Reversible Data Hiding in Encrypted Images byReserving RoomBefore Encryption

Objective:

The methodby reserving Room before encryption with a traditional RDH algorithm, and thus it is easy for the data hider to reversibly embed data in the encrypted image.

Synopsis:

There are also a number of works on data hiding in the encrypted domain. The reversible data hiding in encrypted image is investigated in. Most of the work on reversible data hiding focuses on the data embedding/extracting on the plain spatial domain.This method by reserving room before encryption with a traditional RDH algorithm, and thus it is easy for the data hider to reversibly embed data in the encrypted image. The proposed method can achieve real reversibility, that is, data extraction and image recovery are free of any error.Thus the data hider can benefit from the extra space Emptied out in previous stage to make data hiding process effortless. The proposed method can take advantage of all traditional RDH techniques for plain images and achieve excellent performance without loss of perfect secrecy.

Furthermore, this novel method can achieve real reversibility, separate data extraction and greatly improvement on the quality of marked decryptedImages.Experiments show that this method can embed more than 10 times as large payloads for the same image quality as the previous methods.The data extraction and image recovery can be achieved by examining the block smoothness. After encrypting the entire data of an uncompressed image by a stream cipher, the additional data can be embedded into the image by modifying a small proportion of encrypted data. With an encrypted image containing additional data, one may firstly decrypt it using the encryption key, and the decrypted version is similar to the original image. According to the data-hiding key, with the aid of spatial correlation in natural image, the embedded data can be successfully extracted and the original image can be perfectly recovered.

Existing system:

1. In the existing System more attention is paid to reversible data hiding (RDH) in encrypted images, since it maintains the excellent property that the original cover can be lossless Recovered after embedded data is extracted while protecting the image content's confidentiality.
2. All previous methods embed data by reversibly vacating room from the encrypted images, which may be subject to some errors on data extraction and/or image.
3. Previous methods implement RDH in encrypted images by vacating room after encryption, as opposed to which we proposed by reserving room before encryption. Thus the data hider can benefit from the extra space emptied out in previous stage to make data hiding process effortless.

Disadvantages:

1. The hackers recover the embedding data in original image because the data placed in particular bit position.
2. Previous methods embed data by reversibly vacating room from the encrypted images, which may be subject to some errors on data extraction and/or image restoration.
3. To attack the hidden data using original image because referred the key value.

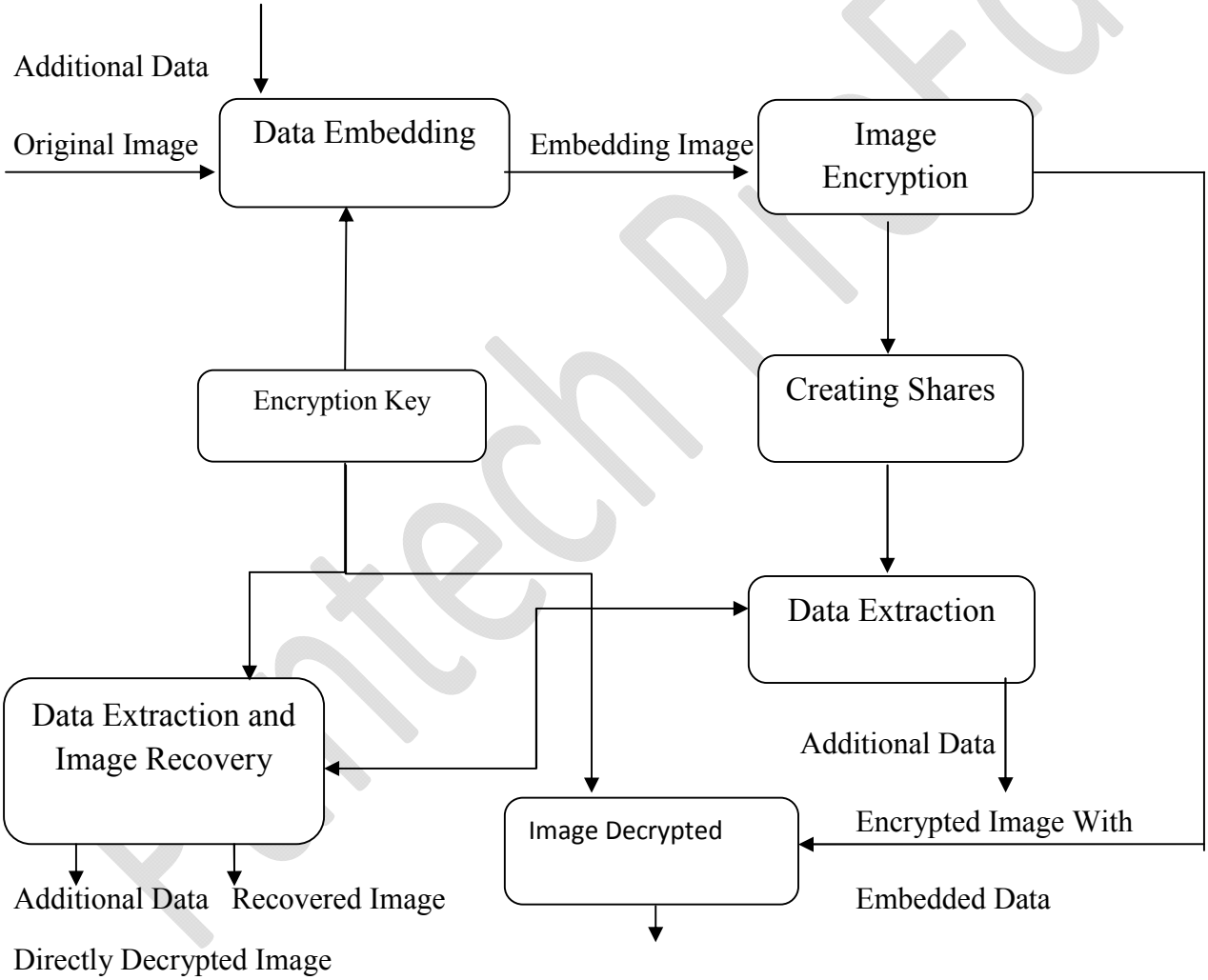
Proposed system:

1. This method can take advantage of all traditional RDH techniques for plain images and achieve excellent performance without loss of perfect secrecy.
2. This method can achieve real reversibility, separate data extraction and greatly improvement on the quality of marked decrypted images.
3. This method by reserving room before encryption with a traditional RDH algorithm, and thus it is easy for the data hider to reversibly embed data in the encrypted image.
4. We can achieve real reversibility, that is, data extraction and image recovery are free of any error.

Advantages:

1. This method can achieve real reversibility, that is, data extraction and image recovery are free of any error.
2. It is easy for the data hider to reversibly embed data inthe encrypted image.
3. This method can embed more than 10 times as large payloads for the same image quality as the previous methods.

Architecture:



Software Requirements:

Language : JAVA, Swing

Hardware Requirements:

OS : Windows 7 32 Bit

Processor : Above 1.5 GHZ

Hard disc : 80 GB

RAM : 1GB