ANALYSIS OF PARABOLIC ANTENNAS FOR RADIO TELESCOPES AND THE DEVELOPMENT OF ENCRYPTION METHODS FOR RADIO ASTRONOMICAL IMAGES

TING KUNG CHUANG

DOCTOR OF PHILOSOPHY IN ENGINEERING

FACULTYOF ENGINEERING AND GREEN TECHNOLOGY
UNIVERSITI TUNKU ABDUL RAHMAN
MARCH 2022

ANALYSIS OF PARABOLIC ANTENNAS FOR RADIO TELESCOPES AND THE DEVELOPMENT OF ENCRYPTION METHODS FOR RADIO ASTRONOMICAL IMAGES

By

TING KUNG CHUANG

A thesis submitted to the Department of Electronic Engineering,
Faculty of Engineering and Green Technology,
Universiti Tunku Abdul Rahman,
in partial fulfillment of the requirements for the degree of
Doctor of Philosophy in Engineering
March 2022

ABSTRACT

ANALYSIS OF PARABOLIC ANTENNAS FOR RADIO TELESCOPES AND THE DEVELOPMENT OF ENCRYPTION METHODS FOR RADIO ASTRONOMICAL IMAGES

Ting Kung Chuang

An analysis on the performance of Cassegrain reflector antennas has been presented. In this study, we have adopted the design parameters for the Cassegrain configuration used in the Atacama Large Millimeter Array (ALMA) project. The focal-length-to-diameter ratio *f*/D of the primary reflector has been adjusted to investigate the optimum performance of the antenna. In this study, signal frequency at the high edge of ALMA band 1, i.e. 45 GHz has been selected. The results obtained from the physical optics simulation show that the aperture efficiency of the antenna is at its optimum (i.e. 80.36%) when *f*/D ranges from 0.5 to 0.6. The radiation characteristics at this range of ratio are found to be similar. The radius of the secondary reflector and edge taper T_e which correspond to the optimum aperture efficiencies ranges from 371 mm to 372 mm and 10.64 dB to 10.75 dB, respectively. With the rapid progress in space technology development, a lot of digital images are transmitted back to ground telescope receiver. Thus, image security plays a significant role during the transmission process. Existing algorithms in image security were developed based on Latin squares, DNA sequence etc. However, the suitability of the techniques is questionable and high cost was needed. In this study, several development of encryption methods for radio astronomical images had been

studied and proposed. The proposed algorithms include Development of Bit-level Scrambling Encryption for Radio Telescope Imageries, Bit-levels Encryption for RGB Telescope Images, Bit-levels Encryption for RGB Telescope Images, Design of Encryption Algorithm in Combined Spatial and Frequency Domains for Telescope Grayscale and Bayer Images, and Combined Spatial and Frequency Domains in Algorithm of RGB Color Image Security for Telescope Images. The outputs were evaluated using histogram distribution, NPCR, UACI, PSNR, SSIM and information entropy. The results showed that this algorithm has better performance compared to other recently developed algorithms.

ACKNOWLEDGEMENTS

Acknowledgements are due to my supervisors, Associate Professor Ir. Dr. Yeap Kim Ho and Associate Professor Ir. Dr. Teh Peh Chiong for their attention and support throughout this study. I am particularly grateful to Associate Professor Ir. Dr. Yeap Kim Ho, without whose advice this study would be harder to understand and appreciate. Thanks are also due to Associate Professor Ir. Dr. Teh Peh Chiong, whose encouragement ensured the completion of the study. Thanks are due to my employer, Universiti Tunku Abdul Rahman for funding my study. I also would like to dedicate this thesis to my parents and colleagues. Many thanks are due to Dr. Lai Koon Chun for his encouragement towards the end of the project, and friends who have helped me in other ways. Last but not least, special thanks are due to my wife, my sons and my daughter, who have been very co-operative and also my source of inspiration.

APPROVAL SHEET

This dissertation/thesis entitled "***ANALYSIS OF PARABOLIC ANTENNAS FOR RADIO TELESCOPES AND THE DEVELOPMENT OF ENCRYPTION METHODS FOR RADIO ASTRONOMICAL IMAGES***" was prepared by TING KUNG CHUANG and submitted as partial fulfillment of the requirements for the degree of Doctor of Philosophy in Engineering at Universiti Tunku Abdul Rahman.

Approved by:

_____
(Assoc. Prof. Ir. Dr. YEAP KIM HO)
Date:……..
Professor/Supervisor
Department of Electronic Engineering
Faculty of Engineering and Green Technology
Universiti Tunku Abdul Rahman

_____
(Assoc. Prof. Ir. Dr. TEH PEH CHIONG)
Date:……..
Professor/Co-supervisor
Department of Electronic Engineering
Faculty of Engineering and Green Technology
Universiti Tunku Abdul Rahman

FACULTY OF ENGINEERING AND GREEN TECHNOLOGY

UNIVERSITI TUNKU ABDUL RAHMAN

Date: _____

SUBMISSION OF FINAL YEAR PROJECT /DISSERTATION/THESIS

It is hereby certified that TING KUNG CHUANG (ID No: 16AGD00953) has completed this thesis entitled "Analysis of Parabolic Antennas for Radio Telescope and The Development of Encryption Methods for Radio Astronomical Images" under the supervision of Assoc. Prof. Ir. Dr. Yeap Kim Ho (Supervisor) from the Department of Electronic Engineering, Faculty of Engineering and Green Technology , and Assoc. Prof. Ir. Dr. Teh Peh Chiong (Co-Supervisor) from the Department of Electronic Engineering, Faculty of Engineering and Green Technology.

I understand that University will upload softcopy of my thesis in pdf format into UTAR Institutional Repository, which may be made accessible to UTAR community and public.

Yours truly,

_____
(*TING KUNG CHUANG*)

*Delete whichever not applicable

DECLARATION

I hereby declare that the dissertation is based on my original work except for quotations and citations which have been duly acknowledged. I also declare that it has not been previously or concurrently submitted for any other degree at UTAR or other institutions.

Name Ting Kung Chuang

Date _____

LIST OF TABLES

LIST OF FIGURES

TABLE OF CONTENTS

CHAPTER ONE

INTRODUCTION

1.1 Background

A radio telescope is an astronomy apparatus that receives radio waves from space. The dish, receiver, detector, and analyser are the four essential components of a radio telescope. A larger dish can collect more radio waves into the receiver, converting them into electrical impulses. To eliminate noise from the motion of the atoms in the metal, the receiver is frequently kept below freezing temperatures, as low as -270 degrees Celsius. The detector detects the electrical signal's power density and converts it into a digital image. The analyser, which is usually a computer, takes the data and converts it into an image.

Digital images are important communication elements in telecommunications development. Different fields of images are transmitted throughout the network such as military, medical, and astronomy images. Therefore, digital image security is demanded in the market to ensure the images are being protected. Digital image security issues increase rapidly nowadays in the era of digitalization. This is due to the fact that images in digital format are vulnerable to cyber-attacks or re-dissemination. Therefore, digital image

security methodologies are demanded in the market so as to protect the security of the images (Ghadirli *et al.,* 2019).

Various researches had been carried out for the purposes of securing data transmission. (Ghadirli *et al.,* 2019) proposed an encryption algorithm that combines chaotic map and DNA sequence operations. The method is applied on R, G and B channels separately with Arnold map. (Wang *et al.,* 2020) on the other hand, applied the chaotic system with Knuth-Durstenfeld algorithm. According to their studies, the hidden attractor chaos system should be selected as it is hard to be decrypted.

1.2 Introduction

The Atacama Large Millimeter/Submillimeter (ALMA) radio telescope is studied here. It is situated at a height of 5000 metres in Chile's Atacama Desert. ALMA is a high-precision radio interferometer made up of 66 antennas. Fifty 12-meter antennas for high-resolution, high-sensitivity imaging, twelve 7-meter antennas, and four 12-meter total power antennas are among the 66 antennas that make up the Atacama Compact Array, which improves wide-field imaging (Wootten, 2008).

With the rapid progress in space technology development, a lot of digital images require processing. Thus, image security plays a significant role during the transmission process. Existing algorithms in image security were developed based on Latin squares, DNA sequence etc. However, the suitability of the

techniques is questionable and high cost was needed. In this research, analysis of parabolic antennas for radio telescopes had been done and various development of encryption methods for radio astronomical images had been studied.

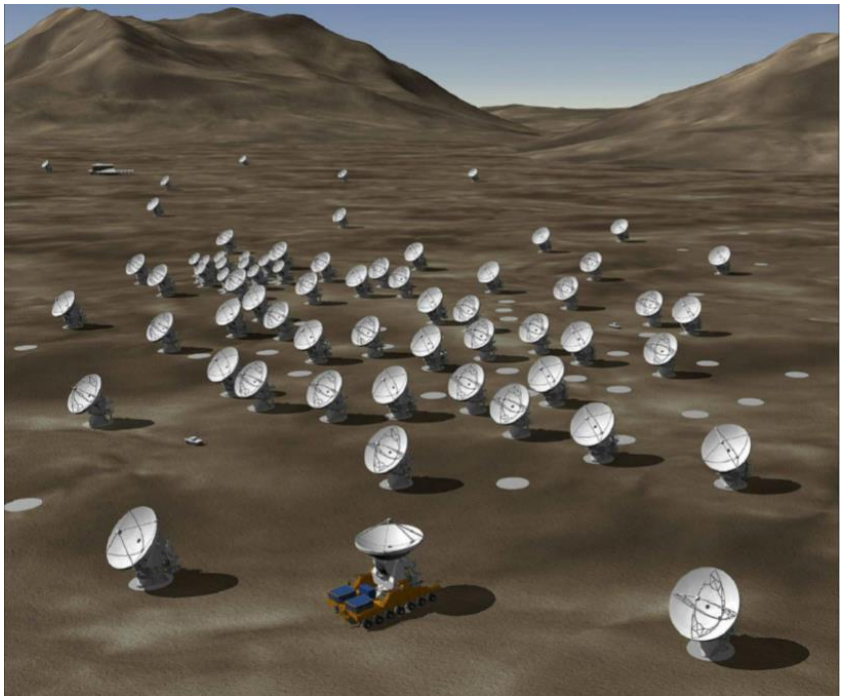


Figure 1.1: Atacama Large Millimeter/Submillimeter (ALMA) radio telescope (About ALMA - ALMA, n.d.)

According to Zhou *et al.,(*2014), the digital images have been increasingly applied, stored and transmitted. Thus, the protection of this type of information is a critical challenge.

1.3 Problem Statements

Below are the problem statements in this research:

1. Hardware design of ground radio telescope can be improved to obtain better outcomes or performance of the received signals
2. Better algorithm for image security of the signal received is needed during transmission of signals.
3. Image security of signal received can be improved by novel algorithm design

1.4 Research Objectives

There are various objectives to be achieved in this research. They are:

1. To optimize the telescope aperture efficiency by performance analysis on current telescope design.
2. To design novel algorithms for optimal security in telescope images.
3. To develop a reliable methodology for Digital Image Security.

1.5 Structure of Dissertation

This thesis is devoted to do analysis on the parabolic antennas for radio telescopes especially ALMA and the development of various encryption methodologies had been studied. The steps and stages of research are documented in this thesis. This thesis consists of six chapters.

Chapter 1 introduces briefly about the project's background of analysis parabolic antennas for radio telescopes and the development of encryption methods for radio astronomical images.

Chapter 2 is brief literature review which is related to this research study which contains electromagnetic spectrum, single dish radio telescopes, ALMA, Gaussian beam quasioptics, color image, grayscale image, Bayer image, bit planes, DNA sequence, Latin squares, skew tent map, and Chipertext feedback.

Chapter 3 reports the design of radio telescope and various methods of digital image encryption for radio astronomical images.

Chapter 4 discusses the output performance of the telescope design and encryption methods for radio astronomical images.

In Chapter 5, conclusion are drawn based on the whole project and the results of the system. Future works are suggested for further research in the future.

CHAPTER TWO

LITERATURE REVIEW

2.1 Background

The numerous analytical methodologies that have been used throughout this thesis are presented in this chapter and brief literature review had been done throughout the research which includes the study of electromagnetic spectrum, single dish radio telescopes, ALMA, Gaussian beam quasioptics, color image, grayscale image, Bayer image, bit planes, DNA sequence, Latin squares, skew tent map, and Chipertext feedback.

