TUNIS BUSINESS SCHOOL

IT360 PROJECT
OVERVIEW OF THE MAIN EXISTING SOLUTIONS

KENZA BACHA

ASMA BOUBAKER

2023/2024

There exist numerous solutions for image encryption, each possessing distinct advantages and drawbacks. Below are several commonly employed techniques:

1- Advanced Encryption Standard (AES) :

Split the image into chunks of AES block size (128 bits), then utilize AES encryption on each block employing a specified mode such as ECB or CBC. In CBC mode, utilize an IV for the first block and XOR subsequent blocks with the previous block's ciphertext before encryption. This process is repeated for all blocks until the entire image is encrypted.

Strengths:

- Efficient encryption/decryption for images, ensuring speed.
- Interoperable across different platforms.
- Flexible key sizes and modes.
- Resilient against brute force and advanced attacks.

Weaknesses:

- Operates on fixed-size blocks of data (128 bits), which may not align well with the structure of image data.
- AES in ECB mode provides deterministic encryption, meaning identical image blocks encrypt to the same ciphertext blocks.
- AES implementations may be vulnerable to side-channel attacks when encrypting images
- Some image encryption schemes may require additional preprocessing or transformation steps to optimize AES encryption for images effectively.

2- Blowfish :

Blowfish encryption for images involves dividing the image into blocks, encrypting each block independently using a generated key, and ensuring data security through diffusion. Decrypting the image involves using the same key to reverse the encryption process and recover the original data.

Strengths :

- Fast encryption and decryption speed
- Flexible key length (32 to 448 bits)
- Effective diffusion of plaintext image bits
- Simple key management processes

- Robust protection against cryptographic attacks

Weaknesses :

- Vulnerable to brute force attacks with advancing computing power.
- Limited adoption may lead to less support and scrutiny.
- Key management complexities persist for large image datasets.
- Aging algorithm raises security concerns regarding undiscovered vulnerabilities.

3- Elliptic Curve Cryptography (ECC) :

Elliptic Curve Cryptography (ECC) efficiently encrypts images by generating a key pair, breaking the image into blocks, and encrypting each block with a random symmetric key. The symmetric key is then encrypted with the recipient's public ECC key and appended to the ciphertext. Decryption involves decrypting the symmetric key with the recipient's private ECC key, allowing the image blocks to be decrypted and reconstructed. ECC's small key sizes and strong security make it ideal for image encryption.

Strengths:

- Shorter key lengths
- faster encryption and decryption processes
- Strong security
- ECC is believed to be more resistant to quantum attacks compared to RSA

Weaknesses:

- Managing ECC keys securely can be challenging, especially in distributed environments or systems dealing with a large number of images
- Potential compatibility issues with older systems or protocols
- Suboptimal configurations or inefficient implementations could impact the overall performance of image encryption systems.

4- Data Encryption Standard (DES) :

For image encryption using the Data Encryption Standard (DES), a 56-bit key is chosen. The image is divided into blocks, each independently encrypted with DES using the key. Decrypting the image involves using the same key to reverse the encryption process and recover the original data.

Strengths:

- Well-established and widely recognized encryption standard .
- Efficient implementation on hardware and software platforms .

Weaknesses:

- Relatively short key length (56 bits), making it vulnerable to brute force attacks
- Prone to security vulnerabilities due to advances in cryptanalysis
- Not suitable for high-security applications due to its limited key length and vulnerabilities

5- Rivest-Shamir-Adleman (RSA) :

RSA, an asymmetric encryption algorithm primarily employed for key exchange and digital signatures, can also be utilized for image encryption in educational, experimental, or compatibility-required scenarios.

Strengths :

- It relies on the difficulty of factoring large integers, making it resistant to attacks by classical computers.
- RSA's asymmetric nature allows for secure key exchange and digital signatures.
- RSA simplifies the distribution of public keys since only the public key needs to be shared for encryption, while the private key remains confidential.
- RSA is a versatile encryption algorithm that can be used for various cryptographic tasks beyond image encryption.

Weaknesses :

- Encrypting and decrypting large image files with RSA can be significantly slower compared to symmetric encryption algorithms like AES.
- Managing RSA keys securely can be challenging, especially in distributed environments or systems dealing with a large number of images.
- May impact storage and transmission efficiency, particularly for large image files.
- Inadequate padding schemes or vulnerabilities in padding implementations could compromise the security of encrypted images.