**BPCS Algorithm based Steganography with Integration of RSA**

**INTRODUCTION**

**Overview**

Cryptography and steganography are cousins in the spy craft family: the former scrambles a message so it cannot be understood, the latter hides the message so it cannot be seen. A cipher message, for instance, might arouse suspicion on the part of the recipient while an invisible message created with steganographic methods will not A basic steganographic model is shown in Figure 1. The message ‘M’ is the secret data that the Sender wishes to hide without any suspicion. The secret data can be audio, video, image, text. The cover ‘X’ is the original image, audio file, video file, in which the secret message ‘M’ is to be embedded. The cover ‘X’ is also called as “Message Wrapper”. It is not necessary that the cover ‘X’ and the message ‘M’ should have homogeneous structure. For example, text message or an audio file can also be hidden into video or image. In this project the cover ‘X’ is image and Message ‘M’ is text.

**Purpose**

The goal of steganography is to hide a message in plain sight. BPCS is a method to embed a message in an image by replacing all "complex" blocks of pixels in the image with portions of our message. It turns out that portions of the image with high complexity can be entirely removed (or in this case, replaced with our message) without changing the appearance of the image at all. Because most blocks of pixels are complex (i.e., with complexity above some threshold, alpha), you can usually replace around 45% of an image with a hidden message. Below, the 300x300 image on the right contains the text of an entire novel, while still looking virtually identical to the vessel image on the left.



VESSEL IMAGE

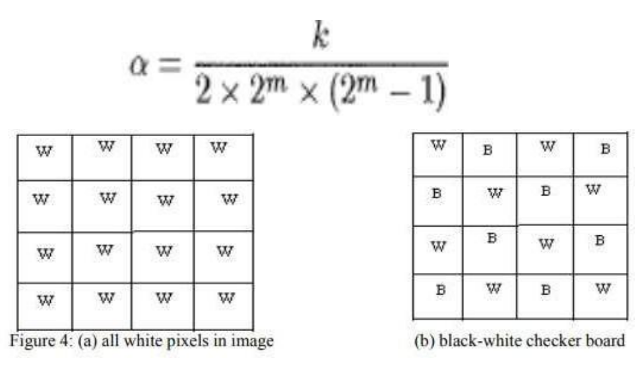


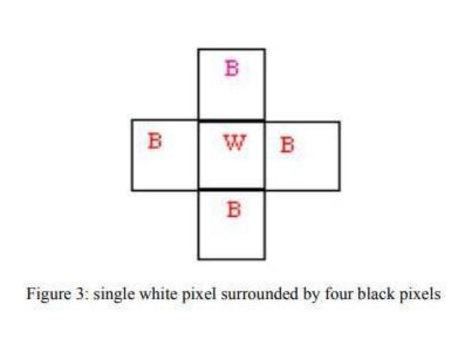
**LITERATURE SURVEY**

Existing problem / Existing approaches or method to solve this problem

Note that with BPCS, the hidden message doesn't have to be text. It can be any file type, including another image. You could upload a profile photo to a website that contains a secret image. Or you could embed an image of a turtle inside an image of a turtle inside an image...turtles all the way down. This is an implementation of the method discussed in: Kawaguchi, Eiji, and Richard O. Eason. "Principles and applications of BPCS steganography." In Photonics East (ISAM, VVDC, IEMB), pp. 464-473. International Society for Optics and Photonics, 1999. The goal of steganography is to hide things in plain sight. For this reason, BPCS doesn't use a secret key or password for encoding and decoding. However, aside from varying the alpha parameter, one way to customize the BPCS procedure is by adding custom encryption and decryption to the message before and after using BPCS and we have done this with RSA algorithm. There are various ways the complexity regions are described in various research papers, but in this project, we use complexity definition on the basis of alpha parameter. The important step in BPCS steganography is to find “complex” region in the vessel image so that data from secret image can be hidden without any suspicion. Also, there is no standard definition of complexity. There are basically three methods of complexity measure.

