TUNIS BUSINESS SCHOOL

IT360 PROJECT MAIN CONCEPTS

KENZA BACHA

ASMA BOUBAKER

2023/2024

What is image encryption?

Image encryption involves concealing images to prevent unauthorized access, typically achieved through a secret key. It is a crucial component of Information security that focuses specifically on safeguarding the confidentiality and integrity of digital images. As information technologies continue to advance, digital images—ranging from medical to grayscale, color, and binary formats—are extensively used, stored, and transmitted.

What is the main objective of image encryption ?

The primary objective of image encryption is to transform the visual data within an image into an unreadable and unintelligible form, making it inaccessible to unauthorized individuals. By encrypting images, sensitive information contained within them can be protected from unauthorized viewing, tampering, or interception.

How does it work?

Image encryption methods utilize mathematical algorithms and cryptographic techniques to modify either the pixel values or the visual presentation of an image. These algorithms transform the original image into a ciphered or scrambled form, making it incomprehensible to anyone lacking the correct decryption key.

By encrypting the image, the process guarantees that even if an unauthorized individual obtains access to the encrypted version, they cannot decipher the original content without the proper decryption key.

Functional flow:

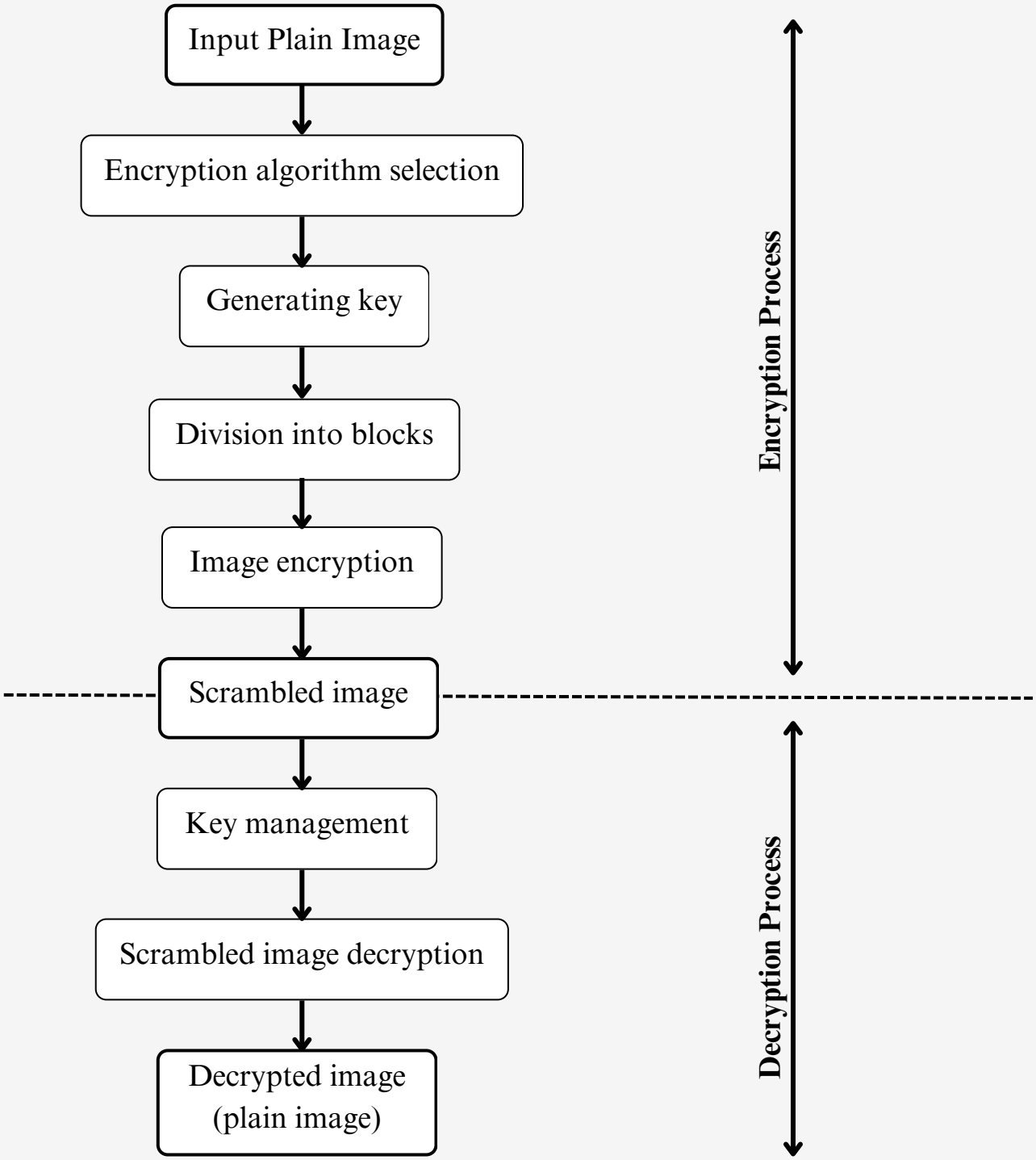
1. **Plain image input:**
   The image designated for encryption serves as the input, which may comprise either grayscale or color variations, expressed through pixel values.
2. **Selecting encryption algorithm:**
   The choice of encryption algorithm is determined by security needs, computational effectiveness, and various other considerations.
3. **Key generation:**
   A secret encryption key, typically a fixed-length sequence of bits or bytes, is generated based on the chosen encryption algorithm. It must be kept confidential and securely shared between the sender and recipient.