Many encryption techniques have been developed in recent years such as those based on Latin squares (Xu & Tian, 2018; Wu *et al.*, 2014), skew tent map (Kadir *et al*., 2014), DNA sequence (Wei *et al.*, 2012) and ciphertext feedback (Zhang *et al.*, 2014). Some of these techniques have an acceptable level of security. Although Latin squares is claimed to be having some good characteristics for image encryption, the suitability of the technique for image encryption is questionable (Wu *et al.*, 2014). Also, even though the DNA cryptography schemes in the research of Gehani (2003) has the benefit of storing a huge one-time pad, a well-equipped laboratory is required and high cost is needed to conduct the experiment.

The focus of this research is to generate encrypted telescope images using a novel algorithm in RGB (Red, Green, Blue) color image security. Fourier transform (FT) is applied for the frequency domain and bit levels decomposition is used in the spatial domain. The encrypted images are generated using two levels scrambling method. The experimental results of this study show that the proposed algorithm has better performance compared to other recently developed algorithms.

Finally, all related information studied are mainly for the purpose of telescope analysis and novel encryption methodologies development.

2.2 Electromagnetic Spectrum

Figure 2.1 depicts the submillimetre or far-infrared waveband, this waveband has been linked to the waveband of terahertz (THz), which falls between among 300 GHz and 3 THz (Yun-Shik, 2008).

This waveband is the least studied portions of the electromagnetic spectrum in astronomy because of the complications in developing sensitive detection and source methods. However, it is sometimes thought to have boundaries ranging from 100 GHz to 10 THz.

Modelling terahertz radiation propagation through receivers has proven challenging in the past. The Terahertz band lies between the microwave and optical regimes. On the other hand, diffraction effects significantly dominate

the propagation of radiation in the extremely low frequency radio spectrum, demanding solutions to Maxwell's equations.

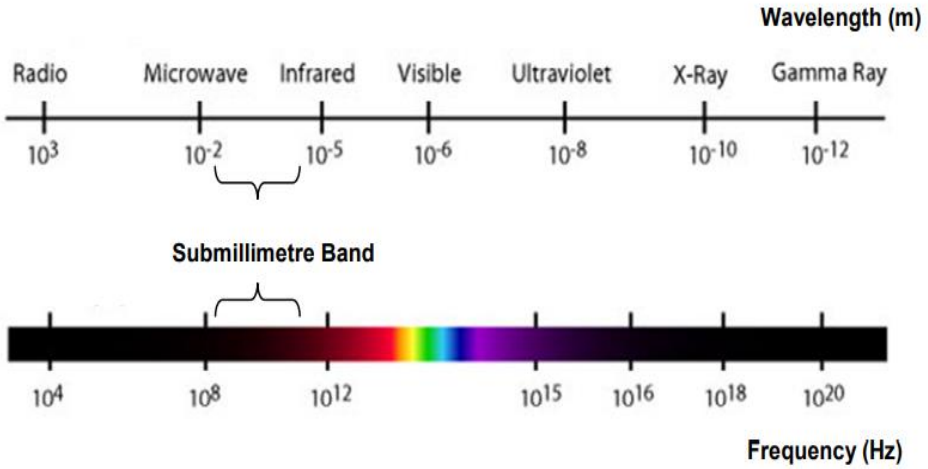


Figure 2.1: Location of submillimetre band in Electromagnetic Spectrum

2.3 Single Dish Radio Telescopes

The frequency range determines how a radio telescope is set up. Wire antennas are used for lower frequency frequencies, whereas reflector antennas are used for higher frequency frequencies. According to Tercero (2008), these antennas concentrate radiation into a single point, with an extra antenna functioning as a system feeder, and the cutting edge between low and high frequencies is not sharp, necessitating the mixing of technologies from multiple frequency regimes.

Reflecting telescopes employ mirrors to gather and concentrate light. Because they depend on reflection rather than refraction, they are devoid of

chromatic aberration. Because they just have one optical surface, mirrors are also simpler to deal with than lenses.

Mirrors are often built of a stiff material with a low thermal expansion coefficient that is coated with a thin coating of aluminium, silver, or gold to increase reflectivity. A reflector is a telescope that uses a mirror to gather and concentrate light. The paraboloid reflector functions as a phase-transformer after reflecting the parabola, turning spherical waves from the focal point to flat phase front waves.

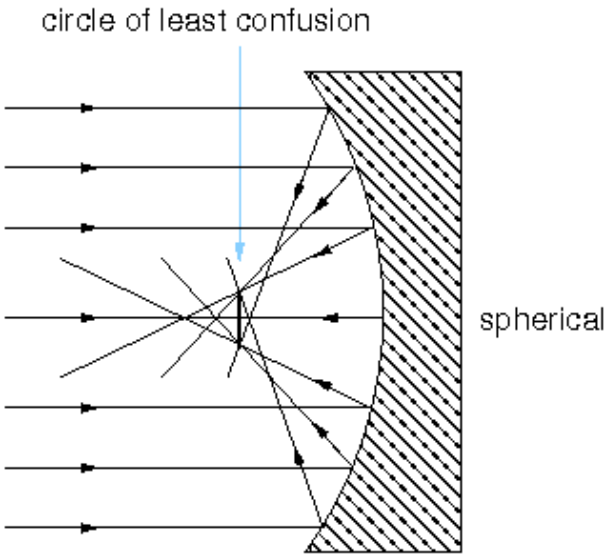


Figure 2.2: Image suffers from spherical aberration (L07: Reflectors, n.d.)

Reflectors, on the other hand, are not without flaws. The simplest mirror to create is a spherical mirror. Figure 2.2 shows how rays from the mirrors edge concentrate closer to the mirror than rays from the centre, resulting in a fuzzy disc image of a point source. This flaw is known as spherical aberration.

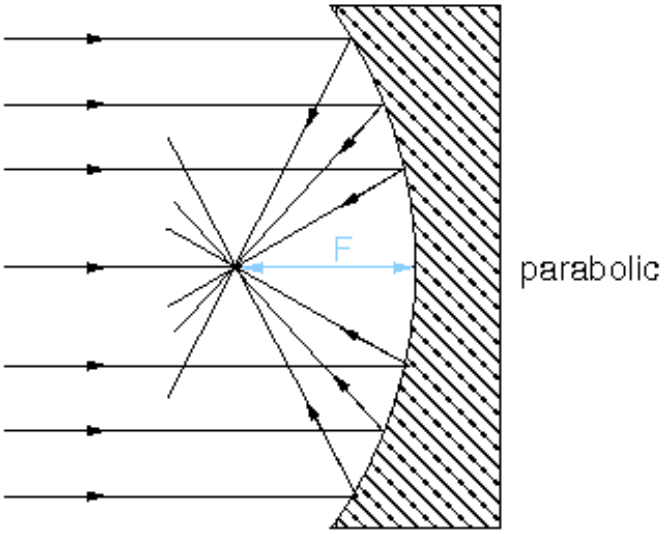


Figure 2.3: Spherical aberration can be removed by parabolic mirror (L07: Reflectors, n.d.)

The Newtonian telescope is a two-mirror system with a concave parabola as the main light path mirror and a flat secondary mirror with no curvature.

The light is simply folded through 90 degrees, with the focal plane just outside the incoming beam. At the Newtonian focus, the focal ratio is usually around 5. In relation to the primary mirror, the secondary mirror is at a 45^{o} angle. The flat's base is elliptical in shape in order to reduce the amount of the circular shadow it produces on the primary.

Although Newtonian setups are still employed in small amateur telescopes, visual access to the focus becomes difficult as the telescope becomes

larger, and installing equipment there would throw the telescope off balance. At professional observatories, Newtonians are quite uncommon.

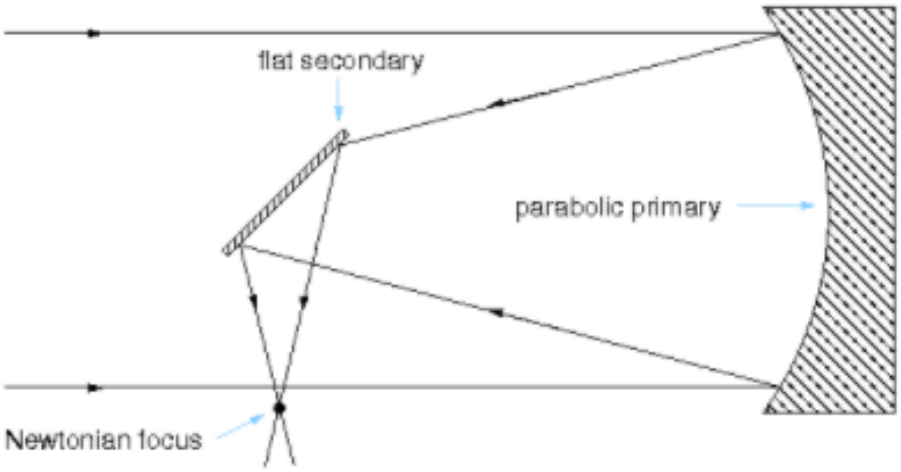


Figure 2.4: Schematic of a Newtonian reflector (L07: Reflectors, n.d.)

The combination of paraboloid and hyperbolic reflectors known as the Cassegrain antenna has the axis of rotation of both surfaces coinciding, according to the research of Reflecting Telescopes (2020).

The Cassegrain telescope features a concave parabolic primary mirror, just like the Newtonian, but a convex hyperbolic secondary mirror. The beam is reflected back to the primary, where it passes through a hole punched in the mirror's centre and focuses immediately below it, increasing the telescope's focal length. This method is much more focus than the Newtonian, and it is an excellent location for large, weighty instruments. When compared to a Newtonian, having a hole in the primary loses nothing because it is in the shadow of the secondary.

Furthermore, since the beam is folded back on itself, a telescope with a substantially longer focal length may be built without a pretty long tube: a typical Cassegrain focus has a focal ratio of 15.

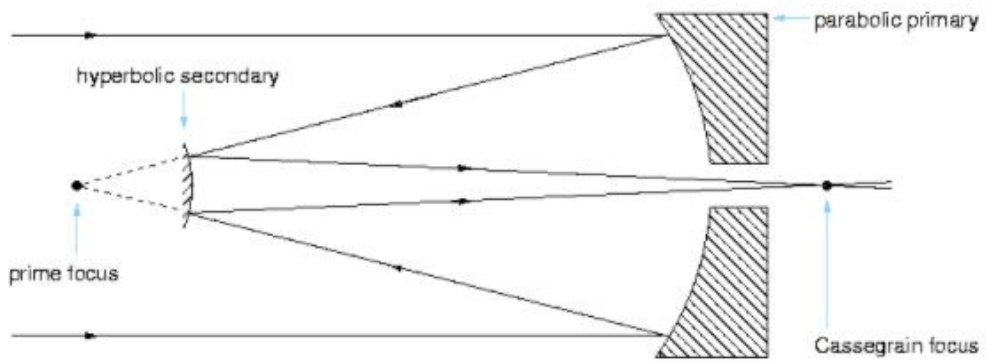


Figure 2.5: Schematic of a Cassegrain reflector (L07: Reflectors, n.d.)

For professional observatories, another benefit of the Cassegrain design is that it permits access to prime focus by removing the secondary mirror. The Newtonian counterpart has a much lower focal ratio and consequently a larger field of vision than the Cassegrain focus. Because prime-focus imaging has a larger field of view than Cassegrain-focus imaging, it is more prone to off-axis aberrations, necessitating the employment of lens-based correctors.

There is another classical two mirror telescopes which is called as Gregorian Telescope. Figure 2.6 shows the schematic of a Gregorian reflector. It contains of two concave mirrors.

The secondary is placed axially outside of the primary's focus, F_1, forms properly oriental final focus F by refocusing diverging light cone coming from the primary. In classical arrangement, primary is paraboloid, hence for the

secondary to maintain zero spherical aberration it has to be an ellipsoid with it near focus coinciding with the primary's focus.

