Cyber Security
J comp – Review 1

Arshdeep Singh 19BCB0086
Shivam Singhal 19BCE2112
Kartik Nahta 19BCE2009

Brief Description of Project

- Title - Steganographic application using Bit-Plane Complexity Segmentation Algorithm
- We propose to implement a steganographic system that is able to perform all the standard steganographic functions using the Binary Pattern Complexity approach.

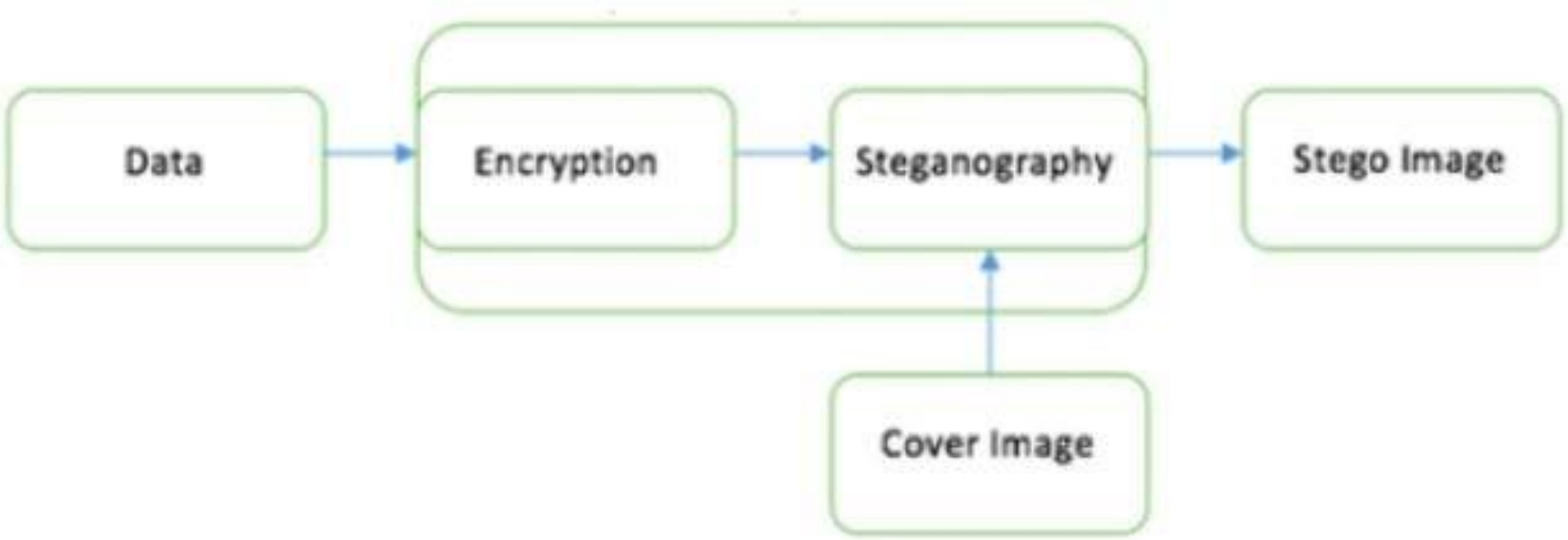
- Language Used
  - Python
- Libraries Used
  - NUMPY
  - Matplotlib