4. **Block division:**
   The image is partitioned into smaller blocks or data chunks, with the block size determined by the encryption algorithm and subject to variation. Each block typically contains a fixed number of pixels or bits.
5. **Encrypt image:**
   The encryption algorithm is applied to individual blocks of the image using the encryption key. It conducts mathematical operations on the pixel values within each block, thereby modifying them according to the algorithm's rules, obscuring the original content.
6. **Scrambled image:**
   The entire image transforms into a scrambled version. Pixel values undergo rearrangement and modification according to the encryption algorithm and key. The resulting encrypted image displays a random array of pixels or patterns.
7. **Key management:**
   The encryption key must be securely stored and handled. It should be conveyed to the intended recipient via a secure channel or utilizing another encryption method.
8. **Decrypt the scrambled image:**
   To restore the original image, the recipient employs the same encryption algorithm alongside the proper decryption key. The encrypted image is segmented into blocks, with each block decrypted using the decryption key. This reverses the encryption steps, reconstructing the original pixel values.
9. **Decrypted image:**
   After decryption, the recipient obtains the original image, which is an exact replica of the input image before encryption. The decrypted image can be viewed or processed as required.

Common Image Encryption Algorithms:

- Advanced Encryption Standard (AES).
- Data Encryption Standard (DES).
- Blowfish.
- RSA (Rivest-Shamir-Adleman).
- Elliptic Curve Cryptography (ECC).

Functional flow diagram:



Applications for selective image encryption:

- **Privacy Protection in Medical Imaging :**

Selective image encryption is vital in medical imaging, prioritizing patient privacy. By encrypting specific areas of medical images (like sensitive anatomy or patient ID), healthcare staff limit access to authorized personnel, while leaving other areas visible for diagnosis and treatment.

- **Secure Image Sharing in Cloud Storage**

Selective image encryption is useful in cloud storage when users need to share images while safeguarding sensitive content. By encrypting specific regions or objects within the image, users manage access to confidential information while permitting viewing of other parts.

- **Copyright Protection and Digital Rights Management**

Selective encryption safeguards digital image copyrights. Encrypting particular segments or watermarked areas with valuable or copyrighted content shields creators' intellectual property, facilitating controlled sharing or licensing while thwarting unauthorized reproduction or distribution.

- **Secure Surveillance Systems**

Selective image encryption in surveillance systems safeguards privacy. Encrypting faces or identifiable features of non-target individuals lets security personnel focus on intended subjects, upholding privacy rights.

- **Confidential Document Encryption**

Encrypting crucial sections ensures only authorized individuals can access the content, preserving confidentiality in documents like contracts or reports.

- **Secure Image Forensics**

Selective encryption in image forensics preserves evidentiary integrity by encrypting sensitive regions or metadata. This secures crucial details, ensuring tamper-proof evidence for legal proceedings.