However, in our experiment and in this paper, we focus on complexity measure based on length of black and white border in binary image. The total length of black and white border is equal to the summation of the number of color changes along the rows and columns in an image.





Proposed solution

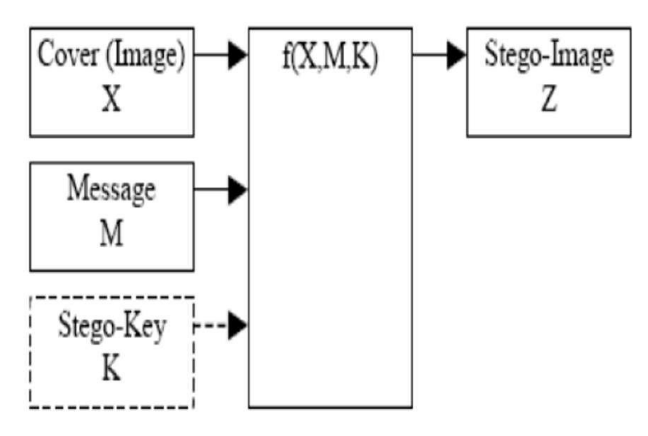
Our project demonstrates the combination of RSA with BPCS steganography. Among the resources we found in the internet, we either found only the steganography or RSA, but the secured channel is when both the components are intertwined. Thus, in this project we bring the implementation using the different modules of Python, the image steganography with BPCS steganography protocol. We even realized the disadvantages of other algorithms posed, like LSB where only 1/8 th of the image can be embedded, because LSB uses only the last 4 significant bits for steganography. But in case of RSA, the use of bits for replacement are based on the complexity region. In this project we have implemented the complexity region based on the theorem we have mentioned earlier in the document. Nowhere we could find the project intertwining the cousins of security mechanism: the cryptography and the steganography. We have implemented the BPCS steganography model using the python language and its modules while the RSA were implemented using C sharp. Thus, the innovation stands in hiding data upto 50 percent of the capacity of image and also encrypting it with one of the most secured public key encryptions algorithms, the RSA. We were just settling with Steganography with BPCS algorithm, and we had completed this project in the mid of November, but one of our team members sought an idea of further extending the project so that the encryption portion could be depicted too along with the steganography. Thus, from embedding to encryption, our model certainly is very much secured in the recent time.

Proposed BPCS Steganography Algorithm

a) Consider a color image as vessel image. Make the size of image as 512 x 512. b) Convert the vessel image to gray scale image. c) Consider a gray scale secret image and make the size of image as 256 x 256. d) Convert the vessel image and the secret image which are in pure binary Code (PBC) form into Canonical Gray Code (CGC) form. e) Perform bit plane slicing on vessel image as well as on secret image. f) Calculate complexity measure ‘alpha’ (α) for each block of each bit plane of vessel image. g) Calculate α for each block of each bit plane of secret image. h) Perform conjugation operation on the ‘simple’ or ‘informative’ blocks of the secret image. I) Perform embedding operation to embed secret image in vessel image. j) Convert the CGC form embedded image to PBC image.

**THEORETICAL ANALYSIS**

Block diagram



Hardware / Software designing

Language Used: Python

IDE USED FOR THE PROJECT IS VS CODE

• Libraries of Python imported:

