CS 512 - FINAL PROJECT

Analysis of Cryptography Algorithms for Images

Understanding the basic terminologies

- What is Encryption?

  Encryption is the process of transforming any digital data item into a form that can only be read by authorized individuals.

- What is Cryptography?

  Cryptography is the process of encrypting and decrypting the data.

- **Why Image Encryption?**
  - Images are one of the prominent ways of communication
  - Security is considered as the top priority for these digitally transmitted images

Image Encryption Algorithms that we have used

- RSA Algorithm
- Arnold’s cat map algorithm
- Henon map

How is data modified?

- A single image is given as input.
- We extract the pixels from the given input image and obtain the Red, Blue, and Green colors from each pixel.
- We apply our image encryption and decryption algorithms on these pixel data.
- We modify this pixel information to encrypt the input image to obtain the encrypted image.
- We apply the pixel information from the generated encrypted images to regenerate the original image back.

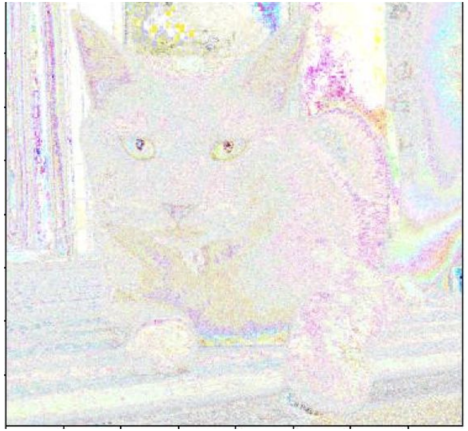
RSA Algorithm

- Asymmetric cryptographic algorithm that uses public key and private key.

- Since this is asymmetric, nobody else except the decrypter can decrypt the data even if a third party has the public key of the browser.

RSA Algorithm for a given image

Asymmetric cryptographic algorithm that uses public key and private key.



Advantages and disadvantages of using RSA Algorithm.

Advantages:

- No Key Sharing
- Proof of Authenticity
- Data cannot be corrupted

Disadvantages:

- Due to the fact that RSA only uses asymmetric encryption and both symmetric and asymmetric encryption are necessary for full encryption, it may occasionally fail.
- Due to large numbers involved the rate of data transfer is slow.
- The dependability of public keys occasionally needs to be verified by a third party.
- Decryption requires intensive processing on the receiver's end.
- For public data encryption, such as electoral voting, RSA cannot be utilized.

Image encryption using Chaotic maps

What is a Chaotic map?

Application of chaos theory to the principles of cryptography.

What are the different types of chaotic maps

One dimensional and multidimensional maps.
One dimensional - logistic map, sine map, tent map, and Arnold cat map.
Multidimensional maps - Henon map and 2D logistic map

Advantages of Chaotic Maps over traditional algorithms

- Simple functions and are iterated quickly
- High security
- Less cost for computation

Arnold’s Cat map Algorithm

- Non-linear chaotic map
- Process where we rearrange the pixels in a given image without losing any information.

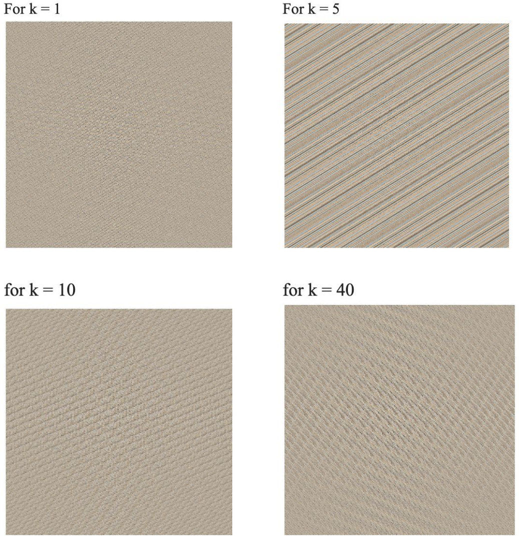
For every iteration, the value of image[x][y] is modified as

