Chapter one
Introduction

CHAPTER I
Introduction

1.1. Background

With the fast progression of data exchange in electronic way (public or local networks) information security is becoming more important in data storage and transmission. Because of widely using satellite images in industrial and government process e.g., confidential transmission, land and sea surfaces, analysis of air masses to monitor the thermodynamic state in the lower part of the atmosphere and environment data collection and relay transmitted by automatic platforms (marine beacons, land and airborne ...) [1]

Image is one of the important forms of multimedia it is carry important information. Image visually present information and information presented by a richer image than presented textually. Digital images (multimedia) are not only stored in the storage such as hard disks, flash drives, CDs, DVDs, and other storage device, but also transmitted via public or private channels in the internet.

multispectral imaging for providing electronic images of clouds it is important to protect the confidential image data from unauthorized access.

Traditional image encryption algorithms such as private key encryption standards (DES and AES), public key standards such as Rivest Shamir Adleman (RSA), and the family of elliptic-curve-based encryption (ECC), as well as the international data encryption algorithm (IDEA), may not be the most desirable candidates for image encryption, especially for fast and real-time communication applications. In recent years, several encryption schemes have been proposed These encryption schemes can be classified into different categories such as value transformation, pixels position permutation and chaotic systems [22]

in this recherché algorithm is use is the chaotic mapping called Arnold's cat map in recognition of Russian mathematician Vladimir I. Arnold, who discovered it using an image of a cat. It is a simple and elegant demonstration and illustration of some of the principles of chaos – namely, underlying order to an apparently random evolution of a system. An image (not necessarily a cat) is hit with a transformation that apparently randomizes the original organization of its pixels. However, if iterated enough times, as though by magic, the original image reappears.

1.1.2 History of satellite

In the context of spaceflight, a satellite is an object that has been intentionally placed into orbit. These objects are called artificial satellites to distinguish them from natural satellites such as Earth's Moon.

A satellite is a human-made device that orbits in an orbit in outer space around the Earth or around another planet, performs many actions such as communications, examination and detection [7].

Or Satellite imagery (also Earth observation imagery or space borne photography) are images of Earth or other planets collected by imaging satellites operated by governments and businesses around the world. Satellite imaging companies sell images by licensing them to governments and businesses [7].

On 4 October 1957 the Soviet Union launched the world's first artificial satellite, Sputnik 1. Since then, about 8,900 satellites from more than 40 countries have been launched[7].

According to a 2018 estimate, some 5,000 remain in orbit. Approximately 63% of operational satellites are in low Earth orbit, 6% are in medium-Earth orbit (at 20,000 km), 29% are in geostationary orbit (at 36,000 km) and the remaining 2% are in elliptic orbit.

In terms of countries with the most satellites the USA significantly leads the way with 859 satellites, China is second with 250, and Russia third with 146. These are then followed by Japan (72), India (55) and the UK (52) [7].

1.1.3 Important of satellite

The bird's-eye view that satellites have allows them to see large areas of Earth at one time. This ability means satellites can collect more data, more quickly, than instruments on the ground.

Satellites also can see into space better than telescopes at Earth's surface. That's because satellites fly above the clouds, dust and molecules in the atmosphere that can block the view from ground level [6].

Satellites are used for many purposes. Among several other applications, they can be used to make star maps and maps of planetary surfaces, and also take pictures of planets they are launched into. Common types include military and civilian Earth observation satellites, communications satellites, navigation satellites, weather satellites, and space telescopes. Space stations and human spacecraft in orbit are also satellites.

Satellites can operate by themselves or as part of a larger system, a satellite formation or satellite constellation.

Satellite orbits vary greatly, depending on the purpose of the satellite, and are classified in a number of ways. Well-known (overlapping) classes include low Earth orbit, polar orbit, and geostationary orbit

Before satellites, TV signals didn't go very far. TV signals only travel in straight lines. So they would quickly trail off into space instead of following Earth's curve. Sometimes mountains or tall buildings would block them. Phone calls to faraway places were also a problem. Setting up telephone wires over long distances or underwater is difficult and costs a lot.

With satellites, TV signals and phone calls are sent upward to a satellite. Then, almost instantly, the satellite can send them back down to different locations on Earth [7].

With the fast progression of data exchange in electronic way, information security is becoming more important in data storage and transmission. Because of widely using satellite images in industrial and government process, it is important to protect the confidential image data from unauthorized access [1].

To fulfill such security and privacy needs, image encryption algorithms are important for satellite imagery protection. There are a number of encryption algorithms available such as DES, AES, International Data Encryption Algorithm (IDEA) and RSA (developed by Rivets , Shamir and Adleman) [2]

1.1.4 Cryptography

Cryptography is the study of secure communications techniques that allow only the sender and intended recipient of a message to view its contents.

A cryptography system (or a cipher system) is a method of hiding data so that only certain people can view it. Cryptography is the practice of creating and using cryptographic systems [2].

1.2 Research Significance

Protect the satellite image that contains confidential information from unauthorized persons.

1.3 Research Problem

the biggest problems of transmitting satellite image is transmission over the unsecure electronic media so:

- pictures transmitted via satellites are not safe.
- sensitive satellite image can Access by unauthorized people
- not maintaining the confidentiality , data integrity and authenticity (consistency, accuracy)

1.4 Research Important

Important of this research is to secure confidential and sensitive satellite image that use government or personal purpose from

unauthorized access so that achieve confidentiality, integrity and authenticity.

1.5 Research Objective

The main objective of research is to protect the satellite images transmutation, security and efficiency of sensitive satellite image between sender and recipe to achieve Confidentiality, Data integrity and Authentication by using chaotic cryptographic algorithms.

1.6 Research Scope

Enhance confidential satellite image security that transmit over unsecure communication media (public or privet) between sender and recipe.

This research area there are many proposed method to implement so in this research using chaotic map Arnold cat map to secure confidential satellite image

1.7 Methodology

- gathering information: first step is gathering information about satellite image and how satellite work then gathering information of different type of cryptographic algorithms (semantics , a semantics), spatially algorithms that use to secure image (AES ,ACM and RSA)algorithms .
- Architecture: after gathering information about algorithm and satellite use tools of ACM, chaotic algorithm to secure image.
- Evaluation: last step is evaluating image before secured and after secured by ACM algorithms.

1.8 Software Requirement

Main software requirement in this research chaotic Arnold cat map algorithm, DWT, histogram analysis, compression and decompression algorithm and adjacent pixel autocorrelation.

1.9 Hardware Requirement

Hardware requirement in this Research require pc (core I7 Linux operating system 8Ram)

1.10 Research Organization

Contain this research on the following chapters:

Chapter Two: Provides the critical literature review and comprehensive reports on the other works related to the topic of the research .We review the basic concepts of encryption schemes ,

honon map , logistic map , chaotic technique and Arnold mapping technique.

Chapter Three: In this chapter we explain the basic concepts of digital images, specifically the satellite images. In addition, this chapter included the proposed method used to encrypt the satellite image based chaotic, Arnold mapping technique.

Chapter Four: This chapter illustrates the implementation work done by python` programming tool, also show the result discussion of the important results of our research.

Chapter Five: This chapter concludes the results and analyzes whether the primary set up aims and objectives were met. Basically this chapter summarizes the thesis‘s achievements and findings.

Chapter two

Literature Review and Related Works

CHAPTER II
Literature Review and Related Works

2.1 Introduction

The amount of satellite image has increased rapidly on the Internet, in public or local networks. satellite image security becomes

increasingly important for many applications, e.g., confidential transmission, multispectral imaging for providing electronic images of clouds, land and sea surfaces, analysis of air masses to monitor the thermodynamic state in the lower part of the atmosphere and environment data collection and relay transmitted by automatic platforms (marine beacons, land and airborne ...)[10].

The unlawful, unofficial, and unauthorized access and illegal use of satellite imagery increases the importance of information security to keep the critical and confidential imagery and transmission process secure, dependable, trustworthy, and reliable. Cryptography is the most widely accepted information security technique employed to make the satellite image transmission processes reliable and secure from unauthorized access and illegal use.

Satellite image Security is playing a vital role in the field of communication system and Internet. This work is interested in securing transmission of satellite images on the Internet, in public or local networks.

2.2 Type of satellite:

2.2.1Type of satellite according to their function:

I. **Dynamic moons** : are satellites which use radio time signals transmitted to enable mobile receivers on the ground to determine their exact location. The relatively clear line of sight between the satellites and receivers on the ground, combined with ever-improving electronics, allows satellite navigation systems to measure location to accuracies on the order of a few meters in real time**[2] [7]** .

II. **Astronomical moons** : For astronomical satellites, astronomical satellites are known (in English: Astronomical) as satellites used to observe planets, distant galaxies and space objects, and they are called space telescopes or space observatories, and it is considered the first two astronomical satellites to be operated are the American Astronomical Observatory-2 and the Orion Telescope**[2]**

III. **Communications satellites**: is an artificial satellite that relays and amplifies radio telecommunication signals via a transponder; it creates a communication channel between a source transmitter and a receiver at different locations on Earth. Communications satellites are used for television, telephone, radio, internet, and military applications.[7] As of 1 August 2020, there are 2,787 artificial satellites in Earth's orbit, with 1,364 of these being communications satellites, used by both private and government organizations.[8] Many are in geostationary orbit 22,236 miles (35,785 km) above the equator, so that the satellite appears stationary at the same point in the sky; therefore the satellite

dish antennas of ground stations can be aimed permanently at that spot and do not have to move to track the satellite**[7]** .

IV. **Earth observation satellites:** Earth remote sensing satellite is a satellite used or designed for Earth observation (EO) from orbit, including spy satellites and similar ones intended for non-military uses
such as environmental monitoring, meteorology, cartography and others. The most common type are Earth imaging satellites, that take satellite images, analogous to aerial photographs; some EO satellites may perform remote sensing without forming pictures, such as in GNSS radio occultation[7] [2] .