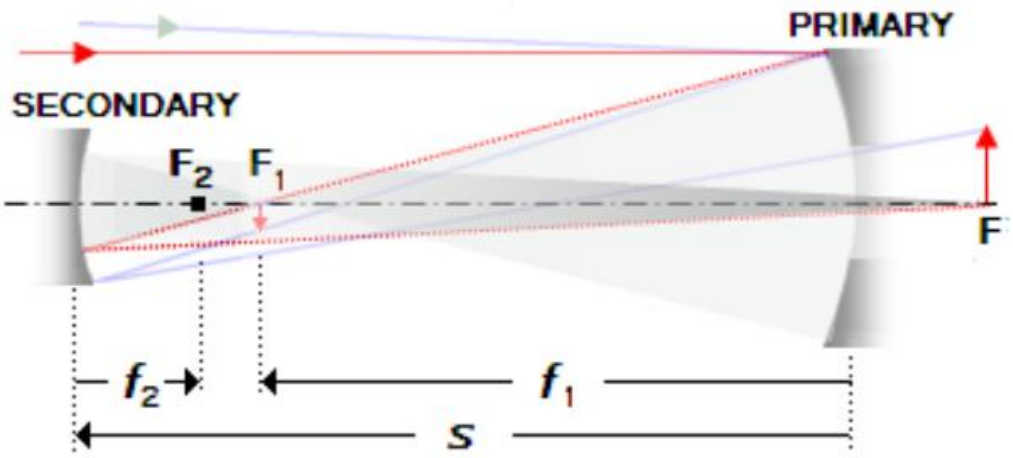


Figure 2.6: Schematic of a Gregorian reflector (Two-Mirror Telescopes: Cassegrain, Gregorian and Variants, n.d.)

2.4 ALMA

As a ground-based observatory, the Atacama Large Millimeter/Submillimeter (ALMA) radio telescope is explored. ALMA is a high-precision radio interferometer which are made up of 66 antennas. Each ALMA receiver is setup uniquely because of the vast frequency covering (30 until 950 GHz), yet they do share certain common traits and requirements. Either feed horn or quasioptical radiator are used in each channel. Every receiver employs a mix of lenses and off-axis mirrors to ensure that emission can be concentrated to the telescope's feed horn. Each ALMA receiver is built to receive linear polarisations of orthogonal. They are coincident on the sky and keep the cross polar energy level at least -24 dB below the copolar power level (Murphy, 1987)

The receiver channel designs are divided into three groups, each representing the changes in beam sizes at different frequencies. Table 2.1 shows the 10 channels of ALMA receivers with its operational frequency ranges. Figure 2.7 depicts the span of receiver channel frequency ranges at the ALMA telescopes (National Radio Astronomy Observatory - Legacy Content - ALMA (CV), 2022)

Table 2.1: Operating Frequency ranges for 10 ALMA receiver frequency Band

Receiver frequency Band	Bottom Frequency (GHz)	Ceiling Frequency (GHz)
1	31	45
2	69	90
3	84	116
4	125	164
5	165	211
6	211	275
7	275	370
8	385	500
9	602	720
10	787	950

Since the receivers in Bands 1 and 2 operate across the largest wavelength ranges, they are considered as most limited in opto-mechanical size. As optical components in frequencies Band 1 and 2 are considered as huge to fit into the Dewar flask. All optics are in the room temperature except feed horns, which are at cold temperature. In Bands 3 and 4, cooled and room temperature reflecting optics are used in the receivers. All optical components in Bands 5 through 10 of receivers are small enough to fit within the cryostat.

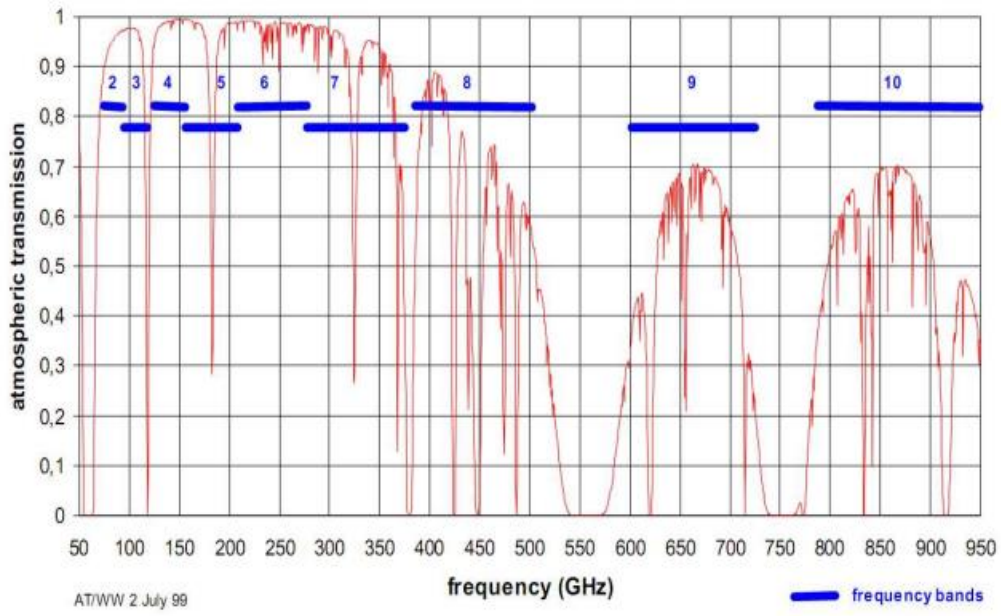


Figure 2.7: The span of the receiver channel frequency ranges (National Radio Astronomy Observatory - Legacy Content - ALMA (CV), 2022)

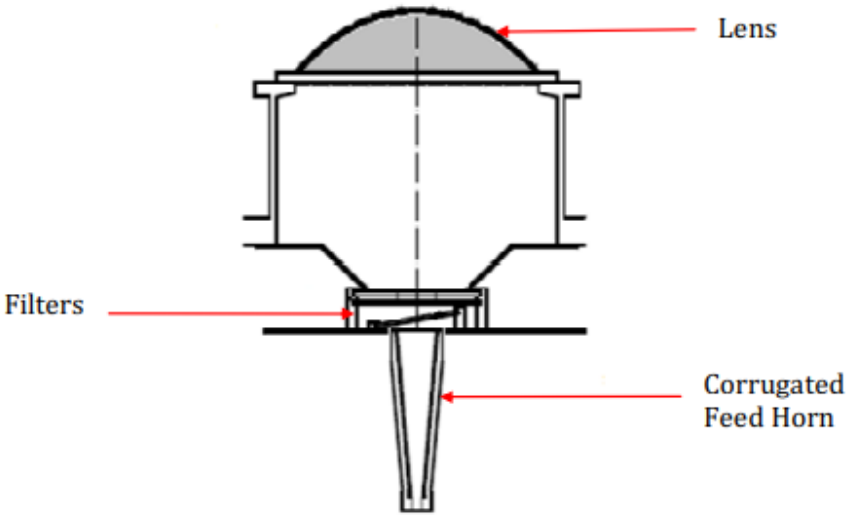


Figure 2.8: Typical Optical Layaout for Receiver in Band 1 and 2 (Carter *et al.*, 2007)

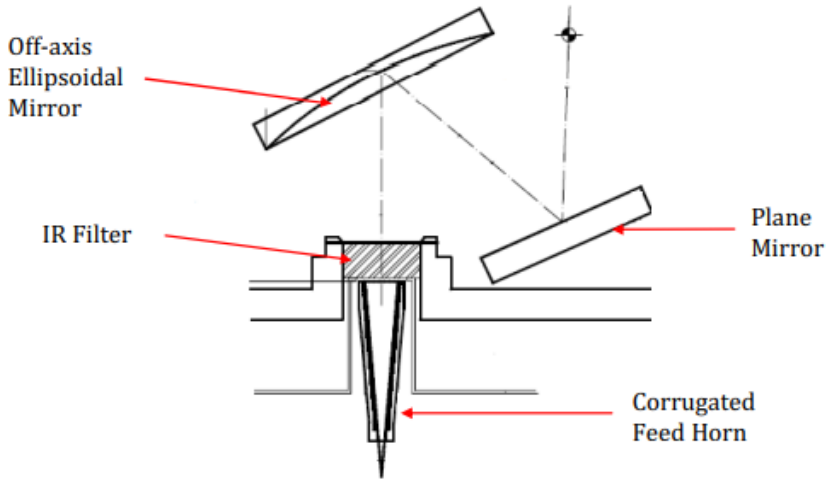


Figure 2.9: Typical Optical Layout for Reciever in Band 3 amd 4 (Carter *et al.*, 2007)

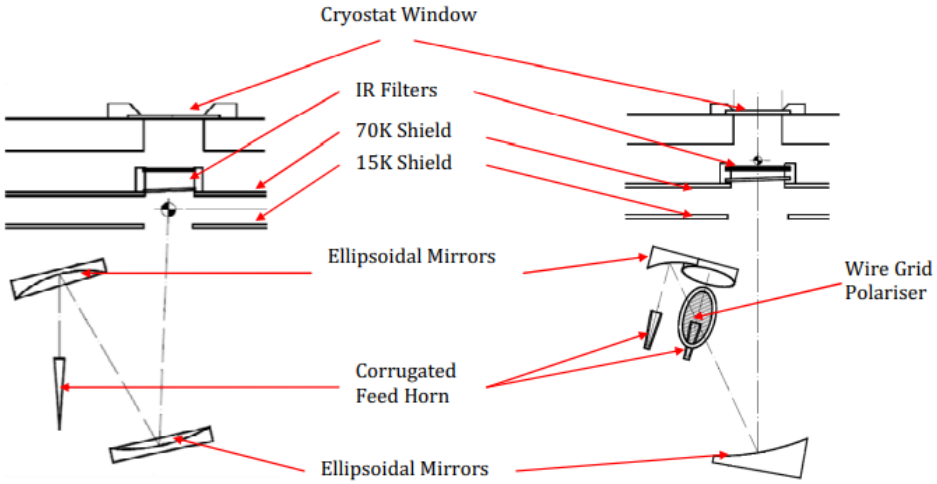


Figure 2.10: Optical Configuration for Band 5 to 10. (Carter *et al.*, 2007)

2.5 Gaussian Beam Quasioptics

In their study, Yeap *et al.* (2017) used Gaussian Bean Quasioptics. Figure 2.12 shows the Gaussian Beam Quasioptics equivalent of the standard optical system setup in Figure 2.11, with the ellipsoidal mirrors simulated using thin lenses.

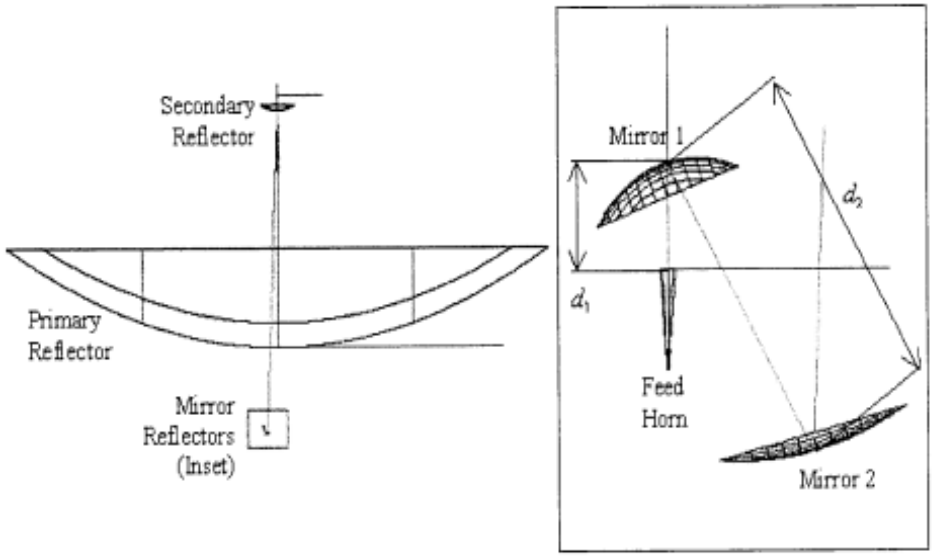


Figure 2.11: Typical Optical System Design for Cassegrain Antenna Comprising the Feed Opics (Tham, C.Y., *et al.* 2007)

To create a quasioptical system, Goldsmith (1998) said that the radiation beam must be confined, which essentially implies avoiding the monotonic expansion of an undisturbed Gaussiam Beam. Quasioptical systems combine optical components and waveguide, demonstrating the diffraction-dominated and the integration of geometrical optics approaches. These systems may be analysed in a variety of ways. The methodologies used in this thesis are a mix

of Physical Optics (PO) and Gaussian Beam Mode Analysis (GBMA). Murphy (1987) offered a rather thorough description of Gaussian Beam Mode Analysis (GBWA). GRASP physical optics compiler is used to compute the spillover efficiency, and plot the radiation patterns of the antennas.