Project Overview

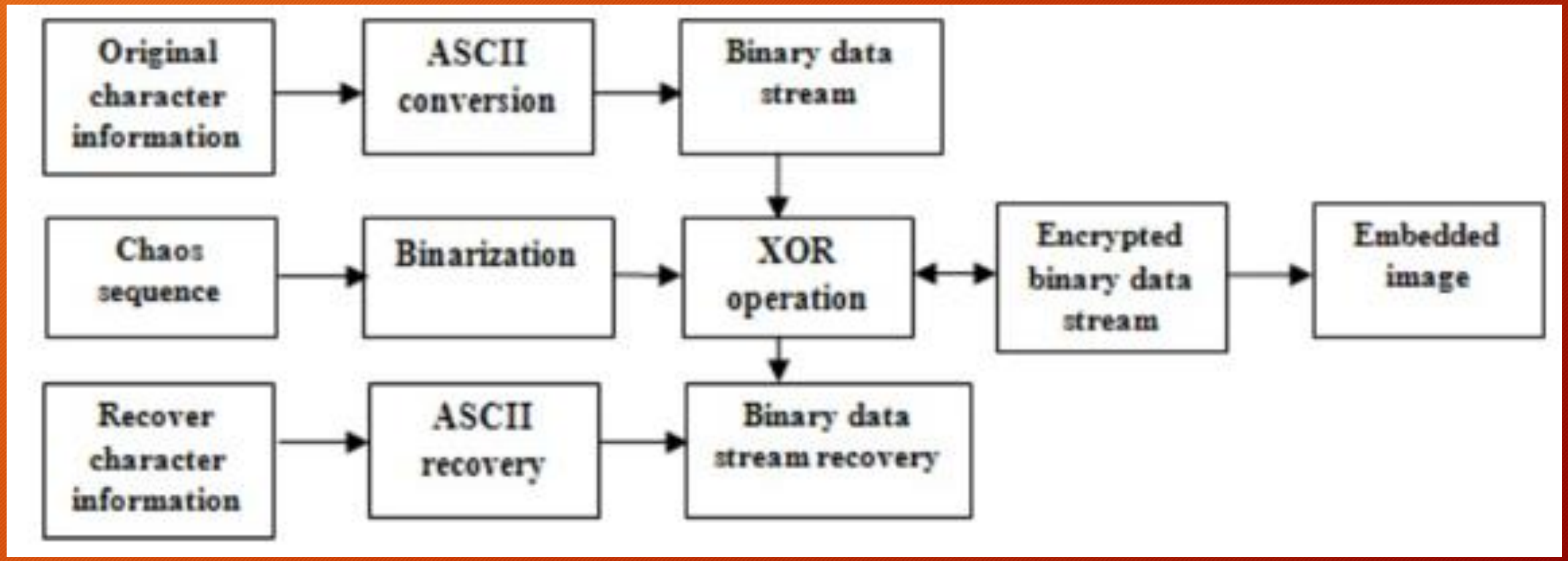
A Steganography system made up of three components:

- Cover-object means which hides the secret message,
- Secret message (information which is meant to be hidden),
- Stego-object means which is the cover object with message embedded inside it.

Flow Diagram



Detailed Flow Diagram



Methodology

- Convert the carrier image from any format into png format.
- Segmentation on carrier image is performed i.e. , Each bit-plane of the carrier image into informative and noise-like regions by using a threshold value (α0). That means complexity of image is calculated.
- Group the bytes of the secret file into a series of secret blocks.
- If a block is less complex than the threshold (α), then conjugate it to make it a more complex block.
- The conjugated block must be more complex than α.
- Embed each secret block into the complex regions of the bit-planes (or, replace all the noise-like regions with a series of secret blocks) where maximum colour changes are observed.
- Convert the embedded dummy image and store.

References

- A Review of Comparison Techniques of Image Steganography By Stuti Goel, Arun Rana & Manpreet Kaur Kurukshetra University https://globaljournals.org/GJCST_Volume13/2-A-Review-of-Comparison.pdf
- Eiji Kawaguchi and Richard O. Eason. (n.d.). Principle and applications of BPCS-Steganography. Citeseerx.ist.psu.edu. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.1018.3664&rep=rep1&type=pdf
- English, R. (2010). Comparison of high capacity steganography techniques. 2010 International Conference of Soft Computing and Pattern Recognition. https://doi.org/10.1109/socpar.2010.5686507

References - 2

- Anderson, R. J., & Petitcolas, F. A. P. (1998). On the limits of steganography. IEEE Journal on Selected Areas in Communications, 16(4), 474–481. https://doi.org/10.1109/49.668971

- Yeuan-Kuen Leea and Ling-Hwei Chen. (n.d.). Secure Error-Free Steganography for JPEG Images. Citeseerx.ist.psu.edu. Retrieved November 23, 2021, from https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.15.7265&rep=rep1&type=pdf