1. NumPy

2. FUNCTOOLS

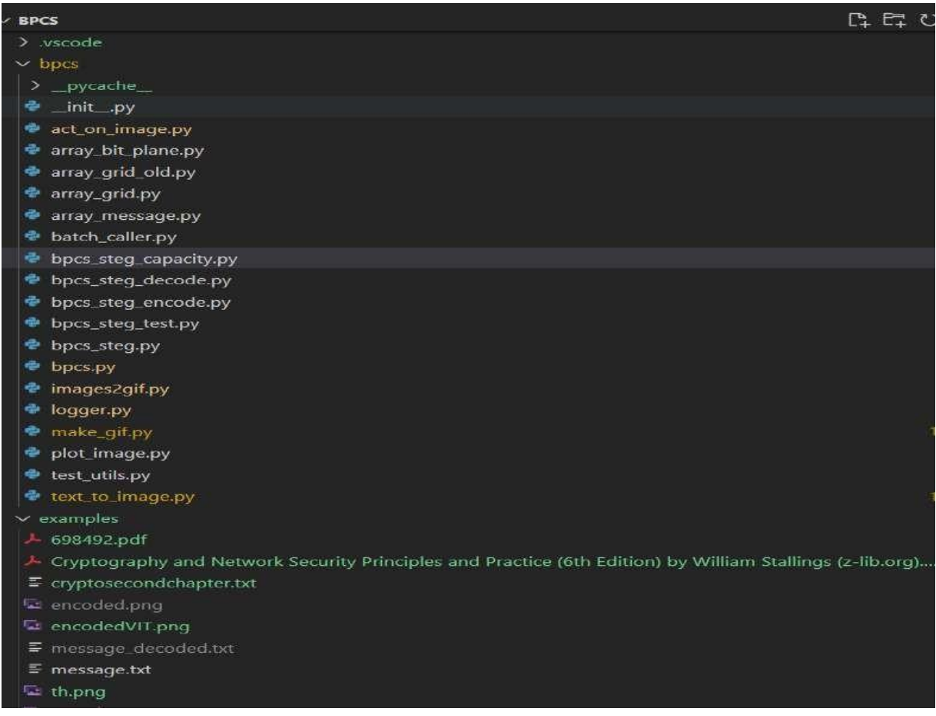
3. PILLOW

4. MATH

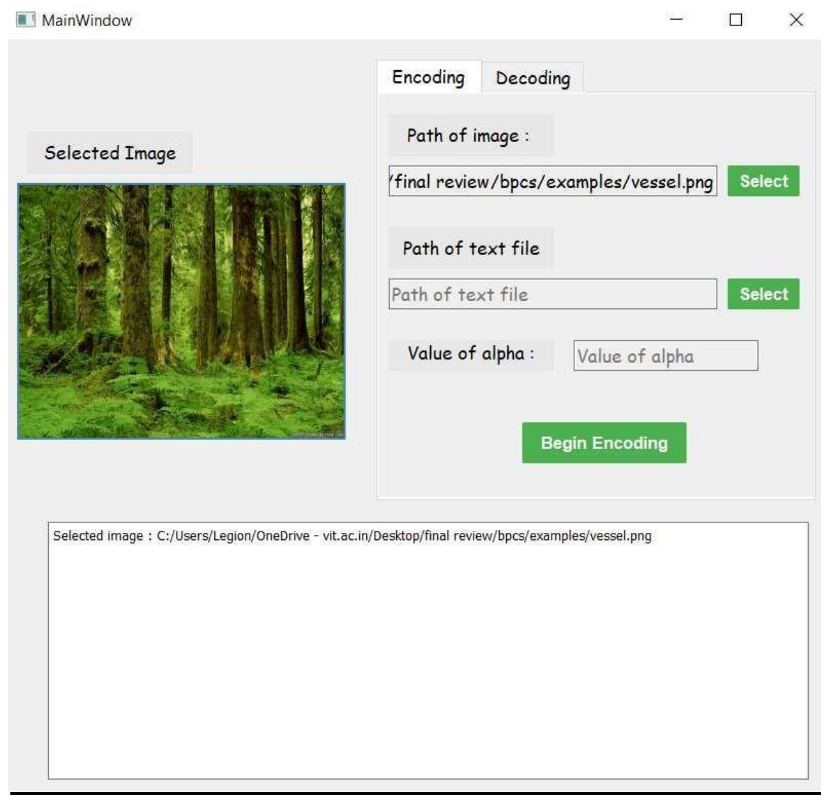
5. OS

6. LOGGER and Matplotlib

ALL The python files are kept in BPCS directory and the Image to Be encoded, Decoded and text to be hidden all are present in the same directory



GUI FOR DECODING and Encoding



**EXPERIMENTAL INVESTIGATIONS**

Analysis or the investigation made while working on the solution.