V. **Satellites for navigation** : or satnav system is a system that uses satellites to provide autonomous geo-spatial positioning. It allows small electronic receivers to determine their location (longitude, latitude, and altitude/elevation) to high precision (within a few centimeters to metres) using time signals transmitted along a line of sight by radio from satellites. The system can be used for providing position, navigation or for tracking the position of something fitted with a receiver (satellite tracking). The signals also allow the electronic receiver to calculate the current local time to high precision, which allows time synchronization. These uses are collectively known as Positioning, Navigation and Timing (PNT). Satnav systems operate independently of any telephonic or internet reception, though these technologies can enhance the usefulness of the positioning information generated**[2]** .

VI. **Weather moons** : is a type of satellite that is primarily used to monitor the weather and climate of the Earth. Satellites can be polar orbiting, covering the entire Earth asynchronously, or geostationary, hovering over the same spot on the equator.[2]
Meteorological satellites see more than clouds: city lights, fires, effects of pollution, auroras, sand and dust storms, snow cover, ice mapping, boundaries of ocean currents, energy flows, etc. Other types of environmental information are collected using weather satellites. Weather satellite images helped in monitoring the volcanic ash cloud from Mount St. Helens and activity from other volcanoes such as Mount Etna.[7] Smoke from fires in the western United States such as Colorado and Utah have also been monitored[7] .

VII. **Killer satellites:** are satellites that are designed to destroy enemy warheads, satellites, and other space assets[7] .

VIII. Military satellites: are satellites of unusually low masses and small sizes.[17] New classifications are used to categorize these

satellites: mini satellite (500–1000 kg), microsatellite (below 100 kg), nano satellite (below 10 kg) [7] [3].

IX. **Vital satellites:** Biosatellites are satellites designed to carry life into space, and the US Space Agency NASA launched the first three vital satellites in the period between 1966-1969 AD, and these moons were carrying fruit flies, wheat seeds, eggs of frogs, and bacteria. And a monkey, and in the date of 1957 AD, Spotik 2 was the first satellite to carry an animal into space, a dog called Leica[7] .

X. **Space tethers:** are long cables which can be used for propulsion, momentum exchange, stabilization and attitude control, or maintaining the relative positions of the components of a large dispersed satellite/spacecraft sensor system.[1] Depending on the mission objectives and altitude, spaceflight using this form of spacecraft propulsion is theorized to be significantly less expensive than spaceflight using rocket engines[7] .

2.2.2 Types of satellites according to orbits

I. GEO (Geostationary Earth Orbit) at about 36,000km above the earth's surface.

II. LEO (Low Earth Orbit) at about 500-1500km above the earth's surface.

III. MEO (Medium Earth Orbit) or ICO (Intermediate Circular Orbit) at about 6000-20,000 km above the earth's surface.

IV. HEO (Highly Elliptical Orbit)

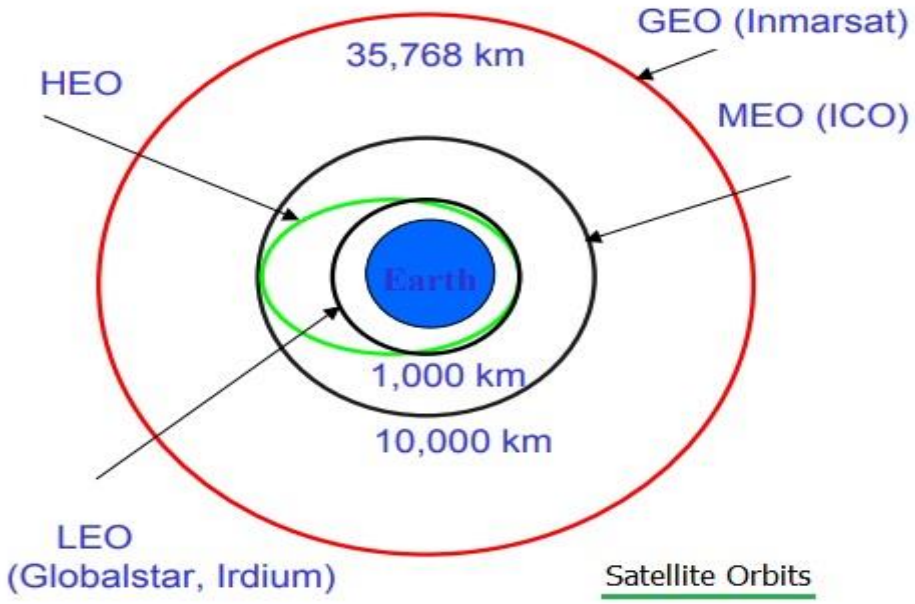


Figure 2.1: satellite orbits type [2]

I. GEO (Geostationary Earth Orbit)

- If a satellite should appear in fixed in the sky, it requires a period of 24 hours. Using the equation of distance earth and satellite, r = (g.r2 /2.r.f)2)1/3 and the period of 24 hours f = 1/24 h. the resulting distance is 35,786 km. the orbit must have an inclination of 0 degree.
- Objects in GEO moves around the earth at the same speed as the earth rotates. This means geostationary satellites remain in the same position relative to the surface of earth [7] [2].

II. LEO (Low Earth Orbit)

- Each LEO satellite will only be visible from the earth for about ten minutes.
- LEO satellites are much closer to earth than GEO satellites, ranging from 500 to 1,500 km above the surface. LEO satellites do not stay in fixed position relative to the surface, and are only visible for 15 to 20 minutes each pass [7].

III. MEO (Medium Earth Orbit)

- MEO satellites are similar to LEO satellites in the context of functionality.
- Medium earth orbit satellites are visible for much longer periods of time than LEO satellites usually between 2 to 8 hours.
- MEO satellites have a larger coverage area than Low Earth Orbit satellites.
- MEOs can be positioned somewhere between LEOs and GEOs, both in terms of their orbit and due to their advantages and disadvantages [7].

IV. HEO (High Earth Orbit)

- The High Earth orbit satellite is the only non-circular orbit of the four types.
- The HEO satellites used for the special applications where coverage of high latitude locations is required [2].

2.2.3There are three basic categories of (non-military) satellite services

2.2.3.1 Fixed satellite services

Fixed satellite services handle hundreds of billions of voice, data, and video transmission tasks across all countries and continents between certain points on the Earth's surface [3].

2.2.3.2 Mobile satellite systems

Main article: Mobile-satellite service Mobile satellite systems help connect remote regions, vehicles, ships, people and aircraft to other parts of the world and/or other mobile or stationary communications units, in addition to serving as navigation systems[3].

2.2.3.3 Scientific research satellites (commercial and noncommercial)

Scientific research satellites provide meteorological information, land survey data (e.g. remote sensing), Amateur (HAM) Radio, and

other different scientific research applications such as earth science, marine science, and atmospheric research [3].

2.3 types of satellite imagery

2.3.1 Visible imagery:

Visible satellite pictures can only be viewed during the day, since clouds reflect the light from the sun. On these images, clouds show up as white, the ground is normally grey, and water is dark. In winter, snow-covered ground will be white, which can make distinguishing clouds more difficult. To help differentiate between clouds and snow, looping pictures can be helpful; clouds will move while the snow won't. Snow-covered ground can also be identified by looking for terrain features, such as rivers or lakes [3].

2.3.2 Infrared imagery:

Infrared satellite pictures show clouds in both day and night. Instead of using sunlight to reflect off of clouds, the clouds are identified by satellite sensors that measure heat radiating off of them. The sensors also measure heat radiating off the surface of the earth. Clouds will be colder than land and water, so they are easily identified. Infrared imagery is useful for determining thunderstorm intensity [3].

2.3.3 Water vapor imagery:

Water vapor satellite pictures indicate how much moisture is present in the upper atmosphere (approximately from 15,000 ft to 30,000 ft). The highest humilities will be the whitest areas while dry regions will be dark. Water vapor imagery is useful for indicating where heavy rain is possible. Thunderstorms can also erupt under the high moisture plumes [3].

2.4 Satellites Work:

Down on the ground, satellites can look very similar -- shiny boxes or cylinders adorned with solar-panel wings. But out in space, these gawky machines behave quite differently depending on their flight path, altitude and orientation. As a result, classifying satellites can be tricky business. One approach is to think about how a device orbits its target planet (usually Earth). Recall that there are two basic shapes of an orbit: circular and elliptical. Some satellites start out elliptical and then, with corrective nudges from small onboard rockets, acquire circular paths. Others move permanently in elliptical paths known as Molniya orbits. These objects generally circle from north to south, over Earth's poles, and take about 12 hours to make one complete trip[3][7].

Polar-orbiting satellites also pass over the planet's poles on each revolution, although their orbits are far less elliptical. The polar orbit remains fixed in space as Earth rotates inside the orbit. As a result,

much of Earth passes under a satellite in a polar orbit. Because polar orbits achieve excellent coverage of the planet, they are often used for satellites that do mapping and photography. And weather forecasters rely on a worldwide network of polar satellites, which covers the entire globe every 12 hours [3].as show below.

Figure 2.2: satellite work[3]

2.5 Satellite Imagery: Resolution vs. Accuracy

The main feature satellite operators highlight about their imagery is resolution; however, this is not the only feature to consider. Accuracy also plays a key role in determining image quality, and it's important to understand the difference between resolution and accuracy. High-resolution is often associated with high-accuracy (and vice versa), but this is not always the case. This distinction is important to consider when purchasing satellite imagery [7].

2.5.1 Resolution:

Resolution refers to the smallest size an object or detail can be represented in an image. Higher resolution means that pixel sizes are smaller, providing more detail. For example, 30cm resolution satellite imagery can capture details on the ground that are greater than or equal to 30cm by 30cm. Anything on the ground that is less than that size will be blended with the surrounding area to make a 30cm by 30cm square. Based on this definition, 30cm resolution imagery would capture more photographic details than 1m resolution imagery [7] as show below.

