**Image Cryptography:**

It is a technique that allows visual images to be encrypted and decrypted to make it even more secure while transferring data. Security of Multimedia/Data/ Images is a crucial aspect, and still an expanding domain. The rapid growth of digital media and multimedia based applications has increased the requirement of transmitting them over public networks. The key obstacle in such applications for scientiﬁc and research community has been the efficient and secure transmission over the network. Hence there is a need for effective encryption techniques for secure data transfer. Image Cryptography is a vast branch, with lot of research going on till date to create new encryption techniques, development is necessary to make encryptions more secure. Various Techniques have been proposed till date, each have an edge over other, to catch up with ever growing need for security. There is a need for protecting images from ***differential, quantitative and statistical attacks*** which when resisted make an image secure from cyber threats. The measure of efficacy among all these modern and grown-up techniques such as Advanced Encryption Standard (AES), Data Encryption Standard (DES), Rivest–Shamir–Adleman (RSA) etc., which exhibit low levels of security, it is identified that ***chaotic schemes*** provides highly scrambled encrypted images. There are different techniques of image encryption, symmetric, asymmetric, spatial domain (based on pixels), frequency domain, full encryption, partial encryption. Using these techniques researches have developed many algorithms. Each technique has 4-5 different types of algorithm proposed by various researchers. Selection of an algorithm is based according to required characteristics of security, processing speed, computation speed, complexity etc.

**What is 2D and 3D Images?**

A digital image is either a gray image represented as two dimensional matrix (2D) having pixel intensities or a colored image represented as three dimensional matrix (3D) or RGB matrix where the three planes of matrix corresponds to red, green and blue.

**Different Cyber Attacks on Images**

* Statistical Attack : While embedding the message in a medium, there are certain statistical properties of the medium that need to be maintained. If not maintained, they can reveal the existence of a hidden message.
* Differential Attack : This attack relies on the fact that input/output difference patterns occurs for a certain value of inputs. Observing the differences, the possible key value is obtained.
* Brute Force Attack : This attack uses trail-and-error method to guess encrypted keys. It involves systematically checking all possible key combinations until the correct key is found. The key length used in the encryption determines the practical feasibility of performing a brute-force attack. longer keys exponentially increase the difficulty to crack.

Attack are done by predicting the type of Algorithm used for the encryption, thereby identifying its weaknesses and using it to their advantage.

**Cryptanalytic**

Cryptanalysis is the process of analyzing the cryptographic algorithm and the breaking of those secret codes. It helps us to better understand the cryptosystems, also helps us improve the system by finding any weak point and thus work on the algorithm to create a more secure secret code. An algorithm is tested against all these attacks before it is implemented.

**Chaotic Schemes :**

This concept is derived from Mathematics concept called Theory of Chaos which discusses about the nonlinear things that are effectively impossible to predict or control and are highly sensitive to the initial conditions. Despite their deterministic simplicity, over time these systems can produce totally unpredictable and wildly divergent (aka, chaotic) behavior. Chaos based algorithms provide a good combination of ***speed, high security complexity, low computational overheads***.

The important characteristics of a Chaos are as follows:

• it must be sensitive to initial conditions

• it must be topologically mixing

• it must have dense periodic orbits

In general**, this means that a small variance in the initial parameters (even in ten-millionth place value) could yield widely divergent results**. Applying properties of chaos-based encryption algorithms will increase the complexity of the cipher image. It can be said that any function that fulfils these behaviors are called a ***Chaotic function***. The map or the graph obtained by plotting the values which is again found by infinite iteration of that function is called ***Chaotic Map*** for that function. In the recent years, researchers have developed many Chaotic Maps by studying different real life incidents or events. These maps are widely used for different encryption techniques specially for image encryption. The first challenging task is the selection of chaotic map(s) which will be suitable according to the designers’ encryption objectives.

There are different types of Chaotic Maps, some of them are:

* Henon Map
* Arnold Cat Map
* Chen’s Chaotic Map
* Logistic Map
* Chebyshev Map

**Dimension Domains for Chaotic Systems :**

Current Image encryptions systems depend on the chaotic sequence but mostly in low-dimensional domains   
(1D & 2D). They offer limited security and provide inadequate key space and have inherent disadvantages. 3D functions offer greater security against cryptanalytic attacks. Hence these are in focus of new research. The 2D maps are extended to 3D and then the encryption schemes are applied.

**Advantages of Chaotic Schemes :**

* These schemes can resist ***statistical attacks*** as these showed very less degree of correlation coefficient values in horizontal, vertical, and diagonal directions.
* These schemes can resist ***differential attacks*** as these showed a high sensitivity for the initial conditions, i.e. pixel and key values.
* Finally, these schemes provide a large key spacing, hence can resist the ***brute force attacks***, and provided a ***very less computational time*** for image encryption/decryption in comparison to other schemes available in literature.