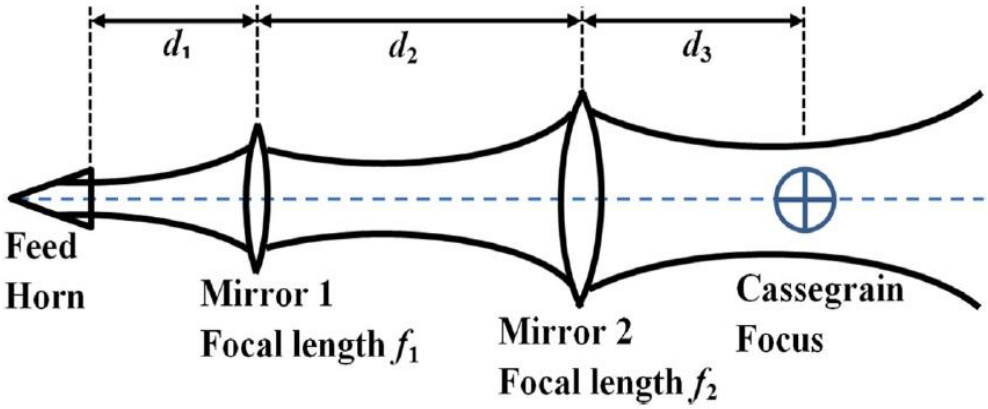


Figure 2.12: Gaussian Beam Quasioptics equivalent of the optical system (Yeap *et al.*, 2017)

The ABCD matrix technique as applied to quasioptical systems is shown below using an example from the Gaussian Beam Telescope (GBT).

The transformation of a Gaussian beam is shown below which is for an arbitrary optical system:

$$M = \begin{bmatrix} A_N & B_N \\ C_N & D_N \end{bmatrix} \begin{bmatrix} A_{N-1} & B_{N-1} \\ C_{N-1} & D_{N-1} \end{bmatrix} \dots \begin{bmatrix} A_1 & B_1 \\ C_1 & D_1 \end{bmatrix} \qquad (2.1)$$

where the ABCD matrices multiplication order is reversed compared to their original multiplication order.

The GBT is made up of two focusing components separated by the sum of their focal lengths. The ABCD matrix used in the GBT is quite simple to be calculated. The GBT is seen to be made up of two thin lenses with a propagation distance of d= *f*1 + *f*2 and focal lengths of *f*1 and *f*2. The optical arrangement in Gaussian Beam telescope is illustrated in Figure 2.13.

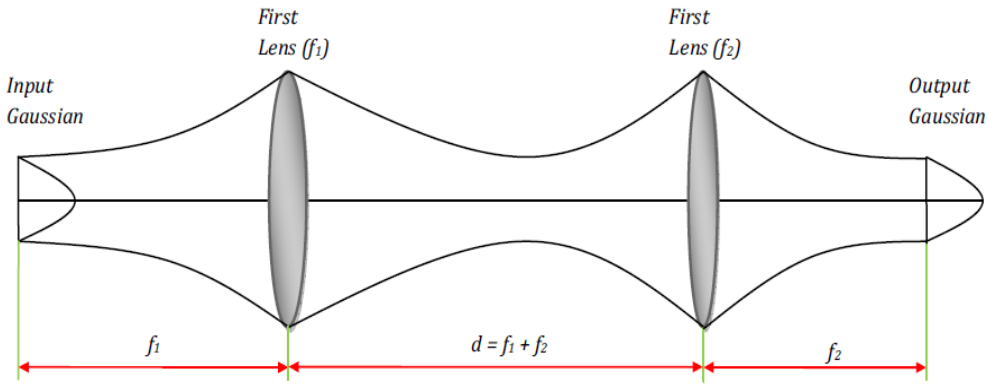


Figure 2.13: Optical Arrangement in Gaussian Beam telescope

This optical system's combined ABCD matrix is written as follows:

$$M = \begin{bmatrix} 1 & f_2 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ -\frac{1}{f_2} & 1 \end{bmatrix} \begin{bmatrix} 1 & f_1 + f_2 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ -\frac{1}{f_1} & 1 \end{bmatrix} \begin{bmatrix} 1 & f_1 \\ 0 & 1 \end{bmatrix} \tag{2.2}$$

Which simplifies to

$$M = \begin{bmatrix} \frac{f_2}{f_1} & 0 \\ 0 & \frac{f_1}{f_2} \end{bmatrix} \begin{bmatrix} 1 & f_1 + f_2 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ -\frac{1}{f_1} & 1 \end{bmatrix} \begin{bmatrix} 1 & f_1 \\ 0 & 1 \end{bmatrix} \tag{2.3}$$

2.6 Color Image

According to Gonzalez et al. (2018), thorough experimental data has revealed that the human eye's 6 to 7 million cones may be split into three main sensory groups, roughly corresponding to Red (R), Green (G), and Blue (B) color. Only around 2% of all cones are sensitive to blue light, while 65 percent of all cones are responsive to red light, 33 percent to green light, and only about 2 percent are sensitive to blue. The blue cones, on the other hand, are the most sensitive.

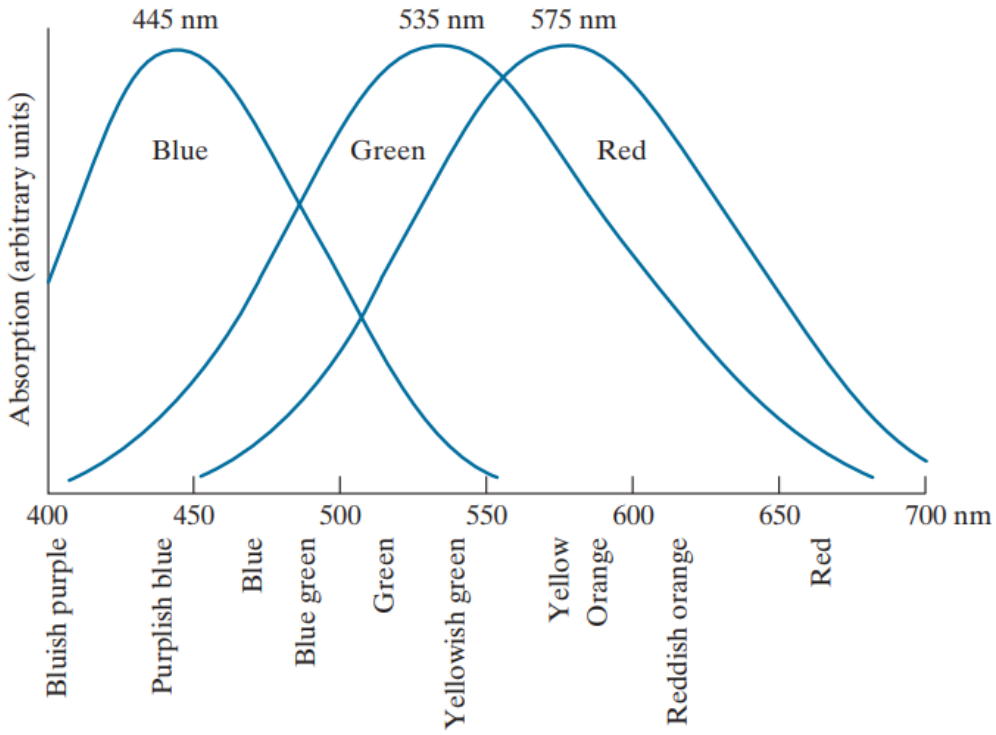


Figure 2.14: Absorption of light by the red, green, and blue cones in the human eye as a function of wavelength. (Gonzalez & Woods, 2018)

Figure 2.14 shows the average experimental curves indicating the absorption of light by the Red (R), Green (G), and Blue (B) cones in the human eye. Due to the absorption properties, the human eye sees colours as various combinations of the so-called primary hues, there are Red (R), Green (G), and Blue (B).

The RGB colour model divides images into three parts, one for each of the primary colours. Primary colours include R, G, and B. The number of bits needed to represent each pixel in RGB space is referred to as pixel depth.

Each RGB colour pixel has a depth of 24 bits with these settings (three image planes are multiplied with the number of bits of each plane). Any digital-color image is frequently referred to a 24-bit RGB colour image. Therefore, the total number of possible colours of any 24-bit RGB image is 28^3= 16,777,216.

Figure 2.15: A 24-bit RGB Color Cube (Gonzalez & Woods, 2018)

Color pixels are vectors, and each full-color picture has at least three components. As shown in Figure 2.15, each colour point in the RGB coordinate system may be seen as the vector spanning as shown in (2.4). In RGB colour space, let C represents any arbitrary vector:

$$C = \begin{bmatrix} C_R \\ C_G \\ C_B \end{bmatrix} = \begin{bmatrix} R \\ G \\ B \end{bmatrix} \tag{2.4}$$

2.7 Grayscale Image

Images in the RGB colour scheme are made up of three parts, generally referred to as the Red, Green, and Blue components (Gonzalez & Woods, 2018). These RGB photos may be transformed to Grayscale images using the approach in Figure 2.16. Any RGB colour image may be converted to a grayscale image using (2.5).

$$Grayscale = \frac{(R+G+B)}{3} \tag{2.5}$$

where R is value in Red component, G is value in Green component and B is value in Blue component.

2.8 Bayer Image

The three components of a digital colour image are R, G, and B., where R stands for red, G for green, and B for blue. A Bayer picture is a colour filtered array with three colour components filtered and organised on a grid of photo sensors. The pattern of a Bayer picture is made up of 50% green, 25% red, and

25% blue components from the original RGB image. The RGB picture and its Bayer counterpart are shown in Figure 2.17.

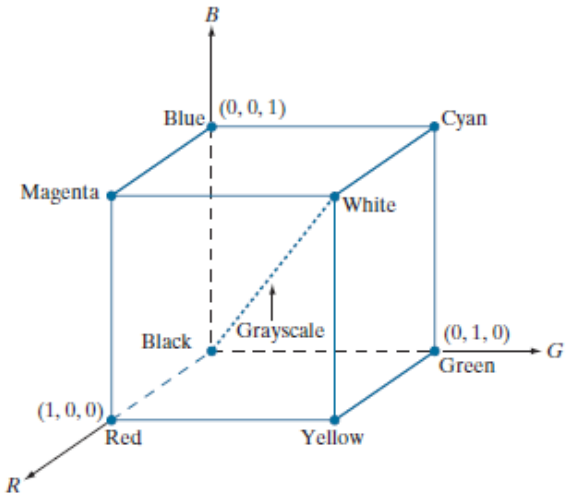


Figure 2.16: RGB Color Model (Gonzalez & Woods, 2018)

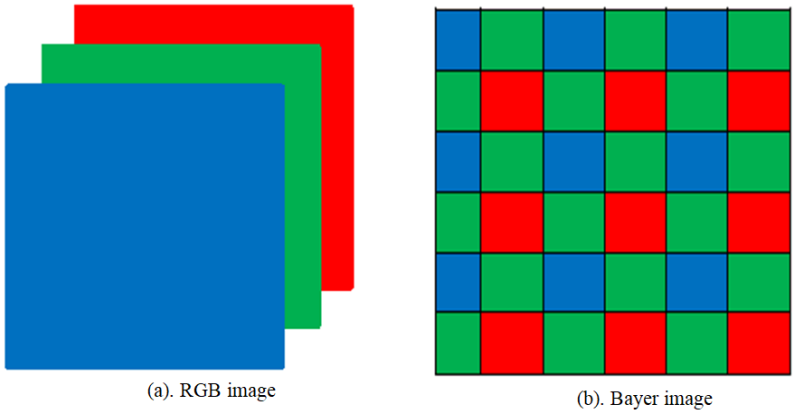


Figure 2.17: RGB and corresponding Bayer image (Gonzalez & Woods, 2018)

2.9 Bit Planes

A digital image is made up of m × n pixels, with each pixel having a level value assigned to it. The pixel value of a digital picture is separated into

two categories: grey level and colour level. According to Ting *et al.* (2013), any digital image is made up of 8-bit levels for both grey and colour levels, ranging from 0 to 255 for each pixel. The fundamental distinction between grey and colour level is that grey level only includes a single plate of grey colour, whereas colour level is made up of Red, Green, and Blue colours, or RGB for short.

