TUNIS BUSINESS SCHOOL
UNIVERSITY OF TUNIS

IT 360
INFORMATION ASSURA NCE & SECURITY

Security Project
Image Encryption

Authors:
Majd Hamdi
Seif Ben Soltana

Submitted to:
Prof. Manel Abdelkader

Introduction:

Image encryption plays a crucial role in safeguarding visual data from unauthorized access, tampering, or interception. It ensures the **confidentiality**, **integrity**, and **privacy** of images, which are often valuable assets in various domains such as healthcare, finance, military, and personal communications.

With the proliferation of digital imagery and the increasing reliance on image-based communication, the importance of image encryption has grown significantly to protect sensitive information and preserve the trust of users.

Some Concepts Explained:

Image encryption:

Fundamentally defined as the process of transforming a plain image into a coded form that can only be deciphered by its intended recipient.

Chaotic Systems:

The concept of chaotic systems is rooted in chaos theory, a branch of mathematics and physics that studies the behavior of dynamical systems that are highly sensitive to initial conditions, exhibit complex and unpredictable behavior, and appear random despite being deterministic.

In the context of implementing them in image encryption; chaotic sequences produced by chaotic systems act as pseudorandom elements, employed to scramble and disperse a plaintext image.It offers advantageous characteristics like non-linearity, sensitivity to initial parameters, speed, and robustness.

Each pixel value in the image is typically represented by an integer between 0 and 255 (for an 8-bit grayscale image) or three integers (for a color image). The chaotic sequences generated are used to modify the pixel values in the image.

Components of image encryption:

Plain Image: The original image that needs to be encrypted.

Encryption Algorithm: The method used to encrypt the plain image. It transforms the image into a cipher image using a secret key.

Secret Key: A critical element in the encryption process, which ensures that only authorized parties can decrypt the image.

Cipher Image: The encrypted version of the plain image, which should appear as random noise to unauthorized viewers.

Functional Flow:

Input: The plain image is inputted into the encryption system.
Preprocessing: Transformation of the image into a suitable format for encryption (e.g., converting to grayscale, resizing, normalization, color space conversion).
Key Generation: A secret key is generated, often using complex algorithms to ensure security.
Encryption Process: The plain image is transformed into a cipher image using the encryption algorithm and the secret key.
Output: The cipher image is produced, ready for secure transmission.
Transmission/Storage: The encrypted image can now be securely stored or transmitted.
Decryption: Using the decryption algorithm and the cipher key to convert the cipher image back to the original image.
Test Performance

Algorithms used:

Traditional Ciphers:

AES (Advanced Encryption Standard) encrypts images by dividing them into blocks and applying multiple rounds of complex transformations, ensuring that only those with the correct key can decrypt and view the image. Its key sizes can be 128, 192, or 256 bits, providing strong protection against brute-force attacks.

DES (Data Encryption Standard) is an older symmetric key encryption algorithm that operates on 64-bit blocks using a 56-bit key. It’s less secure than AES due to its shorter key length and is vulnerable to brute-force attacks.

RSA (Rivest-Shamir-Adleman) can encrypt the image or the key used for another encryption method, like AES, ensuring that only the holder of the private key can decrypt the image.

Chaotic Systems:

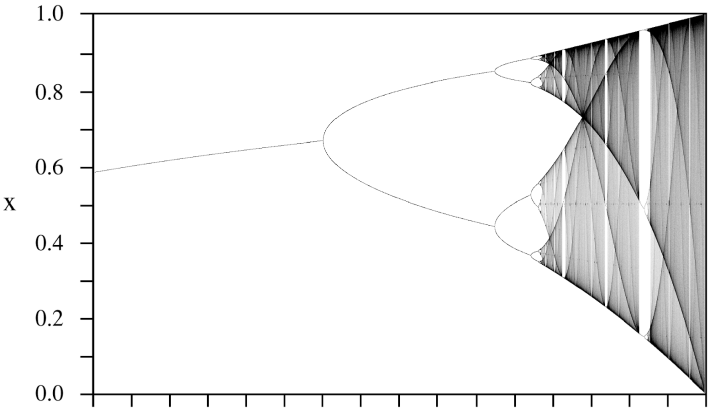
While the basic principles of using chaotic maps for image encryption **remain consistent** across different maps (**generating chaotic sequences** and applying them to **modify pixel values**), the specific implementation details and encryption algorithms may vary.
Different chaotic maps may have distinct properties and behaviors that influence the encryption process, such as the type of transformations applied to the image data or the nature of the pseudorandom sequences generated.
Examples of chaotic systems include: Logistic Map, Arnold Map, Duffing and Henon map.

