TUNIS BUSINESS SCHOOL

IT360 PROJECT
HIGH LEVEL DESIGN OF THE PROPOSED SOLUTION

KENZA BACHA

ASMA BOUBAKER

2023/2024

We propose a novel image encryption solution that leverages advanced cryptographic techniques tailored specifically for images. Our solution aims to provide robust encryption while preserving the integrity of the encrypted images. By incorporating innovative approaches inspired by the intrinsic properties of images, our solution offers enhanced security, efficiency, and scalability compared to existing methods.

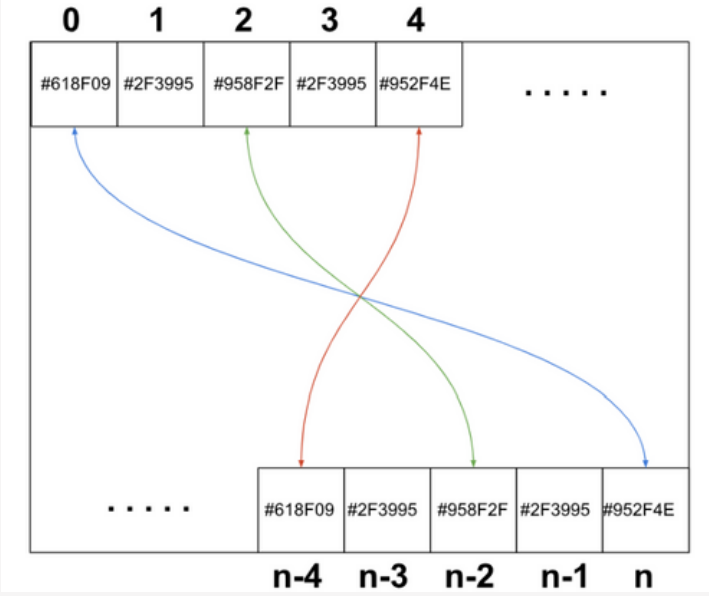
The main goal in this encryption solution is to focus primarily on the Diffusion and Confusion properties of sensitive image data, making it nearly impossible to understand the image visually.

1/Components:

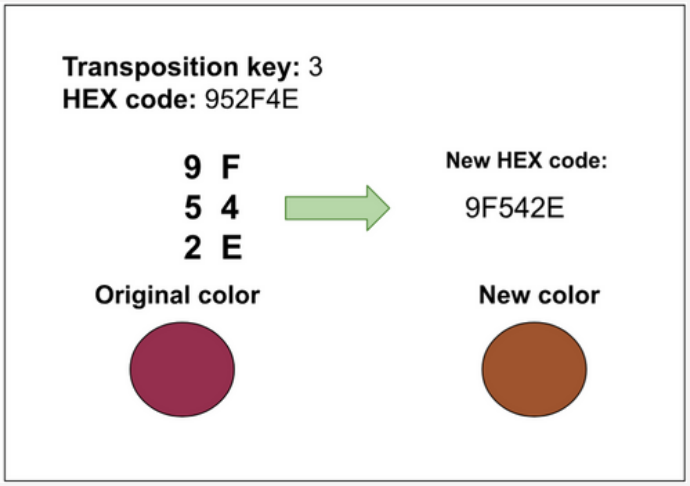
-Encryption Process:

1. **input:** original image and a shared secret key
2. **Explained steps:**

- The original image will be divided into separate pixels.
- Each pixel will have its corresponding HEX color code, they will be ordered in a list.
- A general permutation will be performed on all images' pixels to achieve 'Diffusion' : each pixel with an even index (i) in an ascending order will be permuted with another pixel (n-i) in a descending order, until reaching the middle pixel.



- After performing permutation on pixels, each HEX code will be rearranged using transposition according to a random key; that is, each pixel code will have its own transposition key (the number of transposition keys will be equal to the number of pixels).



- After transposing each pixel, all keys will be arranged in a single long string according to the order of permuted pixels constructing the Transposition Key needed to decrypt the image.
- The image is then reconstructed using the newly generated HEX color codes.
- In addition, the transposition key will be encrypted using the AES algorithm with the first shared secret key used.

3.**Output:** encrypted image and an encrypted transposition key

-Decryption Process:

1.**Input:** encrypted image, encrypted transposition key, and a shared secret key

2.**Explained steps:**

- With the shared secret key, the receiver will decrypt the encrypted transposition key.
- The encrypted image will be also divided into pixels, and transformed into a list of HEX color codes.
- Using the decrypted transposition key, each HEX code will be decrypted according to its transposition key (they both have the same index; in the string and in the list).
- After getting back all original colors, the same general permutation described before will be performed on the obtained pixels.
- Finally, the image will be reconstructed again using the decrypted pixels.

3.**Output**: Decrypted original image.

2/Key Exchange Algorithm Used:

In order for both users to encrypt and decrypt the image, they will be using the Diffie-Hellman key exchange algorithm.

1. Generate a prime number and a base value that are public: g and q
2. Both sender and receiver will calculate their public keys using their own private keys.
3. Then they exchange the public keys generated.
4. Finally both parties calculate the shared secret key needed to encrypt and decrypt the target image

=> the output will be a shared secret key used in encryption and decryption processes.

3/Functional Flow: Exchanged Messages/Data

-Encryption Flow:

Sender:

- Choose the image to encrypt.
- Obtains the shared secret key using the Diffie-Hellman key exchange algorithm.
- Uses the encryption algorithm developed to encrypt the image using the shared secret key.
- Sends the encrypted image along with the encrypted transposition key.

-Decryption Flow:

Receiver:

- Receives the encrypted image and the encrypted transposition key.
- Obtains the shared secret key using the Diffie-Hellman key exchange algorithm.
- Uses the decryption algorithm developed to decrypt the transposition key and the encrypted image using the shared secret key.
- Obtains the original image

4/Users:

-Sender: Calculates the shared secret key, initiates the encryption process, selects the image, and shares the encrypted image with the receiver.

-Receiver: Receives the encrypted image, calculates the shared secret key, and decrypts it to obtain the original image.