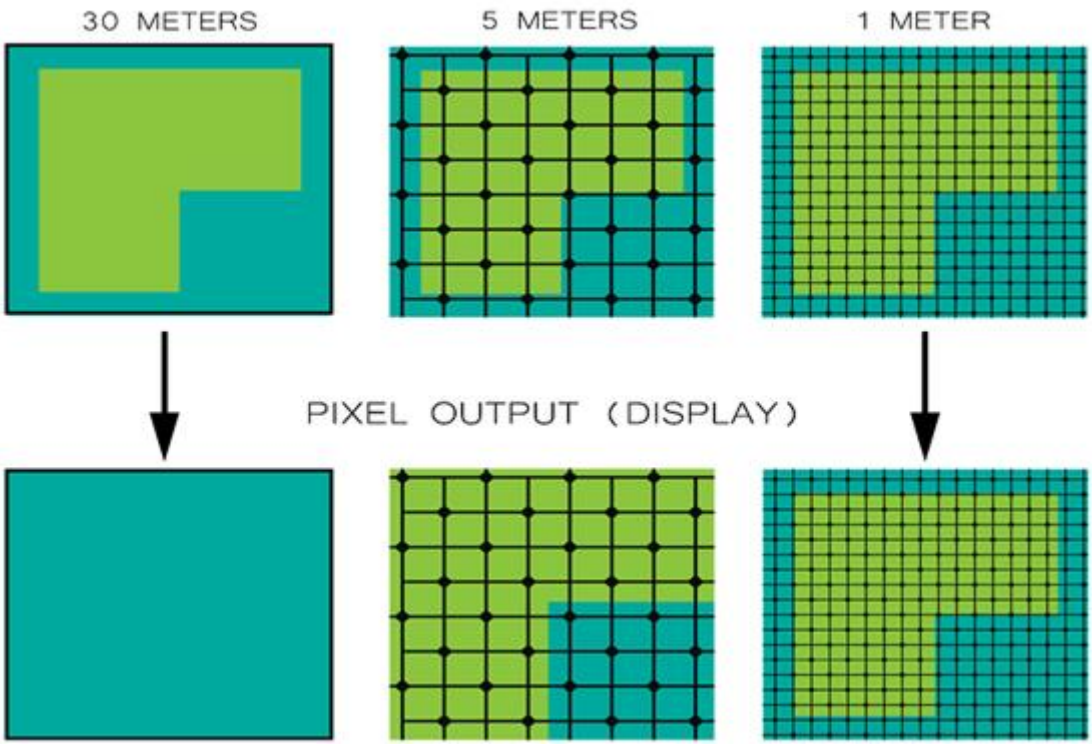


Figure 2.3: pixel size [7]

2.5.2 Accuracy:

Accuracy, on the other hand, is the distance between the actual geographic location of an object or detail compared to the position of the object in the image. Accuracy is dependent on several factors, such as the satellite positioning technology, terrain relief, and sensor viewing angle. The accuracy of an image has no direct relationship with resolution and it's less commonly (and less clearly) specified than an image's resolution.

When a satellite sensor captures an image, a positioning device on the satellite computes its orbital position relative to the earth and stores that information in the metadata for that image. The accuracy of the positioning device is related to the absolute accuracy of the captured image. Since satellites orbit 500km above the earth at a speed of more than 20,000km/h, the positioning device needs to be very sophisticated to be accurate [7].

2.6 Information security:

Information security is a set of practices designed to keep personal data secure from unauthorized access and alteration during storing or transmitting from one place to another.

Information security is designed and implemented to protect the print, electronic and other private, sensitive and personal data from unauthorized persons. It is used to protect data from being misused, disclosure, destruction, modification, and disruption [10].

2.7 Information security principle

There are some basic components of information security which are discussed below [10].

- Confidentiality: is one of the basic elements of information security. Data is confidential when only authorized people access it. To ensure confidentiality one needs to use all the techniques designed for security like strong password, encryption, authentication and defense against penetration attacks(ensure data is read only by authorized parties,)
- Data integrity: is refers to maintaining data and preventing it from modifications either accidentally or maliciously. Techniques used for confidentiality may protect data integrity as a cybercriminal can't change data when they can't get access to it (ensure data wasn't altered between sender and recipient,)
- Availability: is another basic element in information security. It is vital to make sure that your data is not accessed by unauthorized persons but only those who have permission can access it.

Figure 2.4: Confidentiality, integrity, and availability (CIA Triangle) [10]

2.8 Cryptography

Cryptography is the study of secure communications techniques that allow only the sender and intended recipient of a message to view its contents [2].

Cryptography system (or a cipher system) is a method of hiding data so that only certain people can view it. Cryptography is the practice of creating and using cryptographic systems [2].

Cryptanalysis is the science of analyzing and reverse engineering cryptographic systems. The original data is called plaintext. The protected data is called cipher text. Encryption is a procedure to convert plaintext into cipher text. Decryption is a procedure to convert cipher text into plaintext. A cryptographic system typically consists of algorithms, keys, and key management facilities [2].

2.8.1 Type of cryptographic algorithms

There are two basic types of cryptographic systems: symmetric ("private key") and asymmetric ("public key").

1. Symmetric key

systems require both the sender and the recipient to have the same key. This key is used by the sender to encrypt the data, and again by the recipient to decrypt the data. Key exchange is clearly a problem. How do you securely send a key that will enable you to send other data securely? If a private key is intercepted or stolen, the adversary can act as either party and view all data and communications. You can think of the symmetric crypto system as akin to the Chubb type of door locks. You must be in possession of a key to both open and lock the door [10].

2. Asymmetric key

   Cryptographic systems are considered much more flexible. Each user has both a public key and a private key. Messages are encrypted with one key and can be decrypted only by the other key. The public key can be published widely while the private key is kept secret. If Alice wishes to send Bob a secret, she finds and verifies Bob's public key, encrypts her message with it, and mails it off to Bob. When Bob gets the message, he uses his private key to decrypt it. Verification of public keys is an important step[13]. Failure to verify that the public key really does belong to Bob leaves open the possibility that Alice is using a key whose associated private key is in the hands of an enemy, Public Key Infrastructures or PKI's deal with this problem by providing certification authorities that sign keys by a supposedly trusted party and make them available for download or verification [10].

Asymmetric ciphers are much slower than their symmetric counterparts and key sizes are generally much larger. You can think of a public key system as akin to a Yale type door lock. Anyone can push the door locked, but you must be in possession of the correct key to open the door [2].

2.8.2Cryptography can be used to provide

I. Confidentiality - ensure data is read only by authorized parties,
II. Data integrity - ensure data wasn't altered between sender and recipient.
III. Authentication - ensure data originated from a particular party.

2.9 Image Encryption using Chaos Maps

2.9.1 chaos maps

Chaotic systems are a simple sub-type of nonlinear dynamical systems. They may contain very few interacting parts and these may follow very simple rules, but these systems all have a very sensitive dependence on their initial conditions. Despite their deterministic simplicity, over time these systems can produce totally unpredictable and wildly divergent (aka, chaotic) behavior[14].

2.9.2 chaos maps for encryption

Traditional encrypting mechanisms AES and RSA exhibit some drawbacks and weakness in the encryption of digital images and high computing .

- Large computational time for large images
- High computing power for large images Consequently, there might be better techniques for image encryption.

A few chaos based algorithms provide a good combination of speed, high security complexity, low computational overheads Moreover, certain chaos-based and other dynamical systems based algorithms have many important properties such as

- sensitive dependence on initial parameters
- pseudorandom properties
- ergodicity
- non periodicity

2.9.3 Characteristics of the chaotic maps

This research work is mainly concern with secure satellite image encryption and decryption using chaotic sequences and Arnold cat map is a chaotic map often used for pixel manipulation. It applies a transform on the image that essentially shuffles the pixels by stretching and folding the image. When an optimal number of iterations of the transformation is applied on the image, the resulting image becomes incomprehensible and hence encrypted. More specifically, chaotic maps are used for secure satellite image communication over shared network environments and distributed using any storage media like CDs, DVDs and/or hard disks.A particularly interesting candidate for chaotic sequences generators are logistic and Henon map. The chaotic behaviour of these maps can be verified easily with different desirable properties. These properties can be accessible with the help of rigorous mathematical analysis and experiments as shown subsequently Henon map analysis [17].

2.9.4 Arnold Cat Map

Arnold's cat map is a chaotic map often used for pixel manipulation. It applies a transform on the image that essentially shuffles the pixels by stretching an folding the image. When an optimal number of iterations of the transformation is applied on the image, the resulting image becom
es incomprehensible and hence encrypted [17] [12].

For this implementation The transform applied on the image is: $R([x,y]) = [(x + y) \bmod n, (x + 2y) \bmod n]$ where n is the dimensions of the image

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

2.9.5 Arnold's Cat Map Algorithm

Chaos is a common technique used in the random number generator[5], it's happening because this technique is faster and easier to use in the process stream object both in terms of storage and process objects Only a few functions (chaotic maps) and some parameters (inital conditions) were quite good used if the process takes quite a long time [17]. Arnold's Cat Mapare chaotic two dimensions that can be used to change the position of the pixel of the image without removing any information from the image[15], pixel image can be assumed by S = {(x, y) | x, y = 0, 1, 2 ... N-1} . 2- dimensional image of Arnold's Cat Map can be written by the following equation[12]:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = A \begin{bmatrix} x \\ y \end{bmatrix} (\mathrm{mod}\ n) \longrightarrow (1)$$

$$\begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} (\mathrm{mod}\ n) \longrightarrow (2)$$

Where p and q are positive integers, the determinant (A) = 1. (x ', y') is the new position of the original pixel position (x, y) when Arnold's Cat Map algorithm performed once. Results after application of Arnold's Cat Map to the number of iterations of iterations R will be a random drawing that contains all the values of the same pixel of the original image.
The number of iterations R to complete depending on the parameters p,q and N size of the original image. So Arnold's Cat Map algorithm has parameters p, q, and the number of iterations R, all can be used as a secret key [17]

2.9.6 Discrete Wavelet Transform

The discrete wavelet transform (DWT) is an implementation of the wavelet transform using a discrete set of the wavelet scales and

translations obeying some defined rules. In other words, this transform decomposes the signal into mutually orthogonal set of wavelets, which is the main difference from the continuous wavelet transform (CWT), or its implementation for the discrete time series sometimes called discrete-time continuous wavelet transform (DT-CWT) [9].

Original image is firstly decomposed through Discrete Wavelet transform into sub bands. All the obtained frequency bands are formulated into a band scrambling matric by the horizontal followed by vertical concatenation. Then the Band scrambling matrix is shuffled by using Arnold cat map, whose control parameters [9] [12].

