**REVERSIBLE DATA HIDING IN JPEG BIT STREAMS IS AN ENCRYPTION-BASED TECHNIQUE**

**ABSTRACT:**

This paper proposes a novel framework of reversible data hiding in encrypted JPEG bitstream. We first provide a JPEG encryption algorithm to encipher a JPEG image to a smaller size and keep the format compliant to JPEG decoders. After an image owner uploads the encrypted JPEG bitstreams to cloud storage, the server embeds additional messages into the ciphertext to construct a marked encrypted JPEG bitstream. During data hiding, we propose a combined embedding algorithm including two stages, the Huffman code mapping and the ordered histogram shifting. The embedding procedure is reversible. When an authorized user requires a downloading operation, the server extracts additional messages from the marked encrypted JPEG bitstream and recovers the original encrypted bit-stream losslessly. After downloading, the user obtains the original JPEG bitstream by a direct decryption. The proposed framework out-performs previous works on RDH-EI. First, since the tasks of data embedding/extraction and bitstream recovery are all accomplished by the server, the image owner and the authorized user are required to implement no extra operations except JPEG encryption or decryption. Second, the embedding payload is larger than state-of-the-art works.

|  |  |
| --- | --- |
| **EXISTING CONCEPT:-**   * The content owner encrypts the original image using a stream cipher algorithm and then uploads the encrypted image onto the cloud. The cloud server embeds additional bits into ciphertext by flipping three least significant bits (LSB) of half pixels in each block * On the recipient end, the authorized user decrypts the marked encrypted image and generates two candidates for each block by flipping LSBs again. Since the original block of a nature image is smoother than the interfered block, one hidden bit can be extracted and the original block can be recovered. | **PROPOSED CONCEPT:-**   * Reversible data hiding in encrypted images (RDH-EI) is an emerging technique originated from reversible data hiding in plaintext images, which has been investigated by many researchers. In the cloud storage scenario, this technique is realized by a protocol that contains three parties, an image owner, a cloud server and an authorized user. * The image owner encrypts the contents before uploading images onto a cloud storage server. The server hides additional messages into the encrypted images. The RDH-EI protocol guarantees that the hidden message can be exactly extracted by the server, and the original content of the images can be losslessly recovered by the authorized user. |
| **EXISTING ALGORITHM:-**   * This method was improved in using a side match algorithm to investigate the spatial correlation between neighboring blocks. | **PROPOSED ALGORITHM:-**   * RDH-EI first provides a secure encryption algorithm for the owners to encrypt their images before uploading. |
| **ALGORITHM DEFINITION:-**   * This method was improved in using a side match algorithm to investigate the spatial correlation between neighboring blocks. The flipping based approaches are improved in to reduce errors by comparing more neighbor pixels. However, when the pixels in a block have identical values, data extraction and image recovery in may fail. | **ALGORITHM DEFINITION:-**   * On the cloud side, RDH-EI allows the server to label an encrypted image by data hiding, *e.g.*, hiding the identities, timestamps, and remarks into the ciphertext to generate a marked encrypted copy. Therefore, the labels are attached inside the ciphertext, providing a better management for administrators. |
| **DRAWBACKS:-**   * When the pixels in a block have identical values, data extraction and image recovery may fail. A swapping and shifting based RDH-EI method was proposed to overcome this drawback. * Data extraction must be done after image decryption. This limitation makes the technique less useful in cloud storage. | **ADVANTAGES:-**   * RDH-EI is especially useful for labeling the ciphertext in cloud storage. When image owners hope to protect their privacy, RDH-EI first provides a secure encryption algorithm for the owners to encrypt their images before up-loading. |

**MINIMUM SYSTEM REQUIREMENTS:**

**SYSTEM REQUIREMENTS:**

**HARDWARE:**

PROCESSOR : DUAL CORE 2 DUO.

RAM : 4 GB DD RAM

HARD DISK : 250 GB

**SOFTWARE:**

FRONT END : JAVA (J2EE, SERVLETS, JSP)

BACK END : MY SQL

OPERATING SYSTEM : WINDOWS 07

IDE : NET BEANS, ECLIPSE

|  |  |
| --- | --- |
| **PROPOSED SYSTEM** | **FUTURE ENCHANCEMENT** |
| **PROPOSED CONCEPT:-**   * Reversible data hiding in encrypted images (RDH-EI) is an emerging technique originated from reversible data hiding in plaintext images, which has been investigated by many researchers. In the cloud storage scenario, this technique is realized by a protocol that contains three parties, an image owner, a cloud server and an authorized user.      * The image owner encrypts the contents before uploading images onto a cloud storage server. The server hides additional messages into the encrypted images. The RDH-EI protocol guarantees that the hidden message can be exactly extracted by the server, and the original content of the images can be losslessly recovered by the authorized user. | **FUTURE CONCEPT :** -   * The proposed RDH-EI framework focuses on labeling the encrypted JPEG images on cloud storage. There are three par-ties, including the image owner, the cloud server and the authorized user. The owner encrypts a JPEG bitstream and up-loads it to the cloud. The cloud server embeds additional messages into the encrypted bitstream to generate a marked encrypted bitstream. |
| **PROPOSED ALGORITHM:-**   * RDH-EI first provides a secure encryption algorithm for the owners to encrypt their images before uploading. | **FUTURE TECHNIQUE:** -   * The future work can also take into considerations of the Quantum computation approaches which can extend Reversible data hiding in encrypted images for performance enhancement of the existing techniques. |
| **ALGORITHM DEFINITION:-**   * This method was improved in using a side match algorithm to investigate the spatial correlation between neighboring blocks. The flipping based approaches are improved in to reduce errors by comparing more neighbor pixels. However, when the pixels in a block have identical values, data extraction and image recovery in may fail. | **ALGORITHM DEFINITION:-**   * The proposed RDH-EI framework focuses on labeling the encrypted JPEG images on cloud storage. There are three par-ties, including the image owner, the cloud server and the authorized user. The owner encrypts a JPEG bitstream and up-loads it to the cloud. The cloud server embeds additional messages into the encrypted bitstream to generate a marked encrypted bitstream. |
| **ADVANTAGES:-**   * The RDH-EI technique provides an alternative way, which accommodates additional information of the image inside the encrypted bit-stream. Therefore, no metadata files are needed anymore for labeling the uploaded images. | **EXTRAVAGANCE:-**   * In future, images, color information can be separated from texture information, enabling the use of different encryption techniques with different properties for each one, and allowing Reversible data hiding in encrypted images RDH-EI to be performed by third-party, untrusted cloud servers. |

**ALTERNATE TITLE:**

1. New Framework of Reversible Data Hiding in Encoded JPEG Bitstreams.