We collectively sought for the comparison of BPCS steganography model with other model like LSB’s and we started searching and collecting the data regarding the efficiency of both the model.





We examined around 40-50 images with LSB and BPCS algorithm

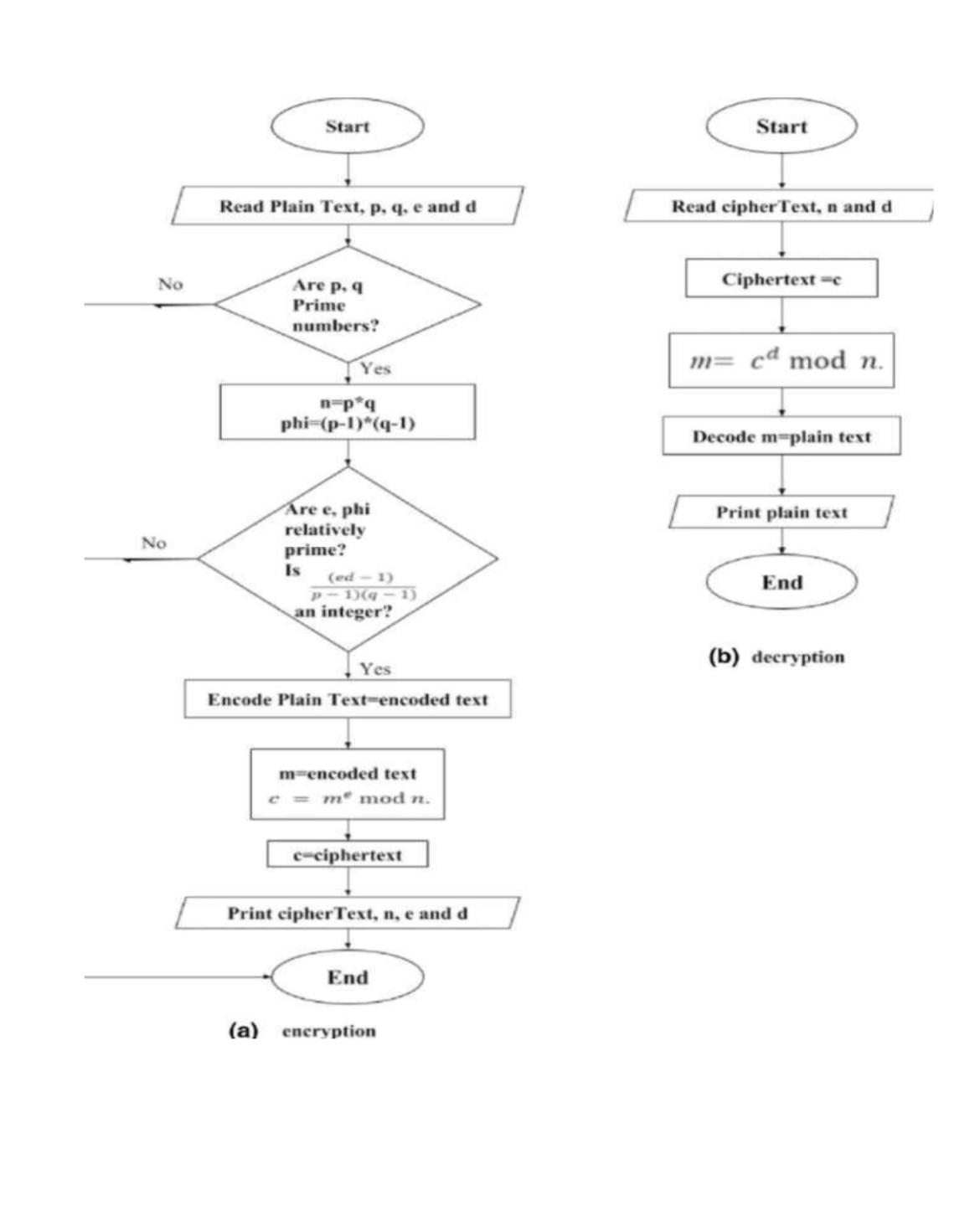


Steganography image with LSB



With LSB steganography certainly the image seems to have some noisy regions and also with distortion, what we also came to know was LSB steganography is well implemented with .png format and with .jpg/.jpeg format the distortion seems to be noticeable. Thus, for large embedding (nearly the text of a novel) can be well implemented using the BPCS steganography. Using the internet readymade tool for LSB, we compared the embedding capacity and the limitation of embedding with both BPCS and LSB. Our project did not even throw exception for an entire cryptography book, but the internet tool for LSB showed exception of file size with only few MB’s. Thus, we came to understand from various experimentation that the LSB steganography is not any near when it comes to BPCS steganography. We took the reference of few research papers and few implementations of steganography and RSA encryption. We certainly had to go through immense research papers and large number of projects, whose analysis we have mentioned in the review section. But we had our own idea of channeling the cryptography after steganography and our combination of BPCS with RSA, is certainly unique and poses lots of security benefits. Our project uses the unique combination of RSA and BPCs.

**FLOWCHART:**

****

**RESULT:**

****

**Advantages:**

1. Robust security: The integration of RSA (Rivest-Shamir-Adleman) encryption with the BPCS (Bit-Plane Complexity Segmentation) algorithm provides strong security for steganographic communication. RSA is a widely used asymmetric encryption algorithm known for its strong cryptographic properties, ensuring confidentiality and integrity of the hidden information.
2. Public-key encryption: RSA employs public-key cryptography, which means that the sender and receiver each have a pair of keys: a public key for encryption and a private key for decryption. This allows for secure communication over untrusted channels without the need for a shared secret key.
3. Resistance to attacks: BPCS algorithm-based steganography provides a high level of resistance to steganalysis techniques. BPCS exploits the complexity of bit-planes in digital images to embed hidden data, making it difficult for adversaries to detect the presence of the hidden information.