There are several types of implementation of the DWT algorithm. The oldest and most known one is the Malaat (pyramidal) algoritm. In this algorithm two filters - smoothing and non-smoothing one are constructed from the wavelet coefficients and those filters are recurrently used to obtain data for all the scales. If the total number of data D=2^N is used and signal length is L, first D/2 data at scale L/2^(N-1) are computed, than (D/2)/2 data at scale L/2^(N-2), etc up to finally obtaining 2 data at scale L/2. The result of this algorithm is an array of the same length as the input one, where the data are usually sorted from the largest scales to the smallest ones [17] [9].

Similarly the inverse DWT can reconstruct the original signal from the wavelet spectrum. Note that the wavelet that is used as a base for decomposition cannot be changed if we want to reconstruct the original signal, e. g. by using Hear wavelet we obtain a wavelet spectrum; it can be used for signal reconstruction using the same (Hear) wavelet[9].

2.9.7 A comparison of Satellite Image

To reduce data volume and facilitate the transmission of satellite communication and storage, we need to apply compression techniques to satellite image data.

Better resolution of remotely sensed satellite images will make images clearer and interpretation easier but will increase the total volume of data that has to be managed. In order to reduce data volume for easier satellite communication transmission and reduce the total volume of data needed to be stores, the images should be compressed. Image compression in wavelet domain can be used for both lossy or lossless compression [16].Four major compression methods are available using the wavelet domain, i.e. CCSDS, Wavelet, Bandelet, and JPEG 2000. Some optical satellite images, were used as input data in simulation software which analyzed and compared the four compression methods in the wavelet domain The result showed that the CCSDS method yielded the fastest compression and

decompression time, but the Bandelet method retained better image quality when reconstructing original images or approximations of them compared to CCSDS. The JPEG 2000 method delivered better quality images than CCSDS for low bit rate. In summary at a rate of 0.25 bpp, CCSDS is 15 times faster than Bandelet and 3 times faster than JPEG2000. However, CCSDS quality is lower by up to 8.77% compared with Bandelet and up to 13.64% compared with JPEG2000. So The discrete wavelet transform associated with sub-band coding provides high image compression ratio. Although the wavelet transform performs well on smooth areas, the wavelet representation of edges is not sparse [16]. Indeed, wavelet coefficients have high magnitude around the edges and correlations between those coefficients remain. All post processing in wavelet domain is aim to exploit remain redundancies between the wavelet coefficients to achieve higher compression and higher quality. Finding efficient geometric representations of images is a central issue to improving image compression [16].

2.9.8 Henon map

The Henon map is a discrete-time dynamical system which can be used in cryptography because of chaotic effect. Henon map is one of the well studied dynamical systems because of its simplicity and chaotic behavior [14].It is a simple two-dimensional map with quadratic nonlinearity (Álvarez et al., 2002; Long and Huang, 2010). Mathematically, Given initial conditions (x0,y0), a henon map is given by the following equations:

$(Xn+1) = (Yn) + 1 - a.(Xn)$

$(Yn+1) = b * (Xn)$

Classical Henon map have values of a = 1.4 and b = 0.3. For the classical values the Henon map is chaotic. For other values of a and b the map may be chaotic, intermittent, or converge to a periodic orbit[14] [12].

The Henon map depends on two parameters, a and λ . The pseudorandom behaviours of the Henon map have values of $09 .10 \leq a \leq 7.1$ and $3 .0 = \lambda$. For these basic values, the Henon map is chaotic. For other values of a and λ , the map can be behaved like chaotic, recurring, irregular or unpredictable behaviours. An overview of the type of behaviours of the map at different parameter values may be obtained from its orbit diagram. The Henon map takes a point (x, y) in the plane and maps it to a new point. For many values of 0 a and 0 b , the dynamics of this map are chaotic. We consider the range $09.10 \leq a \leq 7.1$ and $3 .0 = \lambda$; the analysis diagrams are shown in Figure 1. To examine the behaviour of the Henon map, the parameter value

lambda λ can be divided into three segments as) 28.0,0(∈ λ ,) 32.0,2 9.0(∈ λ and) 1,3 3.0(∈ λ) [17].

with initial condition 56 .02 =x and 34 .03 =x . These parameters λ and initial values 2 x and 3 x may be used as a secret key for cryptography system. When) 28.0,0(∈ λ , as shown in Figure 1a, the calculation results come to the same value after several iterations without any chaotic behaviour. When) 32.0,2 9.0(∈ λ , it becomes a chaotic system and random behaviour with periodicity disappeared, 1,3 3.0(∈ λ , the phase space concludes several points only[12].

2.9.9 Logistic map analysis

The Logistic map is one-dimensional discrete chaotic map which can originate chaotic behavior using simple non-linear dynamical equation (Grassi, 2002; Long and Huang, 2010). Mathematically, the Logistic map is defined by following equation:

1(1 nnn xxx −=+ λ) [14] [12].

2.9.10 Logistic Chaos Maps with key mixing

The logistic map instead uses a nonlinear difference equation to look at discrete time steps. It's called the logistic map because it maps the population value at any time step to its value at the next time step

The basic formula is: (X_t+1) = r.X_t.(1 - X_t)

For this implementation we have included key mixing. The initial values of the chaos map are recalculated after every pixel encryption based on the previous encryption value as well as the key value [14].

2.10 Histogram Analysis

The cipher text image histogram analysis is one of the most straight-forward methods of illustrating the image encryption quality. A good image encryption method tends to encrypt a plaintext image to a random incomprehensible form. Thus a good image encryption technique generates a cipher image that has a uniformly distributed intensity histogram [12] [17].

2.11 Adjacent Pixel Auto-Correlation

Since images exhibit high information redundancy, it is desirable to have an encryption algorithm that breaks this redundancy. Thus as a metric of encryption performance we find the correlation between adjacent pixels in a direction (Horizontal, Vertical or Diagonal). We have considered the Horizontal direction.

1024 random pixels are picked up from the image and its correlation between it's rightmost neigh bour is found and plotted. For a good algorithm, the correlation plot should appear random with no discernable pattern [17].

2.12 Related work:

No	Paper Name	Date	Author	techniques	Results	Open issues

1	Meteosat Images Encryption based on AES and RSA Algorithms	2015	Boukhatem Mohammed Belkaid , Lahdir Mourad And Cherifi Mehdi	a hybrid encryption algorithm based on Advanced Encryption Standard (AES) and Rivest Shamir Adleman (RSA) algorithms so AES algorithm is used for data transmission and RSA algorithm is used for the encryption of the key of the AES	strength of the confusion and diffusion properties , security and resistance level against some known attacks.	Traditional algorithms
2	Satellite Image Encryption for C4I System	2011	Abdullah Sharaf Alghamdi, Hanif Ullah , Muhammad Usama Khan, Iftikhar Ahmad and Khalid Alnafajan	Global command and control system (GCCS-Joint) and intelligence (C4I) system which consists of hardware, software and The algorithm uses the	achieve the high level of confusion and diffusion during the entire process	requires negligible computation time and suitable for real-time application of satellite imagery

				idea of chaotic maps that is Henon and logistic		
3	Secure Satellite Images Transmission Scheme Based on Chaos and Discrete Wavelet Transform	2018	Musheer Ahmad and Omar Farooq Department of Computer Engineering, Faculty of Engineering and Technology, Jamia Millia Islamia, New Delhi 110025, India	permuting the pixels of satellite image, then improving the pixels gray value distribution from cryptographic viewpoint. The permutation of image pixels is carried out in discrete wavelet domain and the relationship between the encrypted and the original satellite image is confused using chaotic-state modulation technique	thereby significantly increasing the resistance to statistical attacks high sensitivity to secret key	large key space and doesn't work on pixel and object level

4	An Improved Image Encryption Algorithm Based on Cyclic Rotations and Multiple Chaotic Sequences : Application to Satellite Images	2017	MADAN Mohammed BENTOUTOU Youcef , TALEB Nasreddine Djillali Liabes University of Sidi Bel-Abbes, Algeria Communication Networks, Architecture and Multimedia Laboratory, BP. 89 22000 Sidi Bel Abbes, Algeria	used the chaos model based on combining three different chaotic maps and the Graph theory rotation for the encryption of satellite images	is able to resist differential, brute-force, statistical, and plain image attacks, and is therefore highly secure and efficient.	Those combination work on the place of pixel image image not on object

