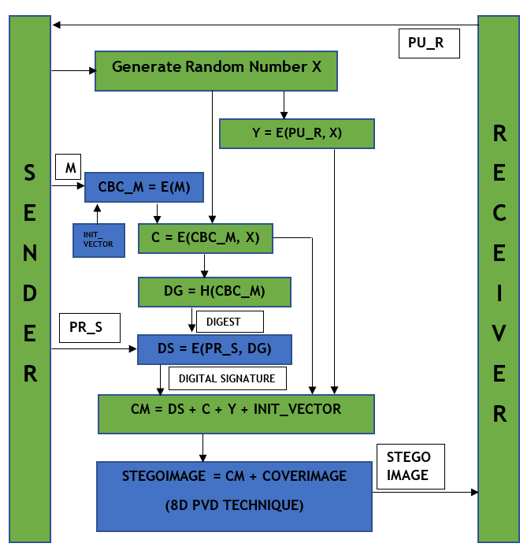
**[Secured-Data-Transmission-SenderEnd-ReceiverEnd-With-Steganography--Text-hidden-in-Image--With-GUI.](https://github.com/esakki712/Secured-Data-Transmission-SenderEnd-ReceiverEnd-With-Steganography--Text-hidden-in-Image--With-GUI.)**

**Sender Side Flow:**

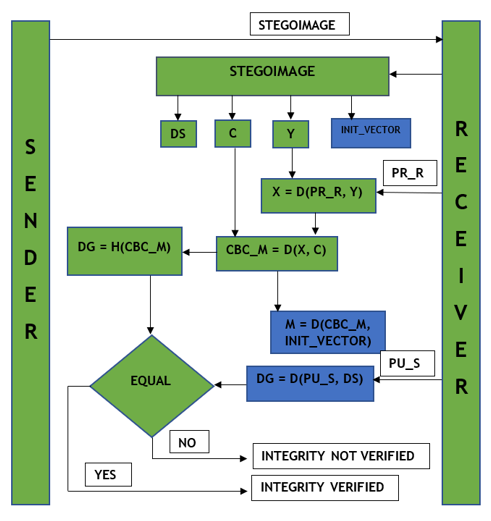


Top of Form

**Sender Side Working:**

* **The public key of receiver will be used by the sender as the ceiling to generate a random number X, which will be acting as the symmetric key to encrypt the message using AES algorithm.**
* **Digest will be generated using SHA512 algorithm, which will be encrypted using the private key of the sender using RSA algorithm. This is called as Digital Signature.**
* **The random number, X is encrypted using the public key of receiver using RSA algorithm. This encrypted key is denoted as Y.**
* **All the encrypted data i.e. encrypted message, encrypted digest, encrypted key is combined together to form the complete message.**
* **Using steganography technique, 8D PVD (Pixel Value Differencing), the whole message will be hidden in the cover image and the output image will be referred as the stego image.**

**Receiver Side Flow:**

****

**Receiver Side Working:**

* **The complete message will be extracted from the stego image and then all the encrypted data, i.e. encrypted message, encrypted digest, encrypted key are separated from the complete message.**
* **Using the private key of receiver, the receiver will decrypt the Y to generate the random number X which will be used as the key to decrypt the encrypted message.**
* **The digital signature will be decrypted using the public key of the sender and the digest will be found.**
* **The hash value from the message is generated which has been denoted as digest.**
* **If the digest from the message and the digest from the digital signature are equal, the message integrity is verified. Otherwise the message integrity is violated.**