Higher order bits, according to Gonzalez & Woods (2018), carry the bulk of visually significant data, while lower order bits include the image's fine details. As a result of the bit order, eight groups are generated, and the grouped binary information is referred to as the bit plane. All of the pixels' least significant bits are in bit plane 0, while all of the pixels' most significant bits are in bit plane 7. The following equation depicts the process of obtaining eight bit planes with *M* rows and *N* columns pixels:

$$f(x,y) = \begin{bmatrix} f(0,0) & \cdots & f(0,N-1) \\ \vdots & \ddots & \vdots \\ f(M-1,0) & \cdots & f(M-1,N-1) \end{bmatrix} \tag{2.6}$$

$$f_{bit-plane\ i} = R\left[\frac{1}{2} floor(\frac{1}{2^i}[f(x,y)]\right] \tag{2.7}$$

where $f(x,y)$ is original image, R is the remainder, and $floor\ (x)$is round the elements to x nearest integers less than or equal to x.

Each pixel value in a grayscale image is separated into two parts, they are known as the Least Significant Bits (LSB) and Most Significant Bits (MSB), according to Liu *et al.* (2019). All of the *i*-th bits of each pixel's binary

representation are included in the *i*-th bit plane (David *et al.*, 2009). The outcome of 8 bit planes extraction is shown in Figure 2.18.

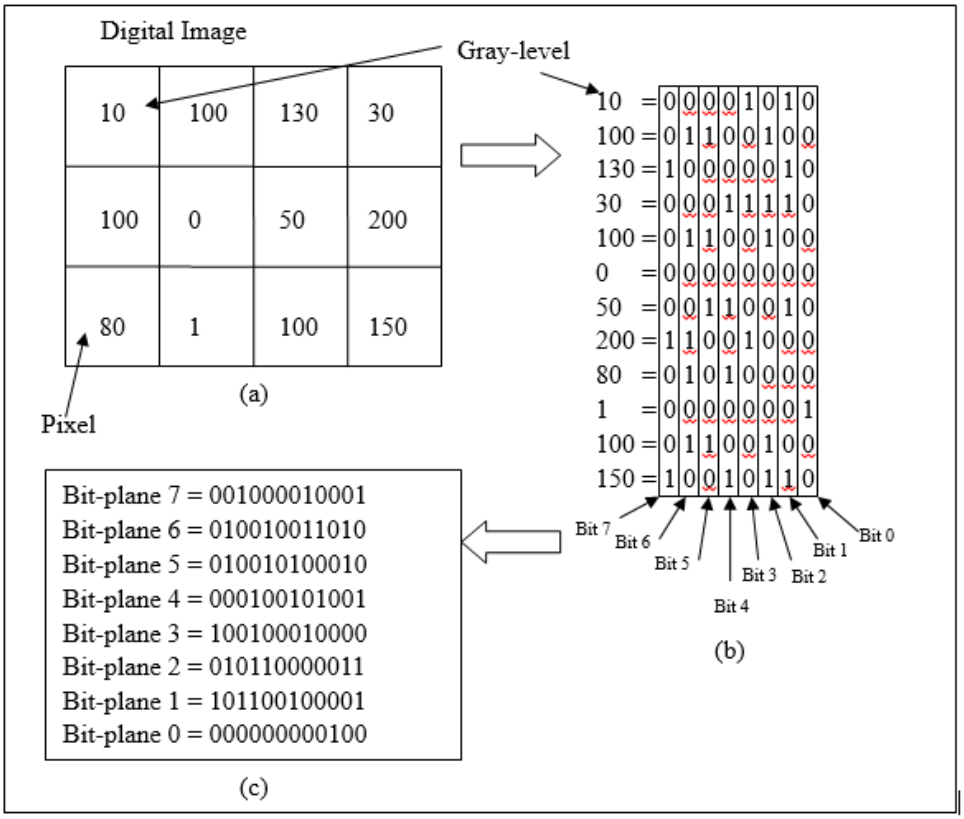


Figure 2.18: Output of 8 bit-plane extraction (Ting *et al.*,2013)

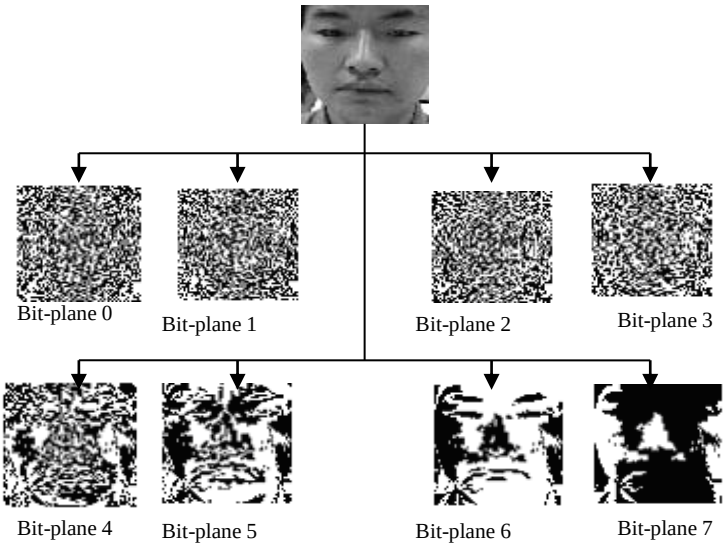


Figure 2.19: Bit-plane extraction from an original image (Ting *et al.*,2013)

2.10 Latin Squares

A symmetric-key Latin Square image with probabilistic encryption was presented by Wu *et al.* (2014) in his research. The name Latin Square was created by Leonhard Euler, a mathematician who used Latin letters as symbols. An $N \times N$ array filled with a set of N different symbol elements, where each symbol occurs precisely once in each row and column, is known as a Latin Square of order N. An indicator function f_L on tri-tuple (r, c, i as a Latin Square L of order N:

$$f_L(r,c,i) = \begin{cases} 1, & L(r,c)=S_i \\ 0, & otherwise \end{cases} \tag{2.8}$$

where r indicates the row index of an element in L with $r \in N = \{0, 1, \dots, N-1\}$; c denotes the column index of an element in L with $c \in N$; i indicates the indexs of a symbol element in L with $I \in N$; and S_i is the i-th symbol in the symbol set $S = \{S_0, S_1, \dots, S_{N-1}\}$.

As a result, if L is a Latin Square of order N,

1. For any fixed $c, i \in N$, we have

$$\sum_{r=0}^{N-1} f_L(r,c,i) = 1 \tag{2.9}$$

2. For any fixed $r, i \in N$, we have

$$\sum_{c=0}^{N-1} f_L(r,c,i) = 1 \tag{2.10}$$

which indicates that every symbol in L occurs precisely once in each row and column.

Wu et al. (2011) used a Latin Square Generator with the following algorithm:

Algorithm 1:

Input: Two length-N sequences which are Q_1 and Q_2

Output: L is a Latin Square of order N

Q_{seed} = SortMap(Q_1)

Q_{shift}= SortMap (Q_2)

for r=0:1: N-1 **do**

L(r,:) = Rowshift (Q_{seed}, Q_{shift}(r))

End for

It was a self-orthogonal Latin Squares (SOLS), which was proposed by Xu & Tian (2018), as an enhanced approach of standard Latin square. For picture permutation, it employs a 2D map created by SOLS. Algorithm 2 shows how an SOLS is created.

Algorithm 2:

Input: The default value of the Logistic map is Key_0, μ_0 is the system parameter of Logistic map, and *t* is a parameter satisfying $t \in F_N, t \notin \{0, 1\}$ and $2t \neq 1$.

Output: SOLS *L* of order *N*

Step 1: Construct a scrambled sequence, $x = (x_0, x_1, \dots, x_{N-1})$ via Logistic map with default key_0 and parameter μ_0.

Step 2: Create a scrambled sequence x as:

$$[lx, fx] = sort\ (x) \tag{2.11}$$

where $[,] = sort\ (\ \ )$ is the sequencing index function. fx is the new sequence after ascending to *x*, *lx* is the index value of *fx*. Denote *lx* as $lx = \{c_0, c_1, \dots, c_{N-1}\}$.

Step 3: Create a finite field F_N on $lx = \{c_0, c_1, \dots, c_{N-1}\}$, that is, redefine "+" and "x" on *lx* to meet the definition of finite field. Then construct SOLS L of order N as follows:

for i=0:1: N-1 **do**

for j=0:1:N-1 **do**

$$\boldsymbol{L(i,j) = t \times c_i + (l + t) \times c_j}$$

end for

end for

where 'x","+", and "-" denote the multiplication, addition and subtraction respectively in finite field F_N. *L(i,j)* is the element in the generated SOLS.

2.11 DNA Sequence

Wei et al. (2012) proposed DNA encoding and decoding for a digital colour picture. Red (R), Green (G), and Blue (B) are the three channels that make up a colour picture (Blue). A DNA sequence can be expressed for each pixel in any R, G, or B channel. Adenine, C (cytosine), G (guanine), and T (thymine) are the four nucleic acid bases found in a DNA sequence, with A and T , G and C complementary.

In binary format, the numbers 0 and 1 are complementary. As a result, the numbers 00 and 11 are complementary, as are the numbers 01 and 10. When the four bases A, C, G, and T are encoded into binary format of 00, 01, 10, and 11 as shown in Table 2.2 below, there are 24 different coding schemes.

Table 2.2: Operation for DNA sequences

Rule	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
A	00	00	01	01	10	10	11	11
T	11	11	10	10	01	01	00	00
G	01	10	00	11	00	11	01	10
C	10	01	11	00	11	00	10	01

As illustration, the binary coding is 10101101 if the first pixel value is 173, and according to Table 2.2's DNA encoding rule 1, it is encoded as [CCTG]. When we decode the aforementioned DNA sequence using DNA encoding Rule 1, we obtain the binary sequence 10101101 but if we decode the

same DNA sequence using DNA encoding Rule 2, then binary sequence 01011110 will be the output.

2.12 Skew Tent Map

Kadir *et al.* (2014) developed a colour image encryption approach that uses the skew tent map to construct the encryption confusion sequence. The following is a brief description of the skew tent map:

$$x_{i+1} = F_p(x_i) = \begin{cases} \frac{x_i}{p}, & x_i \in [0,p] \\ \frac{1-x_i}{1-p}, & x_i \in [p,1] \end{cases} \tag{2.12}$$

When $x_i \in [0,1]$ and the parameter $p \in [0,1]$, Because (2.12) has a positive Lyapunov exponent, the system is now in a chaotic state (Zhang & Liu, 2011).

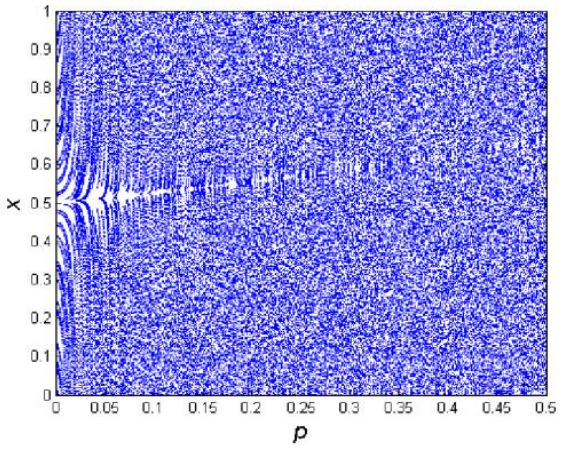


Figure 2.20. The distribution of x with p in 5000 iterations (Kadir *et al*., 2014)

The initial values of (x_0, p_0) can be served as keys. Figure 2.20 illustrates the x distribution with parameter p. Suppose the size of the plain RGB image is W x H, after (2.9) interated $n_t \in [200,1000]$ times, the sequence $X =$

$\{x_1, x_2, \ldots, x_{3WH}\}$ is generated if the iteration process continues for 3WH times. In order to confuse the pixels, the array of $L = \{1,2, \ldots, 3WH\}$ is generated to donate the serials numbers of the pixels sorted rows and red, green and blue in ascending order.

Then sequence L is permuted to get L' by equation below:

$$L'(i) = L\big((x_i \times 3WH) mod\ i\big), \tag{2.13}$$

$$x_1 \in X, i = 3WH, 3WH - 1, \ldots, 2,1$$

2.13 Chipertext feedback

By refining the classic permutation-diffusion structure, Zhang *et al.* (2014) suggested a simple yet safe chaotic cypher for grey images. Zhang *et al.* (2014) enhanced XOR methods in chaotic system (Chen *et al*., 2004). In several chaotic image encryption techniques, the Chen *et al.* (2004) system has been frequently employed. The system illustrates the model by:

$$\begin{cases} \dot{x} = a(y - x), \\ \dot{y} = (c - a)x - xz + cy, \\ \dot{z} = xy - bz, \end{cases} \tag{2.14}$$

where a, b and c are system parameters. The system is chaotic when a = 35, b =3 and $x \in [20,28.4]$.