4. Scalability: The integration of BPCS with RSA allows for the efficient and scalable embedding of data into digital images. BPCS can handle large volumes of data while maintaining the image quality and maintaining a low embedding distortion.
5. Authentication: RSA can be used to authenticate the source of the hidden information. By using the sender's private key to sign the embedded data, the recipient can verify the integrity and authenticity of the message

.

**Disadvantages:**

1. Computational overhead: The integration of RSA encryption adds computational overhead to the steganographic process. RSA involves complex mathematical operations such as modular exponentiation, which can be computationally intensive, especially for large keys and data sizes. This may impact the real-time performance of the system.
2. Key management: RSA requires the management and distribution of public and private keys. Ensuring the secure exchange and storage of keys can be challenging, especially in large-scale deployments. Key management is crucial to maintain the security and integrity of the steganographic communication.
3. Limited capacity: While BPCS provides a relatively high capacity for data embedding, it is still limited by the size of the cover image and the embedding method. The integration of RSA encryption further reduces the available space for data embedding, as some capacity is reserved for the encryption process.
4. Vulnerability to side-channel attacks: RSA is susceptible to side-channel attacks such as timing attacks, power analysis, and electromagnetic analysis. Adversaries may exploit these vulnerabilities to gain information about the encryption keys or hidden data, compromising the security of the steganographic communication.
5. Dependency on image format: BPCS algorithm-based steganography with RSA integration is primarily designed for digital images. It may not be applicable or as effective for other file formats such as audio or video. Different file formats may require different steganographic techniques, limiting the versatility of the approach.

**Applications of BPCS Algorithm with RSA Integration:**

1. **Confidential Communication:** The combined approach allows for secure and confidential communication between individuals or organizations. The hidden message within the image provides an additional layer of security.

2. **Copyright Protection**: The BPCS algorithm can be used to embed copyright information within digital images. The integration with RSA ensures that only authorized parties can extract the copyright details, helping in protecting intellectual property.

