**Methodology**

**AES Algorithm**

In this comparative study of image cryptography algorithms, the work is divided into three stages namely image collecting phase, Encryption phase and Decryption phase. In the image collecting phase various standard image dataset is collected.

After the image acquisition phase, the image will be encrypted using AES algorithm and Blowfish algorithm for the cryptographic process. Advanced Encryption Standard algorithm being the strong cryptographic algorithm has many modes of operation and we will be using AES-CBC (Cipher Blocker Chaining) and AES-ECB (Electronic Codebook) mode of operation for the comparative study.

Decryption

Phase

Encryption

Phase

Image Acquisition Phase

Decrypted Image

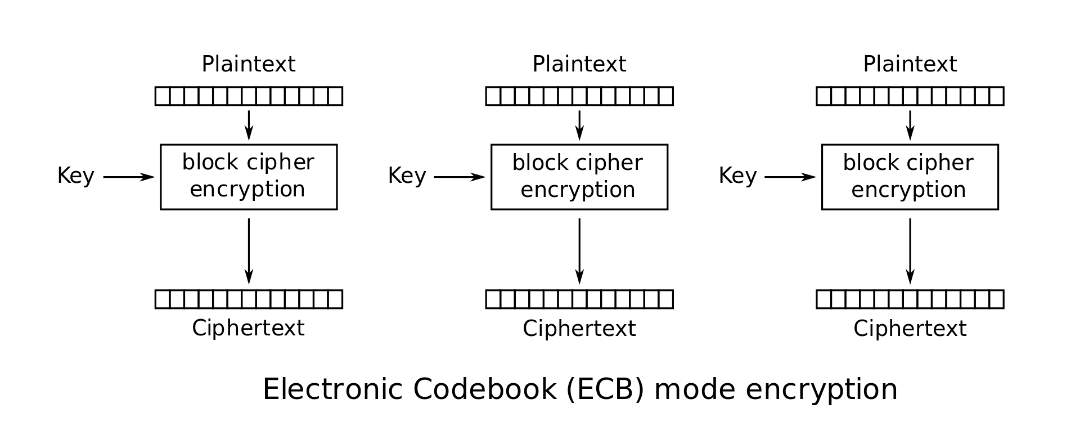
Encrypted Image

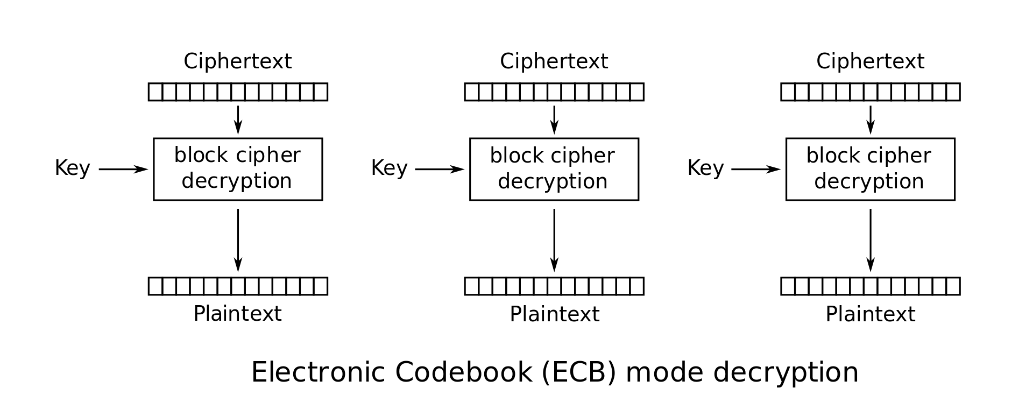
The difference between CBC mode and ECB mode is that CBC mode splits the stream into 16-byte blocks and each block is encrypted using AES and the result is sent to output and XORed with the following block before it gets encrypted. ECB mode is essentially the first generation of the AES. It is the most basic form of block cipher encryption. CBC (Cipher Blocker Chaining) is an advanced form of block cipher encryption. With CBC mode encryption, each ciphertext block is dependent on all plaintext blocks processed up to that point which adds an extra level of complexity to the encrypted data.

The main disadvantage of AES-ECB method is a lack of [diffusion](https://en.wikipedia.org/wiki/Confusion_and_diffusion). Because ECB encrypts identical [plaintext](https://en.wikipedia.org/wiki/Plaintext) blocks into identical [ciphertext](https://en.wikipedia.org/wiki/Ciphertext) blocks, it does not hide data patterns well. In some senses, it doesn't provide confidentiality of the data but it is not in the case of CBC mode where each ciphertext block depends on all plaintext blocks processed up to that point. The uniqueness of the message is achieved by initialization vector used in the first block.

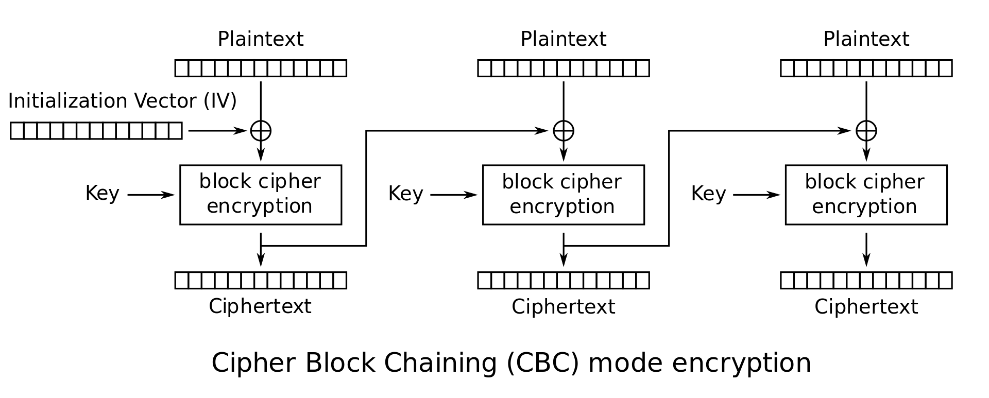
The standard image dataset is acquired from “The USC-SIPI Image Database” is a collection of digitized images and “Blood Cells Images” from Kaggle which has 12,500 images in the dataset are used for cryptographic process and the time required to encrypt and decrypt the image is calculated and compared with respect to database specific and algorithm specific.

**AES – EBC Mode Encryption and Decryption Block Diagrams**





**AES-CBC Mode Encryption and Decryption Block Diagrams**

****

