, it is essential to consider the limitations of steganography, such as low embedding capacity, vulnerability to attacks, sensitivity to image manipulation, and the need for additional security measures. Overall, image steganography plays a significant role in various domains, providing a means to protect privacy, ensure data integrity, and facilitate covert information exchange. Its responsible and ethical use is crucial to maintain trust, privacy, and security in digital communication.

REFERENCES

1. Desoky, A. Noiseless Steganography. CRC Press, 2012.
2. Abd El-Latif, A. A., B. Abd El-Att, S. E. Venegas-Andraca. A Novel Image Steganography Technique Based on Quantum Substitution Boxes. – Optics and Laser Technology, Vol. 116, 2019, pp. 92-102.
3. Al-Afandy, K. A., O. S. Faragallah, A. Elmhalawy, E. S. M. El-Rabaie, G. M. El-B anby. High Security Data Hiding Using Image Cropping and LSB Least Significant Bit Steganography. – In: 4th International Colloquium on Information Science and Technology (CIST'16), IEEE, 2016, pp. 400-404.
4. Kumar, V., D. Kumar. Digital Image Steganography Based on Combination of DCT and DWT. – Communications in Computer and Information Science, Vol. 101, 2010, pp. 596-601.
5. Kumar, S. K., P. D. K. Reddy, G. Ramesh, V. R. Maddumla. Image Transformation Technique Using Steganography Methods Using LWT Technique. – International Information and Engineering Technology Assocation, Vol. 36, 2019, No 3, pp. 233-237.
6. Juarez-Sandoval, O., M. Cedillo-Hernandez, G. Sanchez-Perez, K. Toscano Medina, H. P er ez-Meana, M. Nakano-Miyatake. Compact Image Steganalysis for LSB-Matching Steganography. – In: Proc. of 5th International Workshop on Biometrics and Forensics, IWBF, 2017.
7. Kadhim, I. J., P. Premaratne, P. J. Vial, B. Halloran. Comprehensive Survey of Image Steganography: Techniques, Evaluations, and Trends in Future Research. – Neurocomputing, Vol. 335, 2019, pp. 299-326.
8. Mishra, M., P. Mishra, M. C. Adhikary. Digital Image Data Hiding Techniques: A Comparative Study. – Ansvesa, Vol. 7, 2014, No 2, pp. 105-115.
9. Mishra, B., R. Beg, V. P. Singh. Information Security through Digital Image Steganography Using Multilevel and Compression Technique. – MIT International Journal of Computer Science & Information Technology, Vol. 3, 2013, No 1, pp. 26-29.
10. Hu, D., L. Wang, W. Jiang, S. Zh en g, B. Li. A Novel Image Steganography Method via Deep Convolutional Generative Adversarial Networks. – IEEE Transactions on Information Forensics and Security, Vol. 6, 2018, pp. 38303-38314.
11. Singh, S., R. Beg, T. J. Siddiqui. Robust Image Steganography Using Complex Wavelet Transform. – In: Proc. of International Multimedia, Signal Processing and Communication Technologies, IMPACT, 2013, pp. 56-30.
12. Hussain, M., A. W. A. Wahab, Y. I. Bin Idris, A. T. S. Ho, T. S. Jung. Image Steganography in Spatial Domain: A Survey. – Signal Processing: Image Communication Vol. 65, 2018, pp. 46-66.
13. Z hou, Z., Y. Mu, Q. M. J. Wu. Coverless Image Steganography Using Partial-Duplicate Image Retrieval. – Soft Computing, Vol. 23, 2019, No 23, pp. 4927-4938.
14. Darwis, D., A. Jun aidi, Wamiliana. A New Approach of Steganography Using Center Sequential Technique. – In: Journal of Physics: Conference Series. Vol. 1338. 2019.
15. J u ar ez-S an doval, O., A. Fierro-Radilla, A. Espejel-Trujillo, M. Nakano Miyatake, H. Perez-Meana. Cropping and Noise Resilient Steganography Algorithm Using Secret Image Sharing. – In: Proc. of 6th International Conference on Graphic and Image Processing (ICGIP'14), Vol. 9443, 2015