3. **Covert Data Exchange**: BPCS with RSA integration can facilitate covert data exchange, where sensitive information can be hidden within images without arousing suspicion. This can be useful in scenarios where privacy or secrecy is of utmost importance.

4. **Digital Forensics**: The combination of BPCS and RSA can be employed in digital forensics to hide sensitive information within images for analysis or evidence gathering purposes. The hidden data can only be accessed by authorized investigators using the private key.

**CONCLUSION**

In conclusion, the integration of the BPCS algorithm with RSA encryption in steganography offers a powerful and secure method for hiding information within digital images. This combined approach provides confidentiality, integrity, and authentication to the hidden data. By leveraging the strengths of both techniques, BPCS and RSA, the security of the hidden information is enhanced while ensuring its imperceptibility within the cover image.

The BPCS algorithm identifies regions in the bit-planes of an image suitable for embedding, ensuring that the modifications made are visually indistinguishable. RSA encryption, on the other hand, provides a robust mechanism for encrypting the secret message, ensuring that only the intended recipient possessing the private key can decrypt and access the embedded information.

The applications of BPCS-based steganography with RSA integration are vast. It can be used for confidential communication, copyright protection, covert data exchange, and digital forensics. The integration of these techniques opens up opportunities for secure data hiding and retrieval in various domains.

Looking into the future, advancements in steganalysis techniques, adaptive embedding methods, and hybrid encryption approaches will drive further development and refinement of BPCS-based steganography with RSA integration. The integration may also extend to other multimedia formats and adapt to emerging technologies such as quantum computing.

As technology evolves, it is essential to stay updated with the latest advancements in steganography, encryption, and security practices to ensure the effectiveness and resilience of BPCS-based steganography with RSA integration. Ongoing research and collaboration among experts in the field will continue to push the boundaries of secure data hiding and communication.

**FUTURE SCOPE**

The integration of the BPCS algorithm with RSA encryption in steganography offers a robust solution for secure data hiding. Looking into the future, here are some potential scopes and advancements for this combined approach:

1. **Advancements in Steganalysis Techniques**: As steganography techniques evolve, so does the field of steganalysis, which focuses on detecting hidden information. Future developments in steganalysis techniques may pose challenges to the effectiveness of existing steganographic algorithms, including BPCS. Researchers will continue to innovate and improve steganography methods to stay ahead of detection techniques.

2. **Deep Learning-based Steganalysis**: The application of deep learning algorithms and artificial intelligence in steganalysis is a growing field. Future research may focus on developing more sophisticated deep learning models capable of detecting hidden information in images. This will drive the need for more robust and advanced steganographic algorithms, including BPCS, to withstand such detection methods.

3. **Adaptive and Dynamic Embedding Techniques**: Future enhancements to BPCS-based steganography may involve adaptive and dynamic embedding techniques. These techniques would allow for adjusting the embedding process based on the specific characteristics of the cover image, making it even more challenging for steganalysis algorithms to detect the hidden information.

4. **Hybrid Encryption Techniques**: Integration of BPCS with RSA is just one example of combining steganography with encryption. In the future, researchers may explore hybrid encryption techniques that integrate multiple encryption algorithms, such as AES (Advanced Encryption Standard) or ECC (Elliptic Curve Cryptography), with steganography. This could provide a higher level of security and resilience against attacks.

5. **Multi-Media Steganography**: While BPCS algorithm-based steganography primarily focuses on image hiding, future research may explore extending this approach to other multimedia formats such as audio and video. This expansion could open up new avenues for secure data hiding and communication across various media types.

6. **Cloud-based Steganography**: As cloud computing becomes more prevalent, there may be a shift towards cloud-based steganography solutions. This would involve leveraging the processing power and storage capabilities of cloud platforms to perform efficient and secure steganographic operations, including the integration of BPCS with RSA encryption.

7. **Quantum Steganography**: With the emergence of quantum computing, new cryptographic techniques will be developed to counter quantum attacks. In the future, steganography methods, including BPCS, may need to adapt to quantum-resistant encryption algorithms and techniques to ensure secure data hiding.