Chapter three
Methodology

CHAPTER III
Methodology

3.1 Introduction:

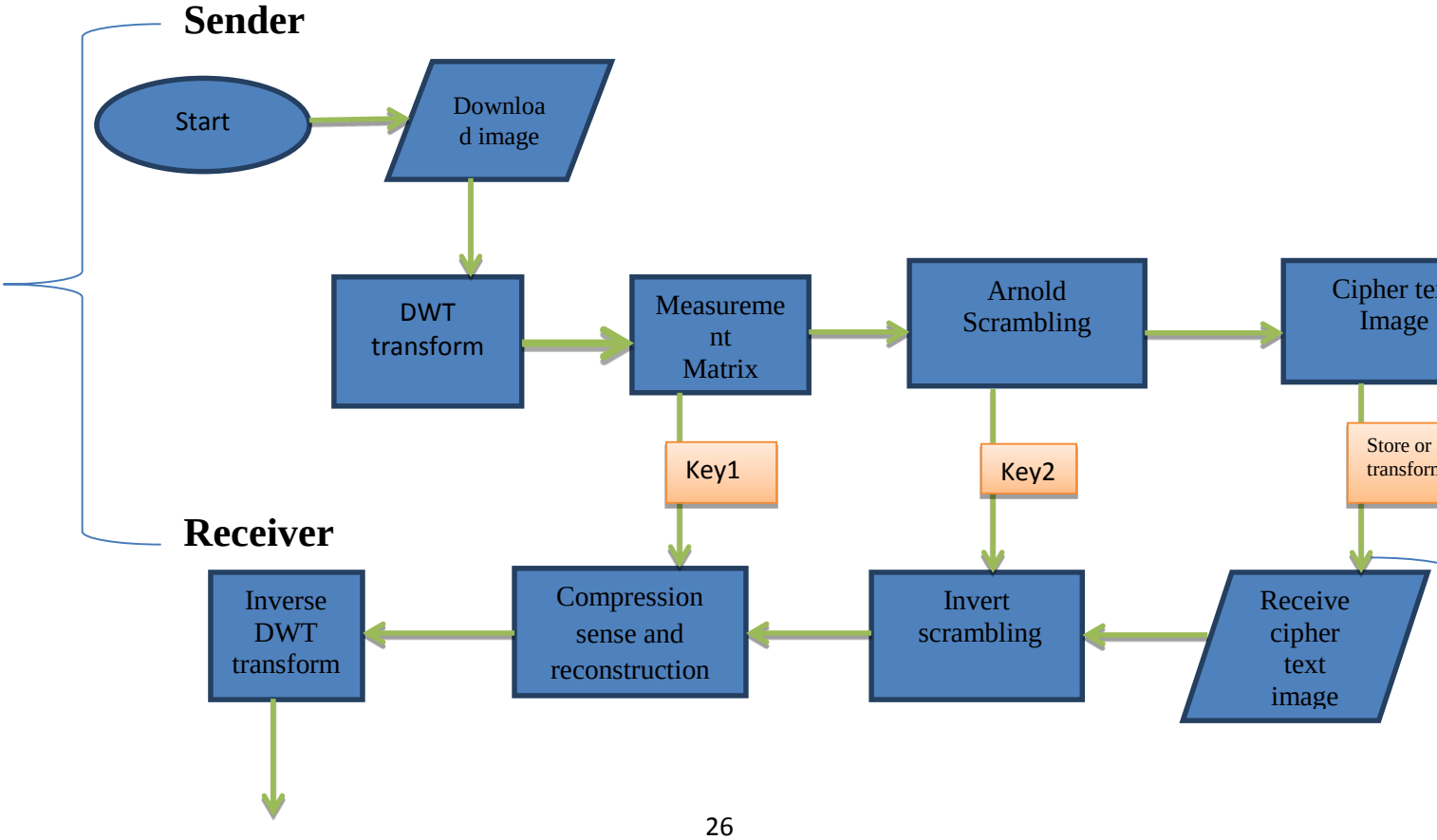
The development of speed that are taking place in the world especially in the technological aspect of satellite and the use of satellite image for covert operations whether they are government serving operation or personal purposes and sending them over the internet if they are (public or private) subjected to violations and it is very necessary to protect the images from heft modification and unauthorized disclosure.

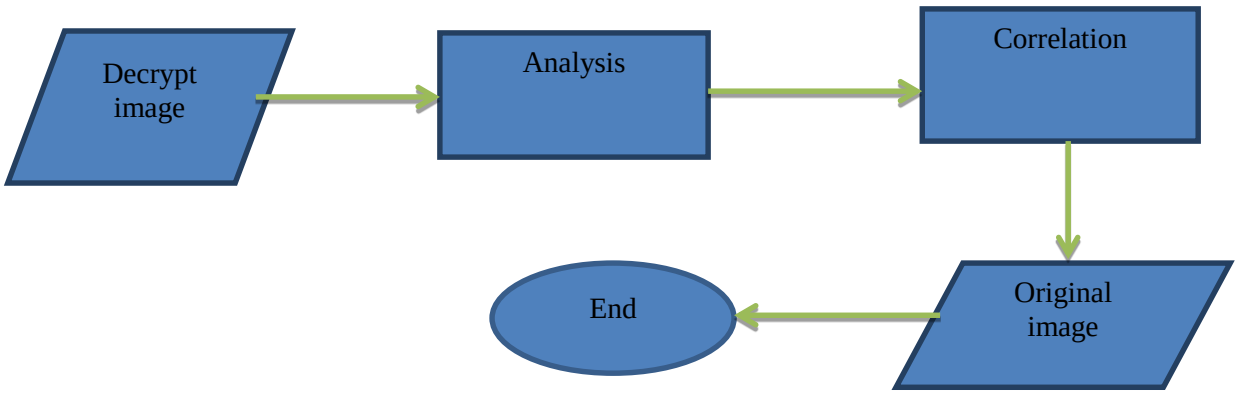
A digital image is a numeric representation, normally binary, of a two-dimensional image. Depending on whether the image resolution is fixed, it may be of vector or raster type. By itself, the term "digital image" usually refers to raster images or bitmapped images (as opposed to vector images) .

The digital image is sampled and mapped as a grid of dots or picture elements (pixels). Each pixel is assigned a tonal value (black, white, shades of gray or color), which is represented in binary code (zeros and ones). The binary digits ("bits") for each pixel are stored in a sequence by a computer and often reduced to a mathematical

representation (compressed). The bits are then interpreted and read by the computer to produce an analog version for display or printing.
To protect the digital information against unauthorized access has become extremely important. Data encryption is one of the most secure ways to protect data. Encryption of images is different from that of texts due to some intrinsic features of images such as bulk data capacity and high correlation between pixels [14][15],which are generally difficult to handle by traditional methods such as Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA) and Advanced Encryption Standard (AES).so This chapter introduce and describes the methodology that has been used in this research.

3.2 Flow chart





Figure(3.1)flow chart of algorithm

3.3 Proposed Algorithm implementation

3.3.1 Algorithm for Encoding

Start

Step 1: download image from satellite

Step 2: DWT transform, make the original image sparse in the wavelet domain

Step 3: The initial conditions and parameters of the new chaotic image are taken as key 1

Step 4: scramble the pixels of an image in such a manner that the image becomes chaotic and indistinguishable, scrambling parameter and iteration number constitute key 2 ={i, j, n}

Step 5: give cipher text image so the cipher text image can be transform of store

End

3.3.2Algorithm for decoding

Start

Step1: Input the cipher text image

Step2: decryption the inverse process of encryption key2 and key1that are in step(4,3) are used sequentially to perform inverse Arnold scrambling

Step 3: inverse DWT transform on the cipher text image

Step 4: compressed sensing and reconstruction is applied to obtain the original image

Step 5: An image histogram illustrates how pixels in an image are distributed by graphing the number of pixels at each intensity level

Step 6: Correlation analysis gives a statistical measure of the similarity between the adjacent pixels of the encrypted image.

Step 7: give image as original image

End

3.4 Arnold's Cat Map algorithm

The analysis algorithm used in this study is Arnold's Cat Map algorithm, here are the steps how algorithms work Arnold's Cat Map a) Read the color pixel RGB On Citra b) Calculate the position X, Y pixel in the image to be encrypted c) rotation (iteration) RGB pixels to the image to be random and cannot be recognized. Based on the above process design scheme writer IPO (Input Process Output) from the analysis are discussed, figure below is a schematic diagram

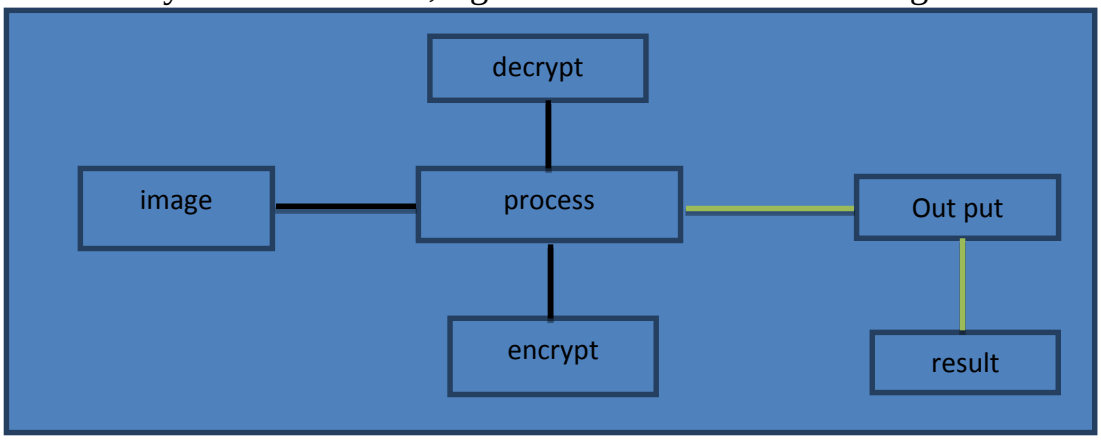


Figure 3.2: Input Process Output System Arnold's Cat Map [12].

3.4.1 Method Encryption Algorithms Arnold Map

- chosen share 1,share 2,share 3 for the process of encryption.
- Pixel extraction is done of the input image (share) by taking the image dimension i.e. Height and Width of the share.

- Pixel shuffling of pixels of the input image is done by using the Arnolds map which is chaotic in nature.
- Input Key number
- Cipher image or Encrypted image (share) is done successfully.

3.4.2 Method Decryption Algorithms Arnold Map

- The cipher image (share) which got from the process of encryption is chosen for the process of decryption.
- Pixel extraction is done of the cipher image by taking the image dimension i.e. Height and Width of the cipher image.
- Pixel shuffling of pixels of the cipher image is Done by using the Arnolds map which is chaotic in nature.
- Input Key number.
- Original image is brought back from the cipher image successfully