[x] = [2*x+y]%n
[y]= [y+x]%n

Arnold cat’s Map algorithm for a different values of k

Input Image

Encrypted images for different values of k



For k = 1

For k = 5

for k = 10

for k = 40

Decrypted image

Henon Map

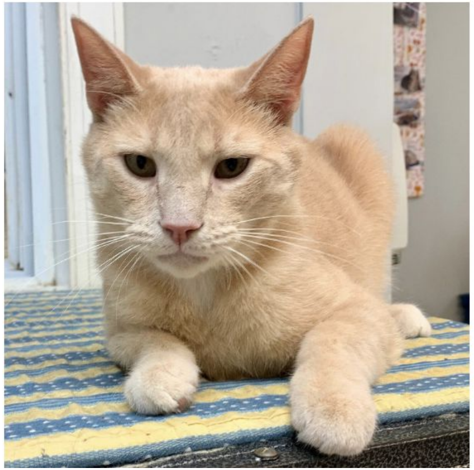
Henon map may be stated as a two-dimensional iterated discrete-time dynamical system with a chaotic attractor

It is mainly stated by the following two equations

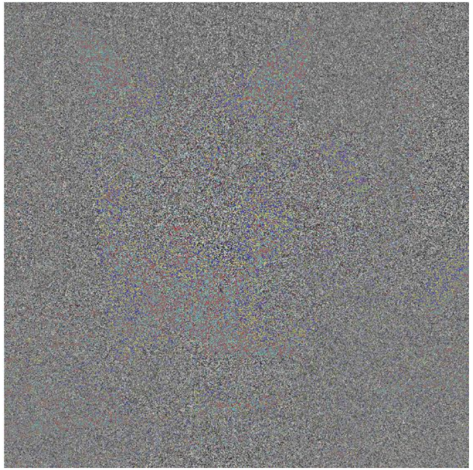
$$x(\,n + 1) = \ 1 - \alpha * (x(n) \wedge 2) + y(n)$$
$$y(\,n + 1) = \beta * x(n)$$

Henon map implementation on an image

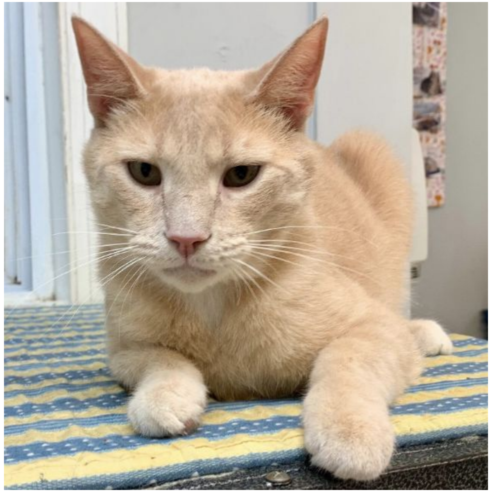
Input Image



Encrypted Image

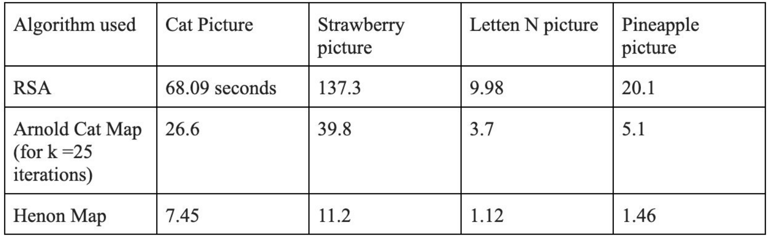


Decrypted Image



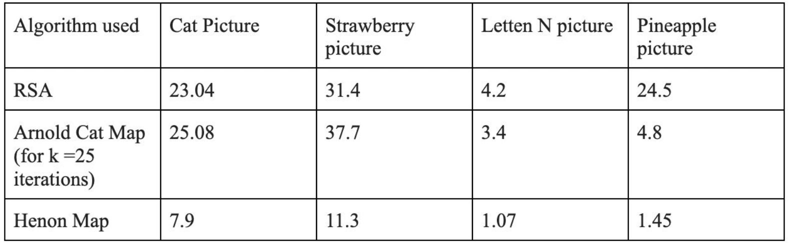
Analysis on all the three algorithms

Time taken for Encryption of the 4 images:



Algorithm used	Cat Picture	Strawberry picture	Letten N picture	Pineapple picture
RSA	68.09 seconds	137.3	9.98	20.1
Arnold Cat Map (for k =25 iterations)	26.6	39.8	3.7	5.1
Henon Map	7.45	11.2	1.12	1.46

Time taken for Decryption of the 4 images:



Algorithm used	Cat Picture	Strawberry picture	Letten N picture	Pineapple picture
RSA	23.04	31.4	4.2	24.5
Arnold Cat Map (for k =25 iterations)	25.08	37.7	3.4	4.8
Henon Map	7.9	11.3	1.07	1.45