**Chaotic Map based Encryption and Decryption Model :**

Though there are several Chaotic Map based Image Encryption Techniques are available, but the whole process or techniques can be generalized into three different phases. These three phases are followed in all Chaotic Map based Image Encryption. These are:

* Selection of Chaotic Maps
* Confusion
* Diffusion

**Step Involved**

1. Initially Different types of chaotic maps and its behavior must be analyzed. Depending on user requirement one or more map needs to be selected.
2. The next step is to select a secret key to be used of initial condition with effective length considering brute force attacks.
3. After that selected chaotic map is ready to use in encryption process in iterative basis.
4. In Confusion stage chaotic mapping functions are applied to the original image to rearrange the pixel values. This process may be repeated several times to give more confusion to the output image.
5. **In confusion phase, original image is changed due to the interchange of pixel values but the histogram of both the images are still same. So, it may easier for attacker to retrieve the original image with help of histogram equalization. Hence Diffusion is performed**
6. The main objective of diffusion is to change the image pixel values so that histogram of the original image and encrypted image will be completely different. Each pixel values of the output generated by confusion stage is XORed with the chaotic function values. This step can also be repeated for multiple times to achieve the higher security level.
7. In decryption model the process is repeated in reverse order. But the main difference is that here, everything is predefined, i.e., chaotic maps, key, diffusion technique and confusion technique. The key has to be considered same as used in encryption model. Then to calculate the initial states and constants same process has to be followed. Once the chaotic map is ready to use, first diffusion step has to done on encrypted image in reverse order. The output of the diffusion step will be the input of confusion step. Finally, after completion of confusion step, final decrypted image can be retrieved.

***NOTE : For a successful Cryptography Model Histogram of Original and Encrypted Image needs to be difference and also Correlation between pixel after encryption needs to be distorted.***

**Image Storage:**

**Bits per pixel (Bpp)** denotes the number of bits per pixel. The number of different colors in an image is depends on the depth of color or bits per pixel. *8 Bpp usually means that there are 256 colors*.

**Image Size :** The size of an image depends on three things, rows, columns, bits per pixels.

**Size of an image = row \* columns \* bits per pixels**

**Type of Image Formats :**

There are many types of Image formats **jpg, jpeg, png, bmp** etc., usually the image file are **vectors/tuples** with RGB format i.e., each pixel has three channel Red, Green, Blue. But **BMP** file format is an Exception

**BMP (Bitmap Image Format)** : A bitmap image is a **raster** image (containing pixel data as opposed to vector images) format. Each pixel of a bitmap image is defined by a single bit or a group of bits. The **image** is represented in a series of **bits/integer** of information that translate into pixels on the screen. Hence, it is called the **bitmap** or a **map of bits and pixels**. It was designed by **Microsoft Corporation** to easily exchange images between different devices without worrying about the device’s logic to display raster images on the screen.

**Checking Proper Encryption :**

After completion of Image Encryption process, it is required to check for security of the encrypted image, which is done using various verification but the most important among them are, checking for the ***Histogram relation and Correlation*** between original image and encrypted image.

**Histogram** : Even if the pixels are jumbled from original image and encrypted image the histogram values of the two images remains the same, this make the image vulnerable for attacks. So, to ensure proper security the histogram value of the images need to defer, A proper Encryption must make sure that the Histogram values doesn’t match.

**Correlation** : An original image has correlations between adjacent pixels, which shouldn’t exist after the image is encrypted. A proper Encryption must make sure that there is no correlation between the pixel of the encrypted image

**Following the above two steps for verification is must and only then the encryption is secured.**

**Henon Map :**

Henon Map is one of the chaotic methods of encryption which encrypts images based on Pseudo-random sequence. It is based on Mathematical Formulas.

Xn+1 = 1+Yn – aXn2

Yn+1 = bXn

Where n=0,1,2..

a,b are initial parameters, (X0,Y0) is the initial point is . Each point  (Xn,Yn) is mapped to a new point (Xn+1,Yn+1) through the Henon map.

Here, the parameters, a and b are prime importance as the dynamic behavior of system depends on these values. The system cannot be chaotic unless the value of a and b are 1.4 and 0.3 respectively. For other values of a and b, the map behaves as chaotic, intermittent, or obtain a periodic orbit.