3.5 Compression

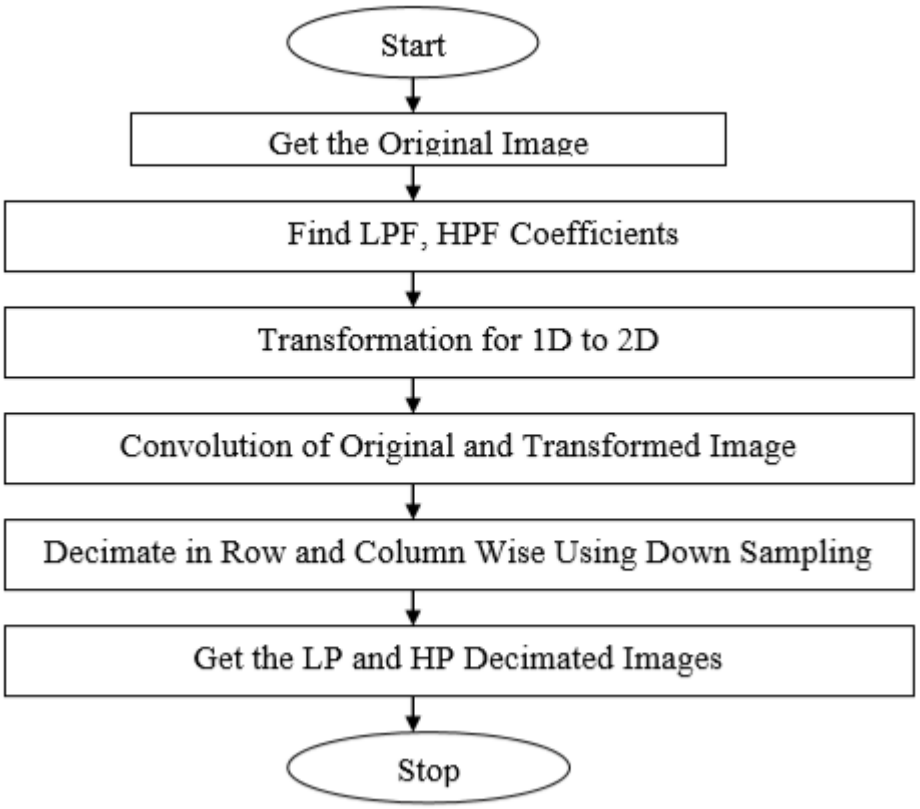


Figure Flow3.3: Compression

- original image is split in to two coefficient filters such as low pass and high pass.
- After the filtering progression the image is sent to the transformation section for 1D to 2D processes so HPL is isolates the low frequencies and allow only the middle and high frequencies to appear and LPF is isolates high frequencies and allow only low and medium frequencies to appear.
- After the transformation process the major modification of convolution process of original image is undergone.
- Here we use 2D convolution because image is having two dimensional function.
- After the convolution processes image is split into decimated row and column wise down sampling process.
- Finally, after the sampling get the low pass and high pass decimated images with high CR, the entire process of compression part is stopped and enter in to the interpolated/ decompression of original image conversion processes.

3.6 Decompression/Reconstruction

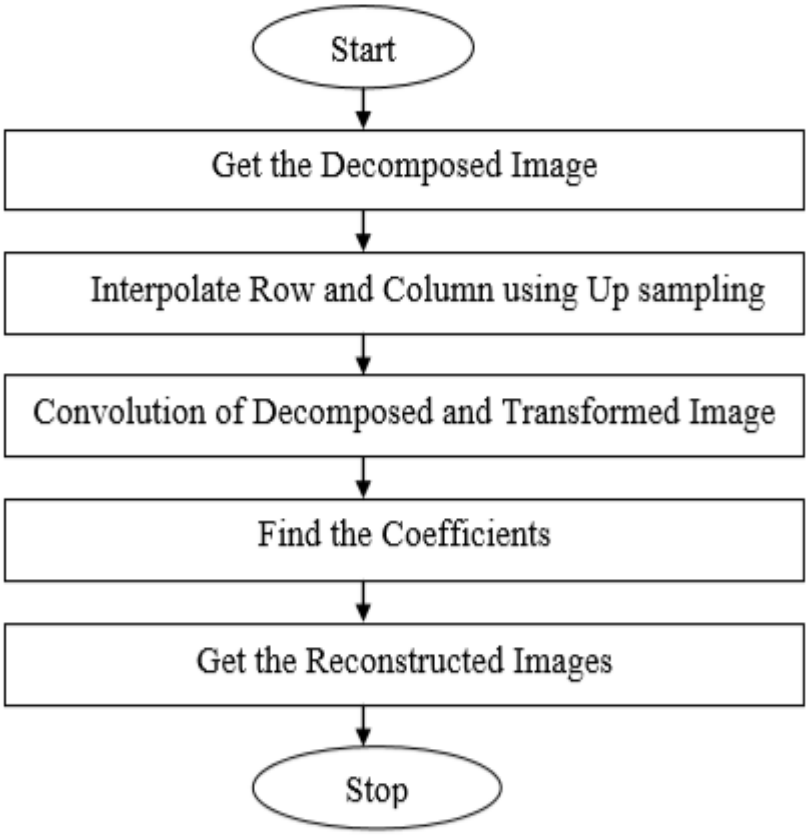


Figure 3.4: decompression/Reconstruction

- In this section after the decomposed image is converted into interpolated section of row and column using up sampling,
- the sampling convolution of decomposed and transformed image are measured.
- This technique is used to find the coefficients
- finally get the reconstructed images, and then stop for the reconstruction process.

Chapter four
Implementation and Results Discussion

CHAPTER IV
Implementation and Results Discussion

4.1 Introduction:

This chapter includes the detailed design phase to all documentation of the main interfaces of the system designed using python language,

data input (plain image), encryption and decryption algorithm, overview of the results that are obtained after implementing the proposed cryptographic of Arnold algorithm so Arnold transformation is commonly known as cat face transformation [11]. When applied to the digital image randomizes the original position of its pixels and the image becomes noisy. However, if iterated enough times the original image reappears.

4.2 Implementation

Figure 4.1: show system main screen that include common line of open the algorithm

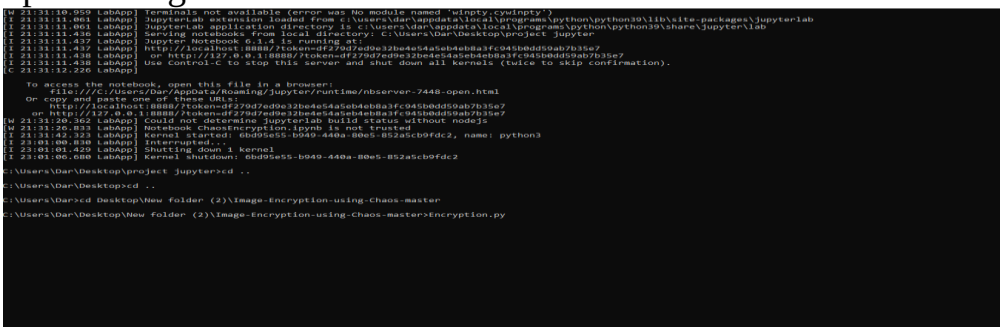


Figure 4.1 Show System main screen

The firest step is dowmlod image foram the google image so his is code for downlod image and figure 4.2 show image that download from google instae of satllite

```
# Downloading HorizonZero.png
!wget https://drive.google.com/uc?id=1Djfm4PqE7Su4WqEdZKiGL-8HtrbVBuMm
!mv uc?id=1Djfm4PqE7Su4WqEdZKiGL-8HtrbVBuMm HorizonZero.png

# Downloading lena.bmp
!wget https://drive.google.com/uc?id=19xZhsjs_r0tLwtu_Wl5DB5rG26dhw069
!mv uc?id=19xZhsjs_r0tLwtu_Wl5DB5rG26dhw069 lena.bmp
```

Figure 4.2 image downlod from google

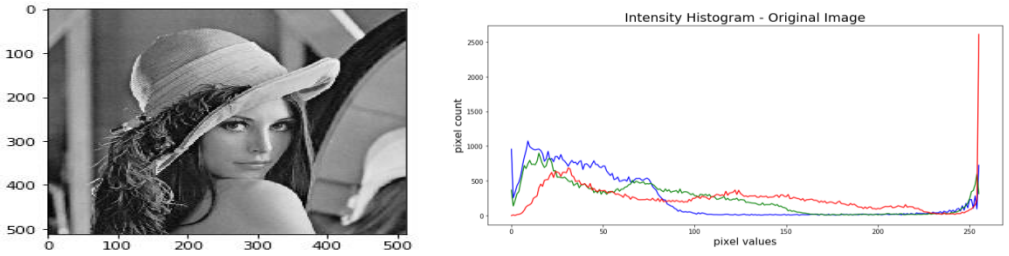
4.2.1 histogram analysis for orginal image

Figure 4.3 show histogram analysis for orginal image and there code so An image histogram illustrates that how pixels in an image are distributed by plotting the number of pixels at each grayscale level. The distribution of cipher-text is of much importance. More specifically, it should hide the redundancy of plain-text and should

not leak any information about the plain-text or the relationship between plain-text and cipher-text.

```
image = "HorizonZero"
ext = ".png"
img = cv2.imread(image + ext,1)
pil_im = Image.open(image + ext, 'r')
imshow(np.asarray(pil_im))
plt.figure(figsize=(14,6))

histogram_blue = cv2.calcHist([img],[0],None,[256],[0,256])
plt.plot(histogram_blue, color='blue')
histogram_green = cv2.calcHist([img],[1],None,[256],[0,256])
plt.plot(histogram_green, color='green')
histogram_red = cv2.calcHist([img],[2],None,[256],[0,256])
plt.plot(histogram_red, color='red')
plt.title('Intensity Histogram - Original Image', fontsize=20)
plt.xlabel('pixel values', fontsize=16)
plt.ylabel('pixel count', fontsize=16)
plt.show()
```



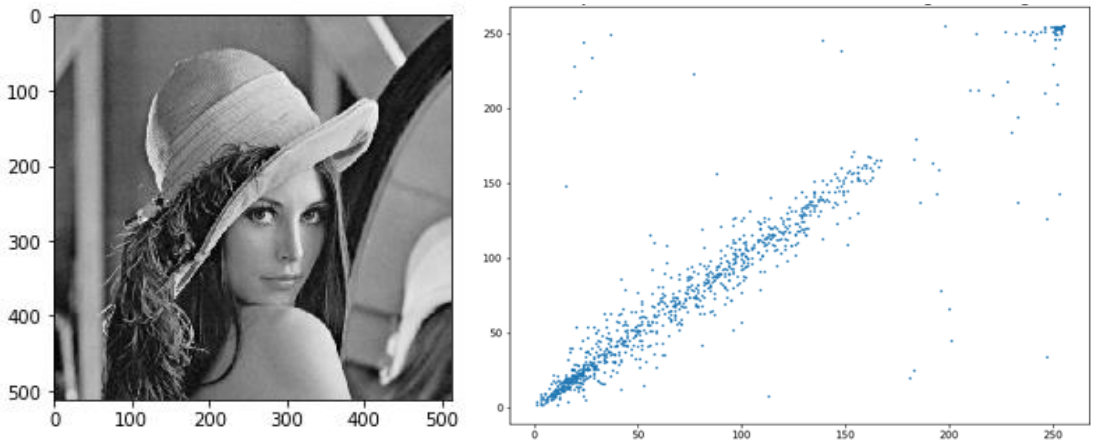
(a) (b)