Brief Mathematical explanation behind Chaotic Systems:

Logistic map:

$$X_{n+1} = rX_n\,(1 - X_n)\,,$$

where X_o represents the initial parameter or starting value of the logistic map,
with $0 \leq X_i \leq 1$. The parameter, r, is the control parameter or growth rate of the logistic map, and it has a range of (0, 4). However, chaotic behavior is observed only when the control parameter, r is within the range of (3.56995, 4).



bifurcation diagram : illustrates how the behavior of a system changes as a parameter of the system is varied.

Arnold Map:

The Arnold map, which was introduced by Vladimir Arnold in 1968, is a nonlinear chaotic transformation that maps a unit square into itself, exhibiting chaotic behavior; this is desirable in image encryption for producing pseudorandom sequences. The Arnold map can be represented by the following formula:

$$\Gamma(x_{n+1}, y_{n+1}) = (2x_n + y_n, x_n + y_n) \mod N,$$

where (x_n,y_n) and (X_{n+1}, Y_{n+1}) are the coordinates of a point in the unit square before and after the transformation, respectively. N is the size of the unit square.

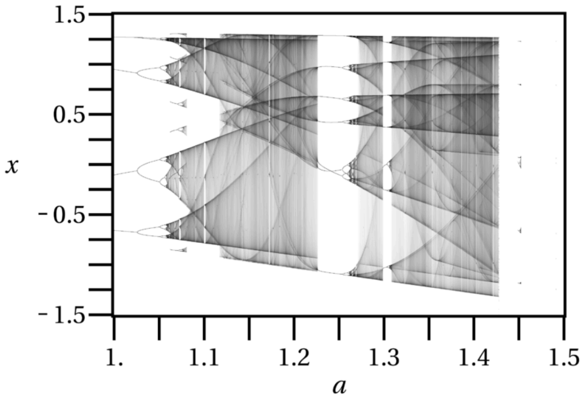
Henon Map:

The Henon map is a two-dimensional map that maps a point (x_n, y_n) to a new point (x_{n+1}, yn+1). The Henon map can be defined as follows:

$$\begin{aligned} x_{n+1} &= 1 - ax_n^2 \\ y_{n+1} &= bx_n, \end{aligned}$$

where (x_n, y_n) and (X_{n+1},y_{n+1}) are the coordinates of a point before and after the mapping, respectively; a and b are the control parameters for the Henon map; however, the map starts to behave chaotically when

a = 1.4 and b = 0.3 . The bifurcation diagram for the Henon map is depicted in:



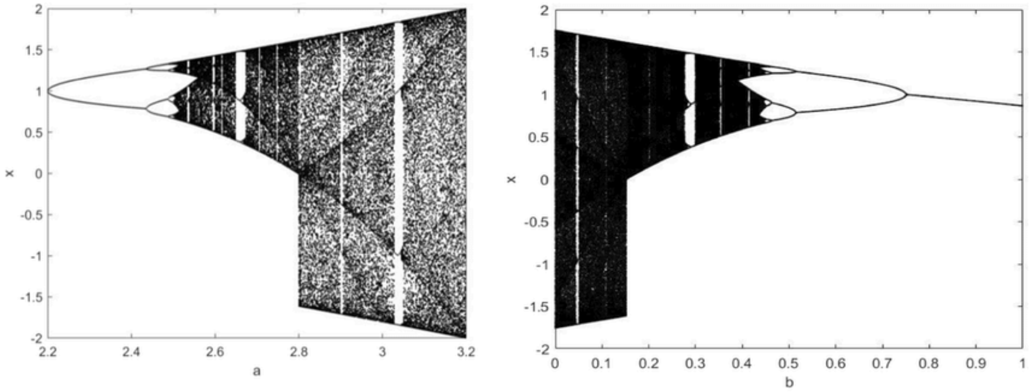
Duffing map:

The Duffing map also called the 'Holmes map' is a discrete-time dynamical system. It is an example of a dynamical system that exhibits chaotic behavior. The Duffing map takes a point (x_n, y_n) in the plane and maps it to a new point given by:

$$\begin{cases} x_{n+1} = y_n \\ y_{n+1} = -bx_n + ay_n - y_n^3 \end{cases}$$

The map depends on the two constants a and b. These are usually set to a = 2.75 and b = 0.2 to produce chaotic behavior.

The bifurcation diagram is depicted as:



(a) **(b)**