Initial points X1 and Y1 work as a symmetric key for chaotic cryptographic system used for encryption at sender’s end and decryption at receiver’s end. Since Henon map is deterministic so the decryption is possible at receiver’s end with the same initial points X1 and Y1. Thus, sensitivity of key and encryption algorithm together contributes to avoid all kind of cryptanalysis attacks

**Algorithm for Henon Map :**

* Converting Original Image into Matrix of Pixels.
* Choose the initial value of (X0,Y0) for Henon map. This value works as an initial secret symmetric key for Henon map.
* Creating Henon map work as a key stream generator for cryptosystem. The size of sequence depends upon the size of image. If the image size is m×n then the number of henon sequence will be m×nx8 (8 bits per pixel).
* Xn+1 = 1+Yn – 1.4Xn2

Yn+1 = 0.3Xn

Where n=0,1,2..

* Based on these formulas next iteration values are calculated are updated.
* The value of bit is determined by Xi. Experimental analysis concludes that cut-off point, 0.3992, has been determined so that the sequence is balanced. The bit values are determined based on the threshold value as given where Z is a binary sequence.

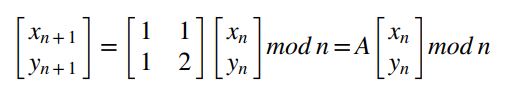
**Zi = 0 if Xi <= 0.3992 / 1 if Xi >= 0.3992**

* Henon Binary sequence is converted into decimal (ever 8 bits are converted into decimal) and is stored into byte array
* Byte Array is then converted into **Transformation Matrix/Henon Map Matrix** (ever mth byte in byte array is stored as a new row to form Matrix)
* Encryption is done by bitwise Exclusive-OR operation between Image Matrix and Transformation Matrix.
* Decryption is done in the same way but the initial values (X0,Y0) which is the key needs to be supplied, reverse XOR operation between Image Matrix and Henon Matrix gives back Original Image.
* Perform Histogram and Correlation Analysis to check the security of the Chaotic Map.

**Arnold-Cat Map :**

**Arnold's cat map** is a chaotic map, named after Vladimir Arnold, who demonstrated its effects in the 1960s using an image of a cat, hence the name. It is used for mapping of two dimensions can be used to change the position of the pixel of the image without removing any information from the image.

**The Matrix Notation** :



**This notation can be expressed as when matrix multiplication is done :**

R([X,Y]) = [(X + Y) mod n, (X + 2Y) mod n] where n is the dimensions of the image

In Arnold’s cat map the determinant of matrix used for transformation is 1, due to this the it has **invertible property** (i.e., when pixels of image are transformed using this matrix, original image can be retrieved since it invertible)

It is possible to define a discrete analogue of the cat map. One of this map's features is that image being apparently randomized by the transformation but returning to its original state after a number of steps.

Calendar

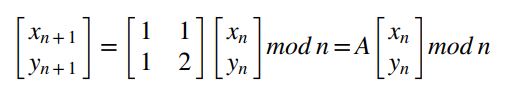
Description automatically generated

**When the transformation is repeated enough times, the original image will reappear.**

The number of iterations 'n' at which the original image will reappear is given by these rules of thumb: Here 'd' is the dimension of the square image:

1. if d = 2.(5^i) for i >=1, n = 3\*d
2. if d = (5^i) for i >=1, n = 2\*d
3. if d = 6.(5^i) for i>=1, n = 2\*d
4. else n <= 12\*d / 7

**Algorithm for Arnold’s Cat Map :**

* Converting Original Image into Matrix of Pixels
* Creating **Arnold’s Cat Map Matrix/ Transformation Matrix** based on the Formula
* 
* R([X,Y]) = [(X + Y) mod n, (X + 2Y) mod n] where n is the dimensions of the image
* Performing Arnold’s Cat Encryption i.e., iterating the image based on Matrix Formula for certain number of time (KEY). Here each and every pixel coordinates of the image are transformed. When all the coordinates are transformed, the image resulted is a scrambled image/ encrypted image.
* To perform Arnold’s Cat Decryption calculating the number of iterations required to get the original image in necessary.
* The number of iterations 'n' at which the original image will reappear is given by these rules of thumb: Here 'd' is the dimension of the square image:

1. if d = 2.(5^i) for i >=1, n = 3\*d
2. if d = (5^i) for i >=1, n = 2\*d
3. if d = 6.(5^i) for i>=1, n = 2\*d
4. else n <= 12\*d / 7

* To decryption of image rest iterations needs to be followed after the secret key to retrieve the image, this is called transformation periods (i.e., the number of iterations to be followed = Arnold’s period − secret key)
* This periodicity forms the crux of the encryption process. Here key is the number of iterations of transformations initially applied to get the encrypted image. n - key is the number of rounds of transformations applied to get the decrypted image.