Figure 4.3 : orginal image(a) histogram analysis of orginal image(b)

4.2.2 Adjacent pixel autocorrelation of orginal image

Figure 4.4: show the original image auto correlation so the images exhibit high information redundancy, it is desirable to have an encryption algorithm that breaks this redundancy. Thus as a metric of encryption performance we find the correlation between adjacent pixels in a direction (Horizontal, Vertical or Diagonal). We have considered the Horizontal direction. 1024 random pixels are picked up from the image and its correlation between it's rightmost neighbour is found and plotted. For a good algorithm, the correlation plot should appear random with no discernable pattern

```
image = "HorizonZero"
ext = ".png"
ImageMatrix,image_size = getImageMatrix_gray(image+ext)
samples_x = []
samples_y = []
for i in range(1024):
  x = random.randint(0,image_size-2)
  y = random.randint(0,image_size-1)
  samples_x.append(ImageMatrix[x][y])
  samples_y.append(ImageMatrix[x+1][y])
plt.figure(figsize=(10,8))
plt.scatter(samples_x,samples_y,s=2)
plt.title('Adjacent Pixel Autocorrelation - Original Image', fontsize=20)
plt.show()
```



(a) (b)

Figure 4.4 : orginal image(a) original image auto correlation (b)

The figure 4.5: illustrates the graphical user interface of executing the application to encrypt such images and it code . calculated of Arnold algorithm , share(DWT)and (arnold scrambling).

```
def HenonEncryption(imageName,key):
    imageMatrix, dimension, color = getImageMatrix(imageName)
    transformationMatrix = genHenonMap(dimension, key)
    resultantMatrix = []
    for i in range(dimension):
        row = []
        for j in range(dimension):
            try:
                if color:
                    row.append(tuple([transformationMatrix[i][j] ^ x for x in imageMatrix[i][j]]))
                else:
                    row.append(transformationMatrix[i][j] ^ imageMatrix[i][j])
            except:
                if color:
                    row = [tuple([transformationMatrix[i][j] ^ x for x in imageMatrix[i][j]])]
                else :
                    row = [transformationMatrix[i][j] ^ x for x in imageMatrix[i][j]]
        try:
            resultantMatrix.append(row)
        except:
            resultantMatrix = [row]
    if color:
      im = Image.new("RGB", (dimension, dimension))
    else:
      im = Image.new("L", (dimension, dimension)) # L is for Black and white pixels

    pix = im.load()
    for x in range(dimension):
        for y in range(dimension):
            pix[x, y] = resultantMatrix[x][y]
    im.save(imageName.split('.')[0] + "_HenonEnc.png", "PNG")
```

```
            pix[x, y] = resultantMatrix[x][y]
    im.save(imageName.split('.')[0] + "_HenonEnc.png", "PNG")
```

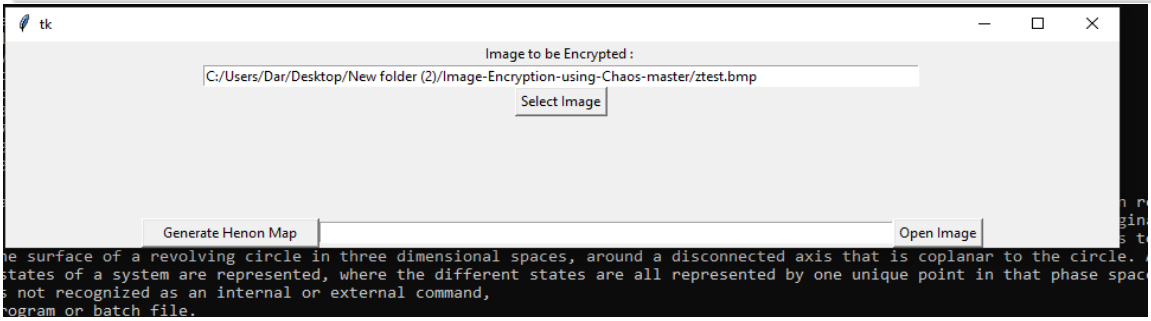


Figure 4.5: encryption boutton

4.2.3 Behavior and periodicity nature of ACM

Figure 4.6: show Behavior and periodicity nature of ACM for encryption ,an experiment is performed in phython to determine the chaotic behavior and periodic nature of Arnold cat map. For this the following 124*124 image of Lena is iterated [14] with the transformation ţ and the original image re appears after 15 iterations.

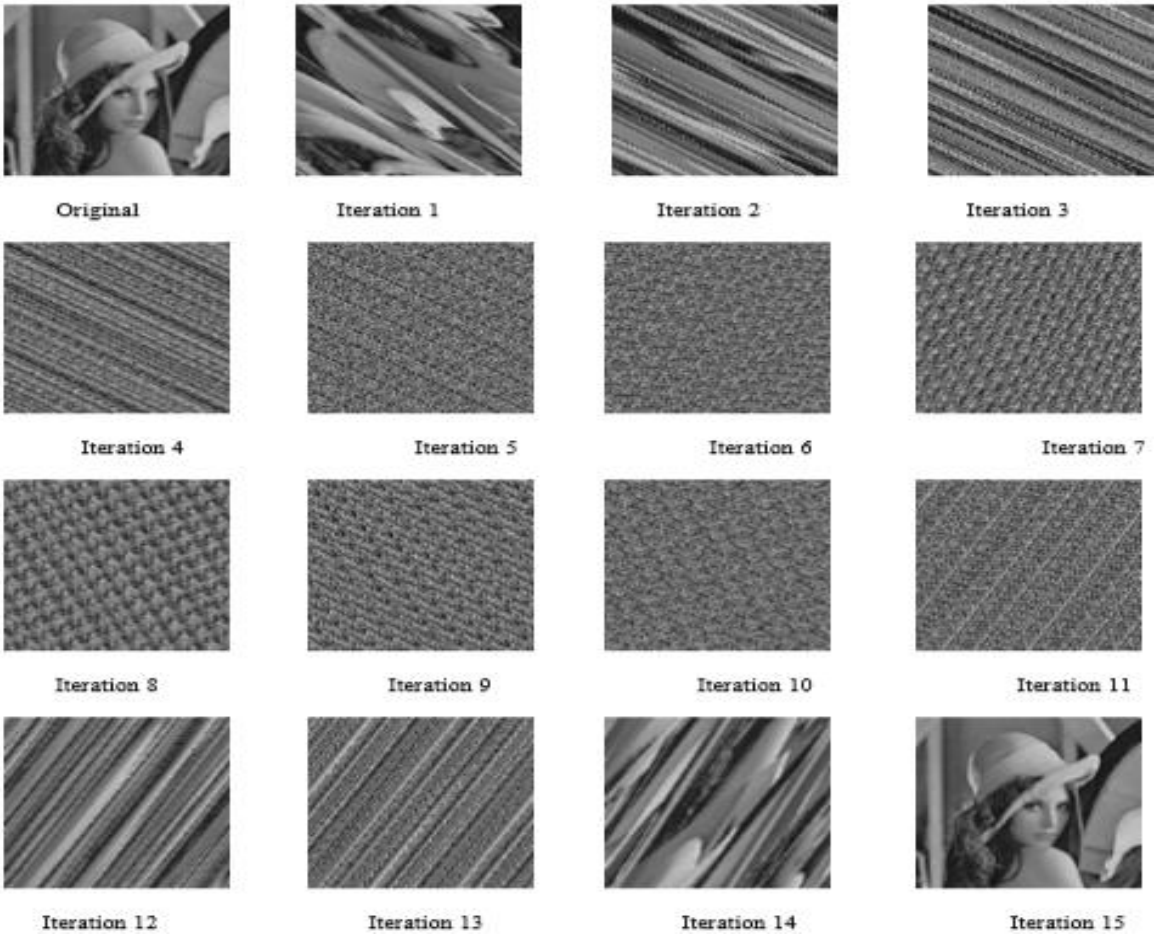


Figure 4.6: result of iteration [14]

4.2.4 Key generation

Figure 4.7: show the image that completely encrypt so key can generation by the number of iterations of transformations initially applied to get the encrypted image so key is put inside image because name of image change ,n - key is the number of rounds of transformations applied to get the decrypted image

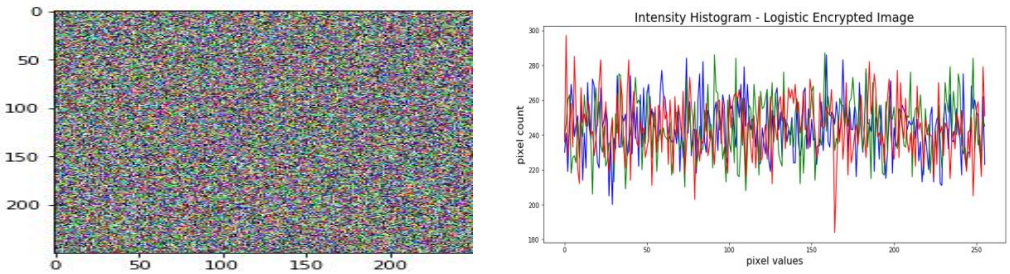
Figure 4.7: encrypt imag

4.2.5 histogram analysis of encrypt image

The figure 4.8: show main screen encrypt image histogram analysis so An image histogram illustrates that encrypt image shoud be deffirent from orginal image

```
image = "HorizonZero_HenonEnc"
ext = ".png"
img = cv2.imread(image + ext,1)
pil_im = Image.open(image + ext, 'r')
imshow(np.asarray(pil_im))
plt.figure(figsize=(14,6))

histogram_blue = cv2.calcHist([img],[0],None,[256],[0,256])
plt.plot(histogram_blue, color='blue')
histogram_green = cv2.calcHist([img],[1],None,[256],[0,256])
plt.plot(histogram_green, color='green')
histogram_red = cv2.calcHist([img],[2],None,[256],[0,256])
plt.plot(histogram_red, color='red')
plt.title('Intensity Histogram - Henon Map Encrypted Image', fontsize=20)
plt.xlabel('pixel values', fontsize=16)
plt.ylabel('pixel count', fontsize=16)
plt.show()
```