The other chaotic system employed in chipertext feedback encryption algorithm is the Logistic map:

$$y_{n+1} = \mu \cdot y_n \cdot (1 - y_n) \tag{2.15}$$

where $y_n \in (0,1)$ and μ is the control parameter.

According to Andrecut (1998), when $\mu \in (3.5699456,4)$, The Logistic map is useful for pseudorandom number generation since the output sequence is ergodic in the unit interval (0,1).

2.14 Summary

Literature review on related information had been done throughout the research which is including the study of electromagnetic spectrum, radio telescopes, ALMA, Gaussian beam quasioptics, color image, grayscale image, Bayer image, bit planes, DNA sequence, Latin squares, skew tent map, and Chipertext feedback. Finally, all related information studied are mainly for the purpose of telescope analysis and novel encryption methodologies development which will be discussed in next chapter.

CHAPTER THREE

METHODOLOGY

3.1 Background

ALMA, or the Atacama Large Millimeter/Submillimeter Array, is the world's famous ground-based astronomical observatory. It is situated at a height of 5000 metres in Chile's Atacama Desert. ALMA is a high-precision radio interferometer made up of 66 antennas. Fifty 12-meter antennas for high-resolution, high-sensitivity imaging, twelve 7-meter antennas, and four 12-meter total power antennas are among the 66 antennas that make up the Atacama Compact Array, which improves wide-field imaging (Wootten, 2008). ALMA is run by the European Organization for Astronomical Research in the Southern Hemisphere (ESO), the National Radio Astronomy Observatory (NRAO), and the National Astronomical Observatory of Japan in a global multinational collaboration (NAOJ). Therefore, basic configurations of radio telescopes are explained in this chapter.

In this emerging era, digital images especially in radio astronomical images play a vital role in many applications. A digital image contains a lot of information that many are used to carry sensitive meaning. The confidentiality of this information is not just to be maintained in the storage, but also during the transmission over a communication network. Any information is considered

as secured when its confidentiality, integrity, and availability are retained (El-Samie *et al.,* 2014).

3.2. Radio Telescope

Radio telescopes are commonly employed in ground-based radio astronomy to study naturally occurring signal emission from celestial objects such as stars and planets (Yeap *et al*., 2013; Phillips and Keene, 1992; Cheng *et al.*, 1994; Wotten, 2008; Yeap *et al*., 2011). As depicted in Figure 3.1, a typical radio telescope consists of four primary components: the main reflector, sub reflector, elevation wheel, and azimuth bearing. The performance of the telescope can be improved by using a reflector with a big aperture to attain great accuracy and sensitivity (Chen *et al*., 2016).

Parabolic reflector antennas are employed in radio telescopes to achieve huge collecting areas and great angular resolution across a wide frequency range. The reflector antennas come in a variety of geometrical forms. The Cassegrain antenna is one of the most often utilised layouts. The Atacama Large Millimeter/Submillimeter Array (ALMA) telescope (Gonzalez & Woods., 2017; Tham *et al*., 2007; Candotti *et al*., 2007) and the Crawford Hill telescope (Gonzalez & Woods., 2017; Tham *et al*., 2007; Candotti *et al*., 2007) are examples of two radio telescopes (Rusch, 1992; Courtney-Pratt et al., 1963; Milligan, 2005). A Cassegrain antenna has main and secondary reflectors, as illustrated in Figure 3.1. The primary reflector has a bigger size than the secondary reflector. The secondary reflector must be hyperboloid in shape and situated below the first reflector's focal point.

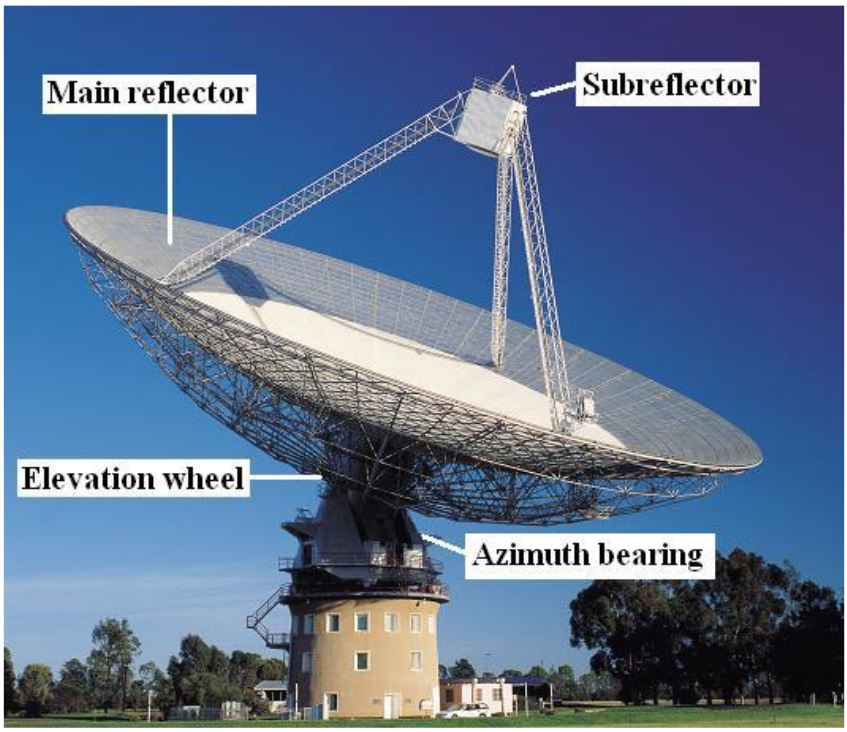


Figure 3.1: Typical radio telescope (photograph by CSIRO, distributed under a CC-BY 3.0 license)

The Atacama Large Millimetre Array is the principal submillimetre instrument examined in this research (ALMA). ALMA is one of the world's biggest interferometric array dedicated entirely to the ground-based submillimetre astronomy. The European Southern Observatory (ESO), the National Radio Astronomy Observatory (NRAO), the National Research Council of Canada, and the National Astronomical Observatory of Japan (NAOJ) collaborated on the array. Up to 66 12-metre on-axis Cassegrain antennas will be used in the array. Three firms have been hired to create these antennas: the AEC Consortium, which works under the ESO, Vertex RSI, which works under the NRAO, and Mitsubishi Electrical Company, which works under the NAOJ. Each firm has developed a prototype 12 metre antenna that

has been thoroughly tested to guarantee its compliance with the ALMA requirements. The array which is placed in Chile's Atacama Desert, precisely in the Chajnantor Plain of the Chilean Andes in the District of San Pedro de Atacama (23°01'9.42"S 67°45'11.44"W), at a height of 5000 metres above sea level. Two different array systems are formed using these antennas. The primary 12 metre array is made up of fifty 12 metre antennas that will be converted into different arrays using specialised transporters. This area's smallest baseline size is 160 x 250 metres, and the greatest configuration baseline spacing between antennas is about 15 kilometres. The Atacama Compact Array (ACA), on the other hand, is made up of four 12 metre antennas and twelve 7 metre antennae. In Table 3.1, the specifications of both of these arrays are presented.

3.2.1 Design of Telescope

The propagation of quasioptics is used to develop the optical system. The beam propagation across the optical system is calculated using multimode Gaussian optics. This approach is also applicable to systems with millimetre and submillimetre wavelengths. The distribution of electric field over the antenna aperture must be reasonably uniform and with sufficient edge illumination to ensure high aperture efficiency with little distortion. The receiving and transmitting antenna modes are the two types of antenna modes. Figure 3.2 illustrates a common telescope antenna configuration.

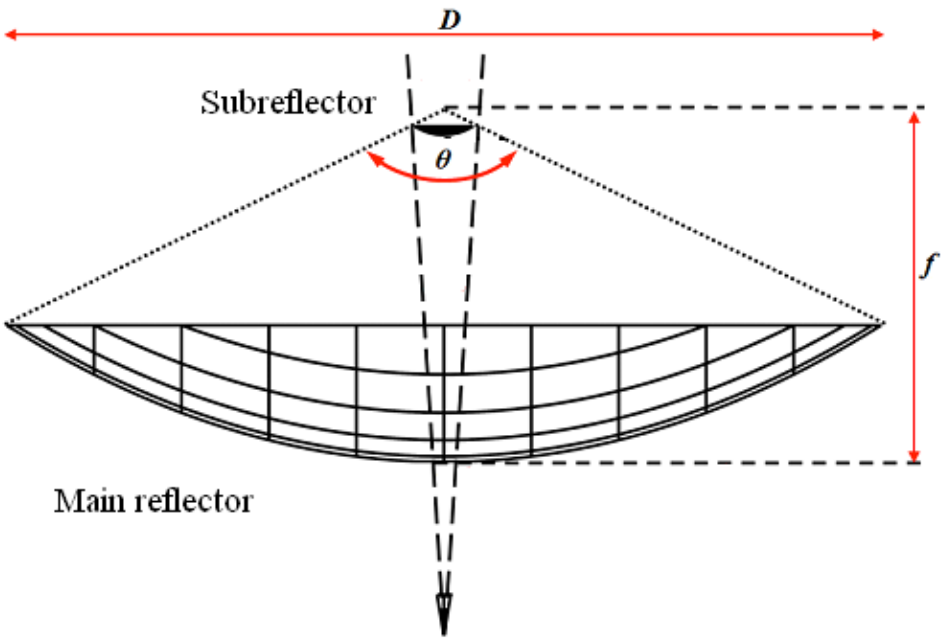


Figure 3.2: Common telescope antenna configuration

In the receiving mode, the signal is a point source that generates a plane wave in the antenna's aperture plane. As a result, it was studied in terms of coupling to a quasioptical, often Gaussian Beam. Gaussian field truncation occurs at the secondary reflectors, where the coupling efficiency is determined. The fields obtained at the secondary reflector must be symmetrically distorted to achieve high efficiency.

When the field is configured off-axis, blockage can be minimised. A balance between the taper and spillover efficiencies is required to achieve optimal aperture efficiency. The aperture efficiency, ε_a can be expressed as the product of spillover efficiency, ε_s and taper effiency, ε_t.

$$\varepsilon_a = \varepsilon_t \times \varepsilon_s \tag{3.1}$$

Goldsmith (2008) provides the equation for taper and spillover efficiencies:

$$\varepsilon_t = \frac{17.3762\left[exp\left(-0.1151 f_b^2 T_{e(dB)}\right) - exp\left(-0.1151 T_{e(dB)}\right)\right]^2}{T_{e(dB)}\left[1 - exp\left(-0.2303 T_{e(dB)}\right)\right]} \quad (3.2)$$

$$\varepsilon_s = 1 - exp\left(-0.2303 T_{e(dB)}\right) \quad (3.3)$$

The f_b is the fractional blockage which can be expressed in terms of the fraction of the radius of the main reflector, $r_a$to the radius of secondary reflector, r_s and $T_{e(dB)}$ is the edge taper expressed in the decibels (dB). The edge taper $T_e$is the relatively power density at a radius r across the profile of a Gaussian beam. It is given by $T_e = \frac{P(r)}{P(0)}$ and $T_{e(dB)}$ can be expressed as

$$T_{e(dB)} = -10\log\left(\frac{P(r)}{P(0)}\right) \quad (3.4)$$

The primary reflector radius for the ALMA is 6000 mm, whereas the secondary reflector radius is 375 mm. By using this radius, the f_b can be identified followed by $T_{e(dB)}$. On Figure 3.3, the relationship between spillover, taper, and aperture efficiency is further discussed. The efficiency of tapering is diminishing, while the efficiency of spillover is increasing. The optimum aperture efficiency can be obtained at the intersection point between the spillover efficiency, ε_s and taper efficiency, ε_t. The maximum aperture efficiency is measured as 81.45% when edge taper, $T_{e(dB)}$ is 10.91dB.

Ideally, when the fractional blockage, f_b is 0.0, the optimal aperture efficiency is reached. The optical system configuration in Band 1 is illustrated in Figure 3.3 and is taken into account for optimization. The distances between

each element are critical for achieving optimal performance on the optical system. To maintain beam propagation continuity, the incident beam's waist must be located in the same location as the Cassegrain focus. With respect to the Cassegrain focus, the lens is positioned so that the focus is kept near to the cryostat window. Thus, the optical system's edge taper, $T_{e(dB)}$ and the distance between the lens and the beam waist, d_3, The optical system's characteristics, such as the distance between the horn's aperture and the lens, d1 and the lens's equivalent focal length, f_1 , are based on the mid-frequency of Band 1, which is 38 GHz. These optimization parameters are then utilised to get the desired T_e value at 38 GHz. Finally, the aperture efficiency, Te, is determined, which corresponds to the edge taper.