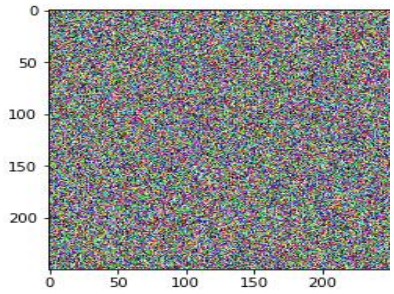
(a) (b)

Figure 4.8: encrypt image (a) intensity histogram of encrypt image (b)

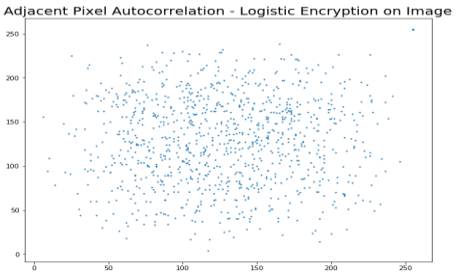
4.2.6 adjacent pixel uto correlation of encrypt image

Figure 4.9: show adjacent pixel uto correlation of encrypt image it will be different from orginal image

```
image = "HorizonZero_HenonEnc"
ext = ".png"
ImageMatrix,image_size = getImageMatrix_gray(image+ext)
samples_x = []
samples_y = []
print(image_size)
for i in range(1024):
  x = random.randint(0,image_size-2)
  y = random.randint(0,image_size-1)
  samples_x.append(ImageMatrix[x][y])
  samples_y.append(ImageMatrix[x+1][y])
plt.figure(figsize=(10,8))
plt.scatter(samples_x,samples_y,s=2)
plt.title('Adjacent Pixel Autocorrelation - Henon Encryption on Image', fontsize=20)
plt.show()
```



(c)



(d)

Figure 4.9: encrypt image(c)autocorrelation of encrypt image (d)

Figure 4.10: illustrates the graphical user interface of executing the application to decrypt such images. By decrypt key1 , key2 click sbutton (Decrypt henon map) to complete decryption process and show image that the user selected

```
def HenonDecryption(imageNameEnc, key):
    imageMatrix, dimension, color = getImageMatrix(imageNameEnc)
    transformationMatrix = genHenonMap(dimension, key)
    pil_im = Image.open(imageNameEnc, 'r')
    imshow(np.asarray(pil_im))
    henonDecryptedImage = []
    for i in range(dimension):
        row = []
        for j in range(dimension):
            try:
                if color:
                    row.append(tuple([transformationMatrix[i][j] ^ x for x in imageMatrix[i][j]]))
                else:
                    row.append(transformationMatrix[i][j] ^ imageMatrix[i][j])
            except:
                if color:
                    row = [tuple([transformationMatrix[i][j] ^ x for x in imageMatrix[i][j]])]
                else :
                    row = [transformationMatrix[i][j] ^ x for x in imageMatrix[i][j]]
        try:
            henonDecryptedImage.append(row)
        except:
            henonDecryptedImage = [row]
    if color:
        im = Image.new("RGB", (dimension, dimension))
    else:
        im = Image.new("L", (dimension, dimension)) # L is for Black and white pixels

    pix = im.load()
    for x in range(dimension):
        for y in range(dimension):
            pix[x, y] = henonDecryptedImage[x][y]
      im.save(imageNameEnc.split('_')[0] + "_HenonDec.png", "PNG")
```

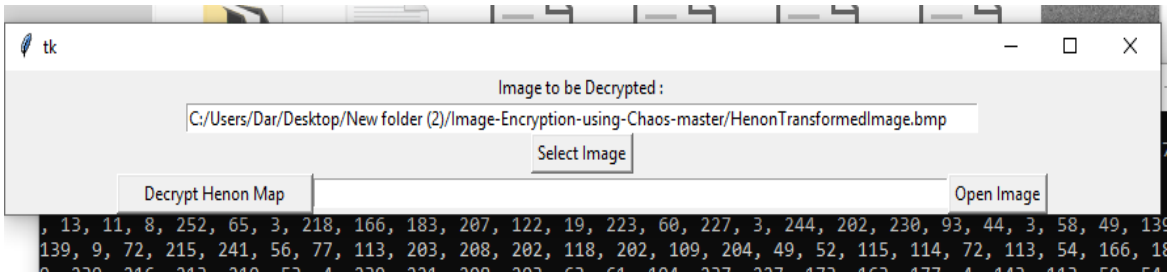


Figure 4.10: screen of decrypt image

4.3 Results Discussion

Arnold’s Cat Map algorithm (ACM) is one of the cryptographic algorithm used to encrypt the image [14]The concept of the algorithm is continuously rotate the image so that it becomes a form that is not visible and random so that the image can not be seen by the naked eye but can still be recognized by the system for image file (image) of the same so this technique is faster and easier to use in the process stream object both in terms of storage and process objects Only a few functions (chaotic maps) and some parameters (initial conditions) were quite good used if the process takes quite a long time

Algorithms Arnold's Cat Map is Encryption is good enough to secure a digital image, especially in the security pixel mostly algorithm cryptography secures files or specific to text, by using auto correlation and histogram analysis this tow step exam that this algorithm is fast and good for encrypt pixel image different with other algorithms Arnold's Cat Map could safeguard the image of a well without reducing the value or information of a digital image that is secured and this is one of the advantages of this algorithm .

Chapter Five
Conclusion and Recommendations

CHAPTER V
Conclusion and Recommendations

5.1 Conclusion

This research is based on the encryption and decryption of satellite imagery used by the Arnold and chaotic system. Arnold's cat map is simple and efficient in implementation to shuffle the image pixels and to completely disturb the correlation between the pixels but it is unsatisfactorily insensitive to changes in its controlling parameters. For image shuffling using the Cat map, the image may be recovered by iterating the chaotic map for some rounds under some control parameters. Arnold cat map has a lower key space so it can be combined with other chaotic maps to produce the encryption that is more resistant to brute force attacks. These maps are used for the key generation process and its purpose is to achieve the high level of confusion and diffusion during the entire process. The performance analysis of the algorithm shows the proposed system can be used efficiently for real time applications to perform encryption and decryption ,after that analysis the encrypt image and autocorrecting to give decrypt image as original

5.2 Recommendations

In this rehear, to overcome security, performance, privacy and reliability issues of satellite imagery, a new cryptosystem based on chaotic and Arnold algorithms has been proposed. This study works on a pixel manipulation analysis. One should note that neighboring pixels of satellite images are spatially auto-correlated. Hence, we can group these pixels based on some criteria and perform the operation at the object level. In general, object-based analysis starts with grouping pixels into meaningful objects through image segmentation techniques. Consequently, recently different image analysis like a satellite image classification has been on the object analysis. For the future, recommend extending the squeeze algorithms to work at the object level. One way could be by integrating the algorithm to the simplest compression algorithms such as quadtree decomposition and run length encoding.

Reference

Reference:

[**1]** Ahmad, M. (2011). Cryptanalysis of chaos based secure satellite imagery cryptosystem. International Conference on Contemporary Computing, Springer.

[2] Michael Mao Wang School of Information Science and Engineering, Southeast University, Nanjing, China 2019 Satellite Machine-Type Communication for Maritime Internet of Things: An Interference Perspective

[3]https://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Space_Threat_V14_020119_sm.pdf

[4] MusheerAhmad(2017)Cryptanalysis of Chaos Based Secure Satellite Imagery Cryptosystemq

[5] Abdullah Sharaf Alghamdi1, HanifUllah, Muhammad Usama Khan, Iftikhar Ahmad1 and Khalid Alnafajan1(2011). Satellite Image Encryption for C4I System

[6]Boukhatem Mohammed Belkaid and Cherifi Mehdi and lahdirmourad(2011)Meteosat Images Encryption based on AES and RSA Algorithms

[7] Barry G. Evans and Paul T. Thompson Centre for Communication Systems Research, University of Surrey, UK1945-2010: 65 Years of Satellite History from Early Visions to Latest Missions

[8] Prof. Dr. Ir. Alfred Stein Dr. Ir. Rolf A.de (2015) .COMPRESSION AND ENCRYPTION FOR SATELLITE IMAGES: A COMPARISON BETWEEN SQUEEZE CIPHER AND SPATIAL SIMULATIONS

[9] Musheer Ahmad and Omar Farooq Department of Computer Engineering, Faculty of Engineering and Technology, Jamia Millia Islamia, New Delhi 110025, India 2018 Secure Satellite Images Transmission Scheme Based on Chaos and Discrete Wavelet Transform

[10]https://www.infoguardsecurity.com/what-is-information-security-definition-principles-and-policies/

[11] Chong Fu,1,* Jun-jie Chen,2 Hao Zou,2 Wei-hong Meng,3 Yong-feng Zhan,3 and Ya-wen Yu(2016) A chaos-based digital image encryption scheme with an improved diffusion strategy

[12] Fredrik Svanström(2017) Properties of a generalized Arnold's discrete cat map

[13] Veena, V., et al. (2012). A robust watermarking method based on Compressed Sensing and Arnold scrambling. 2012 International Conference on Machine Vision and Image Processing (MVIP), IEEE.

[14] Wong, R., et al. (2017). "The compression of a sequence of satellite images based on change detection." International journal of remote sensing 18(11): 2427-2436.

[15] MADAN Mohammed BENTOUTOU Youcef , TALEB Nasreddine Djillali Liabes University of Sidi Bel-Abbes, Algeria Communication Networks, Architecture and Multimedia Laboratory, BP. 89 22000 Sidi Bel Abbes, Algeria 2017 An Improved Image Encryption Algorithm Based on Cyclic Rotations and Multiple Chaotic Sequences: Application to Satellite Images

[16] Tai, S.-C., et al. (2012). A near-lossless compression method based on CCSDS for satellite images. 2012 International Symposium on Computer, Consumer and Control, IEEE.

[17] 1Faculty of Computer Science,Universitas Pembangunan Panca Budi, Jl. Jend. GatotSubroto Km. 4,5SeiSikambing, 20122, Medan, Sumatera UtaraIndonesiaArnold's Cat Map Algorithm in Digital Image Encryption