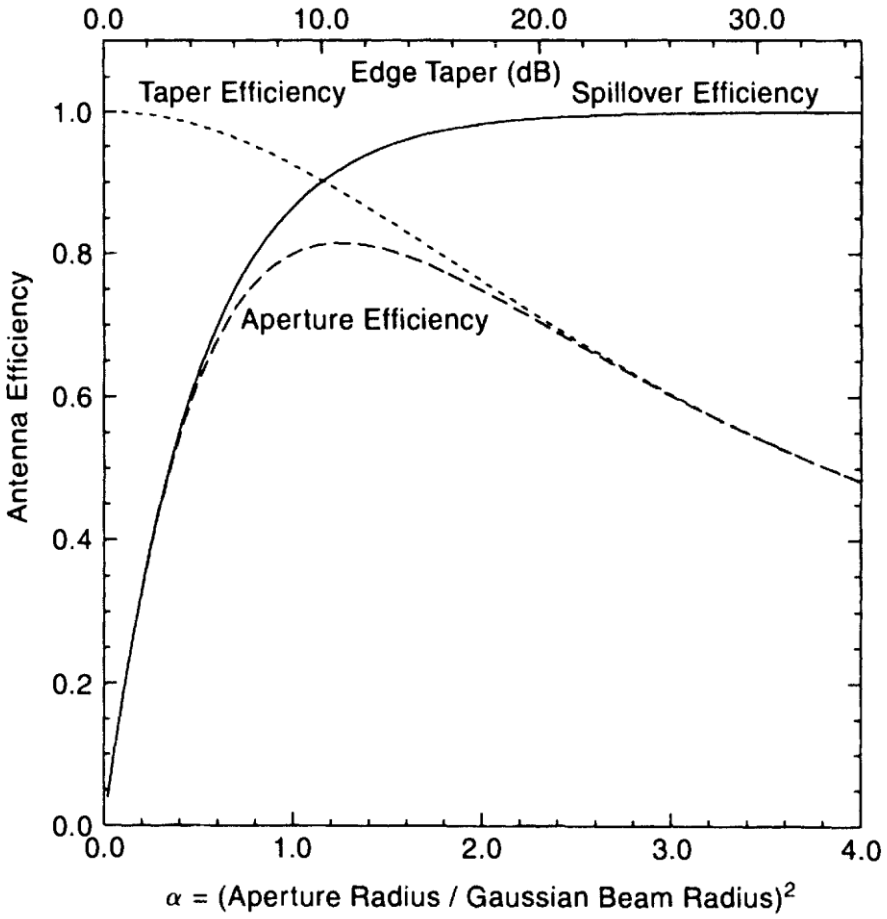


Figure 3.3: The aperture efficiency for unblocked aperture (Goldsmith, 1998)

3.3 Development of Encryption Methods for Radio Astronomical Images

When it comes to the sensitivity of pictures, image security is extremely important during data transfer between sender and recipient. A large number of digital images are broadcast back to the ground telescope receiver due to the rapid advancement of space technology. As a result, a trustworthy image security technique is required to ensure that data is safeguarded during transmission. The RGB colour image security technique is discussed in this study using the combined spatial and frequency domains of the images. Before a colour RGB telescope image is processed in the spatial domain, it is subjected to the Fourier transform.

The spatial domain process, which included components R, G, and B, was extracted before they were encrypted using two stages of scrambling techniques. In comparison to other recently created algorithms, the findings revealed that this method performs better.

In this new era, digital images are used in a variety of applications. A digital image carries a lot of information, and many people utilise it to convey sensitive information. This information's secrecy must be preserved not just during storage, but also throughout transmission via a communication network. When the confidentiality, integrity, and availability of any information are maintained, it is deemed secured (El-Samie *et al.*, 2014). It must also be able to withstand any attacks that are made against it as a guarded information. Number of Pixel Changing Rate (NCPR) and Unified Average Changing Intensity

(UACI) are two measures often used in image encryption to verify the reliability of encryption algorithms in order to avoid various assaults (UACI). A strong NCPR (>90%) and a decent UACI (33%), respectively, imply that the picture can resist many assaults (Gao et al., 2019). The assessment of the degree of resemblance between the original and the encrypted image is another significant key in image encryption. To compare the squared error between the original image and the encrypted image, the mean square error (MSE) and peak-signal-to-noise ratio (PSNR) can be used. A greater PSNR and a lower MSE value suggest that the image is of higher quality (Gu *et al*., 2016). In other words, a low PSNR index shows that the two pictures being compared are not identical (Gu *et al*., 2016).

Many encryption algorithms based on Latin squares (Xu & Tian, 2018), (Wu *et al*., 2014), skew tent map (Kadir *et al.,* 2014), DNA sequence (Wei *et al.*, 2012; Gehani *et al*., 2003; Ning, 2009), and ciphertext feedback have been developed in recent years (Zhang *et al.*, 2014). Some of these approaches are secure enough to be used. Although Latin squares are said to have some favourable properties for image encryption, the technique's appropriateness for image encryption is under doubt (Wu *et al*., 2014). Also, while the DNA cryptography techniques in (Gehani *et al*., 2003) have the virtue of storing a large one-time pad, the experiment requires a well-equipped lab and a significant cost (Gehani *et al*., 2003). Although Ning (2009) proposes a DNA cryptography approach that has a stronger encryption result than Gehani *et al.* (2003), the security of the technology is unknown.

This work focuses on creating encrypted telescope pictures using a revolutionary RGB (Red, Green, and Blue) colour image security technique. In the frequency domain, the Fourier transform (FT) is utilised, whereas in the spatial domain, bit levels decomposition is used. Two stages of scrambling are used to create the encrypted pictures. The results of this study's experiments suggest that the proposed algorithm performs better than other previously created algorithms.

3.3.1 Radio Telescope Images

The Atacama Large Millimeter/submillimeter Array (ALMA) is a ground-based radio telescope that receives signal emission from astronomical objects, examples are stars, pulsars, and active galaxy (Yeap *et al.*, 2017). Inside the receiver, the arriving waves are transformed to electrical impulses, which are then processed to show the spatial information conveyed by the signal (Yeap *et al.*, 2016). The original RGB radio telescope photos are shown in Figure 3.4.

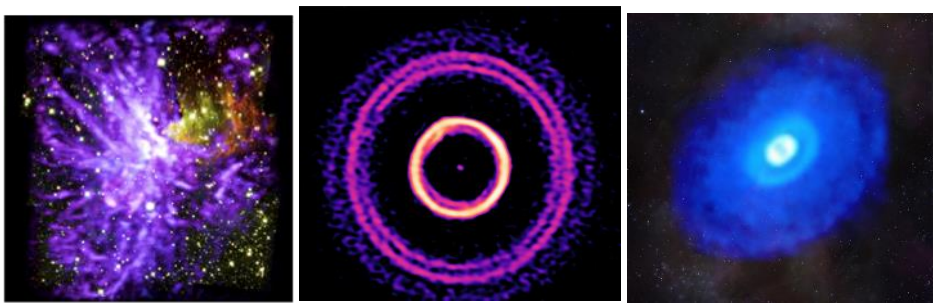


Figure 3.4: Examples of RGB Radio Telescope Images (Credit: ALMA (ESO/NAOJ/NRAO), Y. Cheng et al.; NRAO/AUI/NSF, S. Dagnello; NASA/ESA Hubble)

Red (R), Green (G), and Blue (B) are the three components of a colour RGB picture (Blue). The number of pixels in the component R, G, and B stays the equal number as in the colour RGB image. A colour RGB Radio Telescope colour of 1024 x 1024 pixels is shown in Figure 3.4. Figure 3.5 depicts the R, G, and B components. Pixels with intensities ranging from 0 to 255 and varied saturation levels make up each component (Bong *et al.*, 2009). The value distribution of pixels is represented by the histogram distribution of a colour RGB picture. The histogram distribution pattern is preserved even after the pixels of a colour RGB picture are jumbled. As a result, it is not a safe technique

for picture transmission security. As a result, a qualified safe technique is required to ensure that their histogram distribution is evenly distributed.

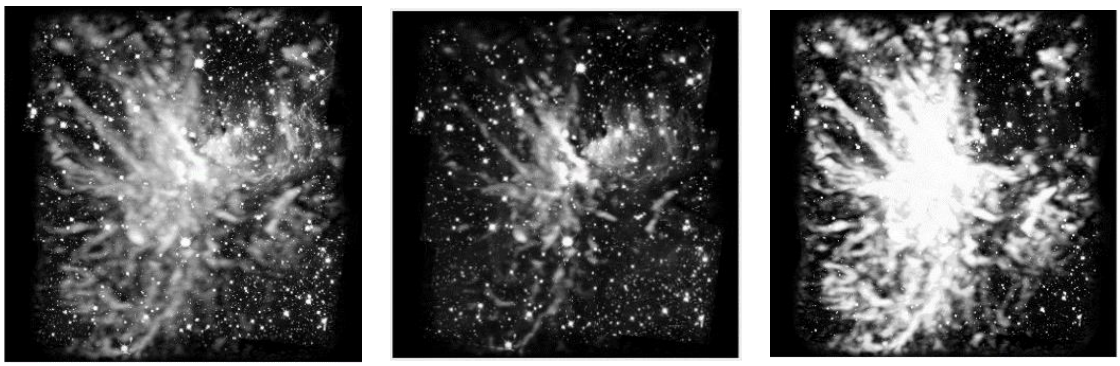


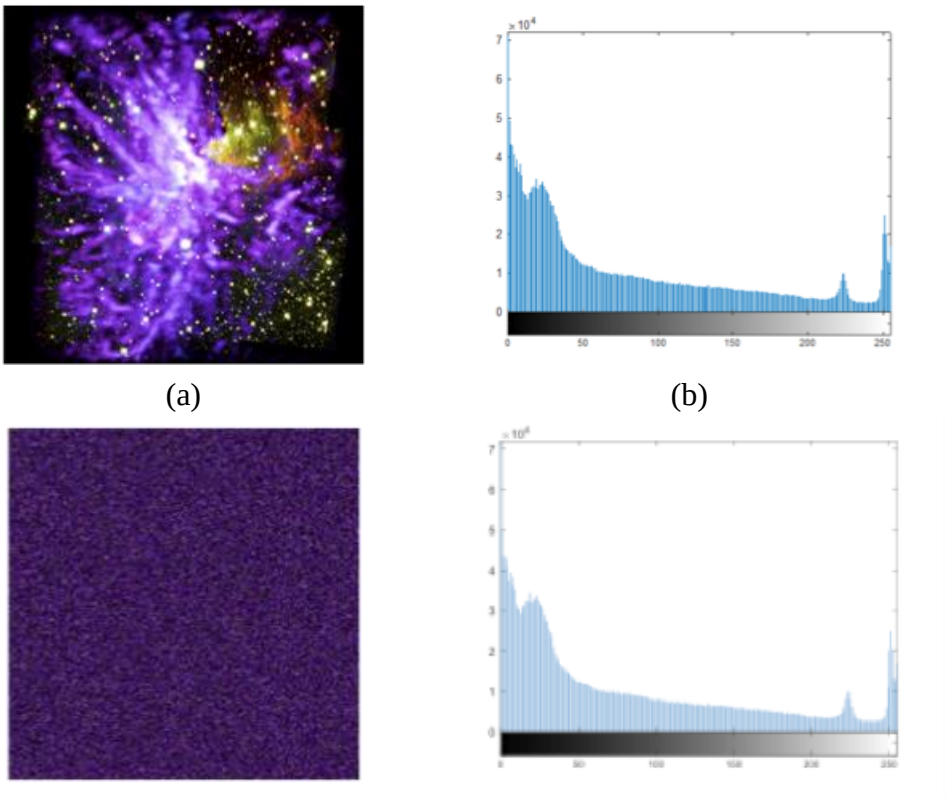
Figure 3.5: Red, Green and Blue Component of Figure 3.4(a)

3.3.2 Bit Planes

The method of extracting eight bit-planes from any grayscale image is known as digital image decomposition. As shown in (3.5), a digital image is made up of $M \times N$ pixels. Each pixel value of any grayscale image is divided into four Least Significant Bits (LSB) and four Most Significant Bits (MSB) (Liu *et al.*, 2019). The i-th bit-plane contains all of the *i*-th bits of each pixel's binary representation (David *et al.*, 2009).

$$f(x,y) = \begin{bmatrix} f(0,0) & \cdots & f(0,N-1) \\ \vdots & \ddots & \vdots \\ f(M-1,0) & \cdots & f(M-1,N-1) \end{bmatrix} \tag{3.5}$$

$$f_{bit-plane\ i} = R\left[\frac{1}{2} floor(\frac{1}{2^i}[f(x,y)]\right] \tag{3.6}$$



(a) (b)

(c) (d)

Figure 3.6: (a) Radio Astronomical Image, (b) Histogram of (a), (c) Scramble image from Original Radio Astronomical Image in (a), (d) Histogram of (c)

The histogram distribution of original and scramble image are shown in Figure 3.6. From both histogram distributions, it can be seen that scrambling the value of pixels will not change the distribution pattern of color image.

3.3.3 Mathematical Derivation of Bit Plane Extraction

Any digital image can be used to extract 8 bit planes using the bit plane extraction method. In mathematical form, the extraction procedure may be derived. With $M \times N$ pixels, it is defined in (3.12) below.

$$f(x,y) = \begin{bmatrix} f(0,0) & \dots & f(0,N-1) \\ \vdots & \ddots & \vdots \\ f(M-1,0) & \dots & f(M-1,N-1) \end{bmatrix} \quad (3.12)$$

$$f_{bit-plane\ i} = R\left[\frac{1}{2} floor\left(\frac{1}{2^i}[f(x,y)]\right)\right] \quad (3.13)$$

3.3.4. Fourier Transform

The Fourier Transfrom method decomposes a picture into a collection of constituent signals. It has the advantage of being simple to adopt and Chapeau-Blondeau & Belin (2020) defines the discrete Fourier transform (DFT) of an image f(m,n) of dimension M x N:

$$F(u,v) \quad = \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} f(m,n) e^{-j2\pi(\frac{u.m}{M}+\frac{v.n}{N})} \quad (3.14)$$

where u and v denote the spatial frequencies for a position m and n.

In general, complex images are formed after DFT (Olbrys & Mursztyn, 2019) as (3.15) and (3.16).

$$\mathrm{M(u,v)} = |F(u,v)| = \sqrt{Re(u,v)^2 + Im(u,v)} \quad (3.15)$$

$$\mathrm{P(u,v)} = \arg(\mathrm{F(u,v)}) = \tan^{-1}(\frac{Im(u,v)}{Re(u,v)}) \quad (3.16)$$

where I_m and R_e represent respectively the imaginary and the real part of the FT of the image *f*.

Because of the Hermitian symmetry features of the fast Fourier transform (FFT), the modules in the first and second quadrants are identical to the coefficient in the third and fourth quadrants, respectively.

3.3.5 Development of Bit-level Scrambling Encryption for Radio Telescope Imageries

Image security is a major concern when sending images over the internet, especially when sensitive data is involved. In order to address this problem, picture encryption is one of the most effective methods for ensuring the uniqueness and security of the image being transferred. As a result, we provide the bit-level scrambling technique for radio telescope imageries utilising the Random Generation Number approach in our suggested methodology. There are two types of scrambling algorithms named Level I scrambling and Level II scrambling.

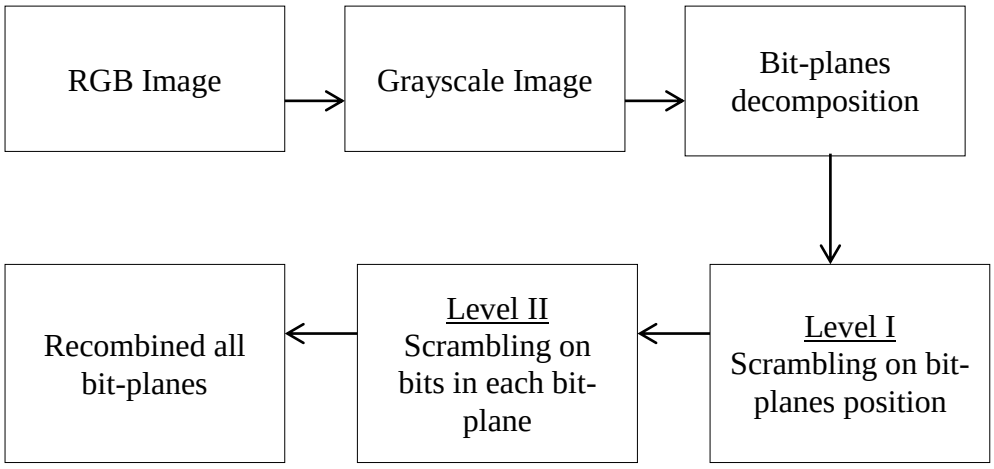


Figure 3.7: Block diagrams of image scrambling

Level I scrambling is used to scramble the location between bit-plane layers, whereas the Level II scrambling algorithm scrambles bits in each bit-plane arbitrarily. We show that the Level II scrambling algorithm is substantially more dependable in scrambling the radio telescope pictures utilised in this work, as measured by stability and scrambling degree and scrambling degree of the image is measured and used to evaluate the study's results.

3.3.6 Bit-levels Encryption for RGB Telescope Images

We offer an encryption algorithm with a twofold level of scrambling in our proposed algorithm. The suggested scrambling encryption algorithm's flow is depicted in Figure 3.8.

Each component will be broken down into eight bit-plane levels, then the location of all bit-planes will be scrambled using Level I scrambling to ensure that the values of the pixels in each bit-plane will then be arbitrarily scrambled. They will be reorganised with random positions to the bit-planes position, followed by Level II scrambling. After that, these three components are going through the recombined process to create a new RGB picture. Figure 3.9 shows the outputs of the eight layers bit-planes decomposition.

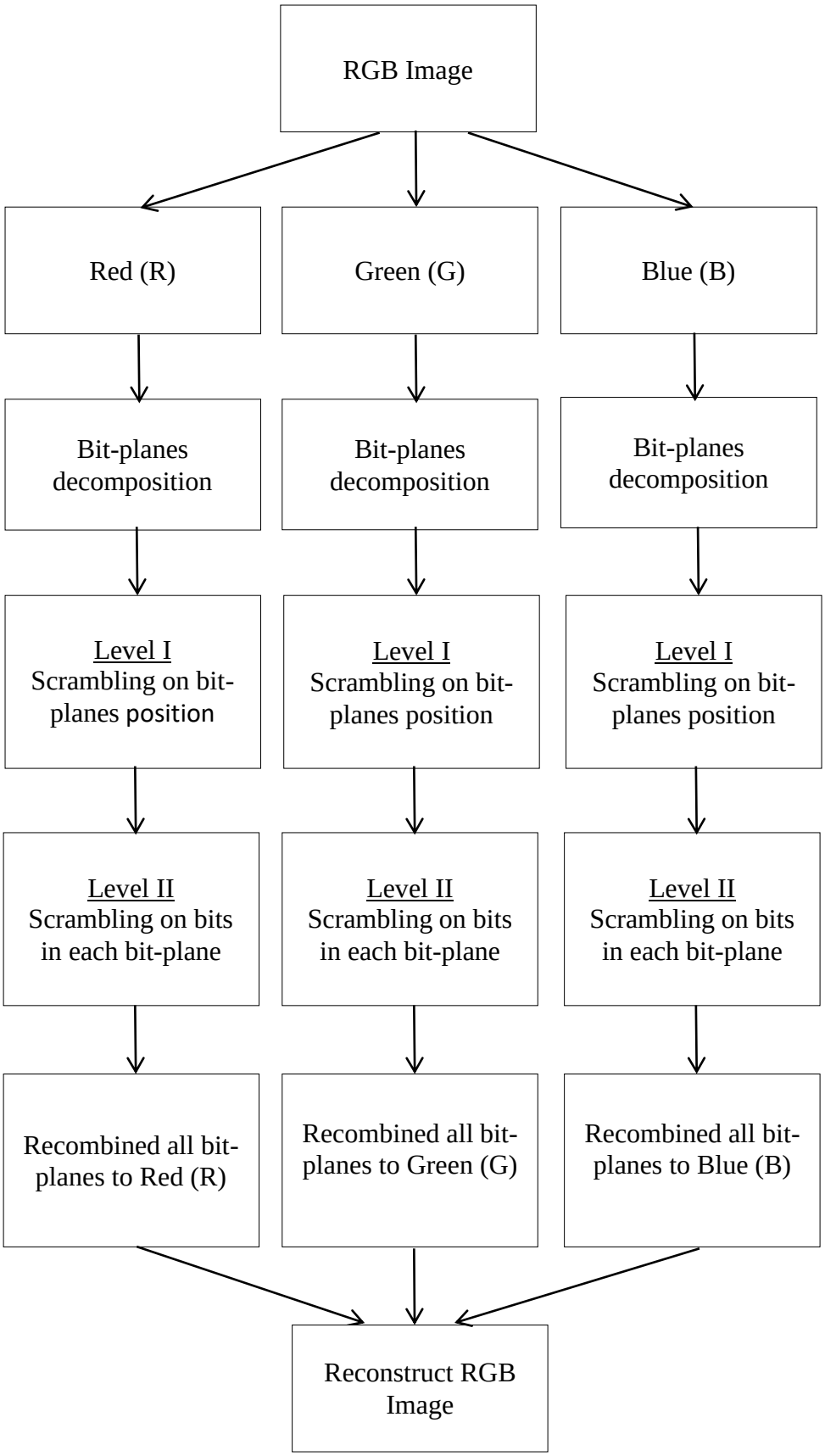
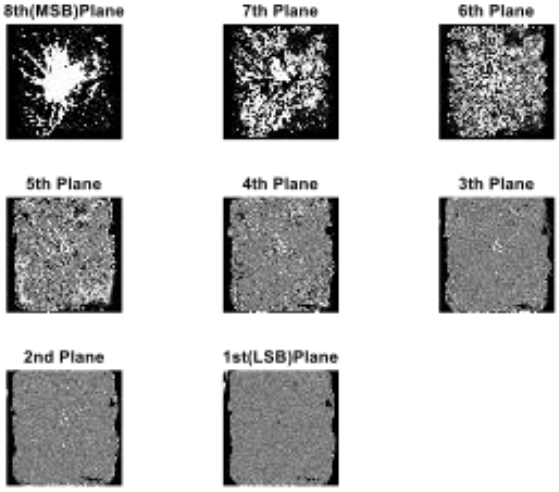
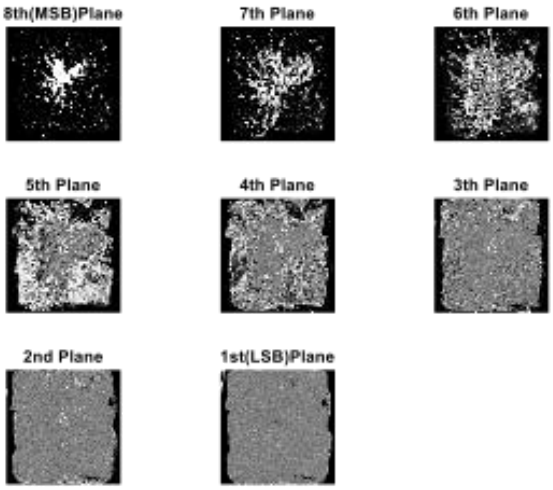


Figure 3.8: Flowchart of Proposed Algorithm II

(a)



(b)



(c)

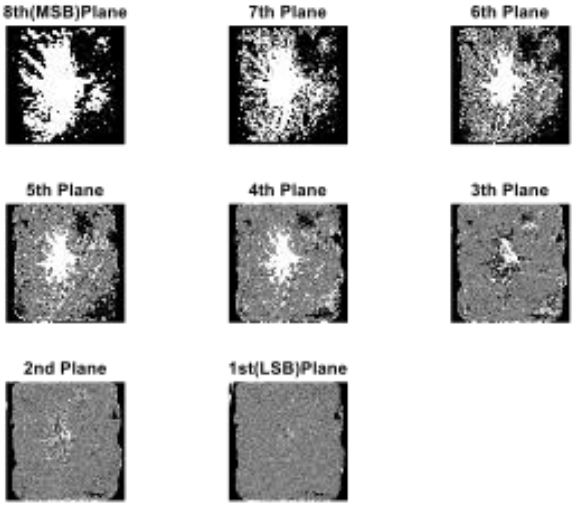


Figure 3.9: (a) Bit-planes of Red component (b) Bit-planes of Green component (c) Bit-planes of Blue component

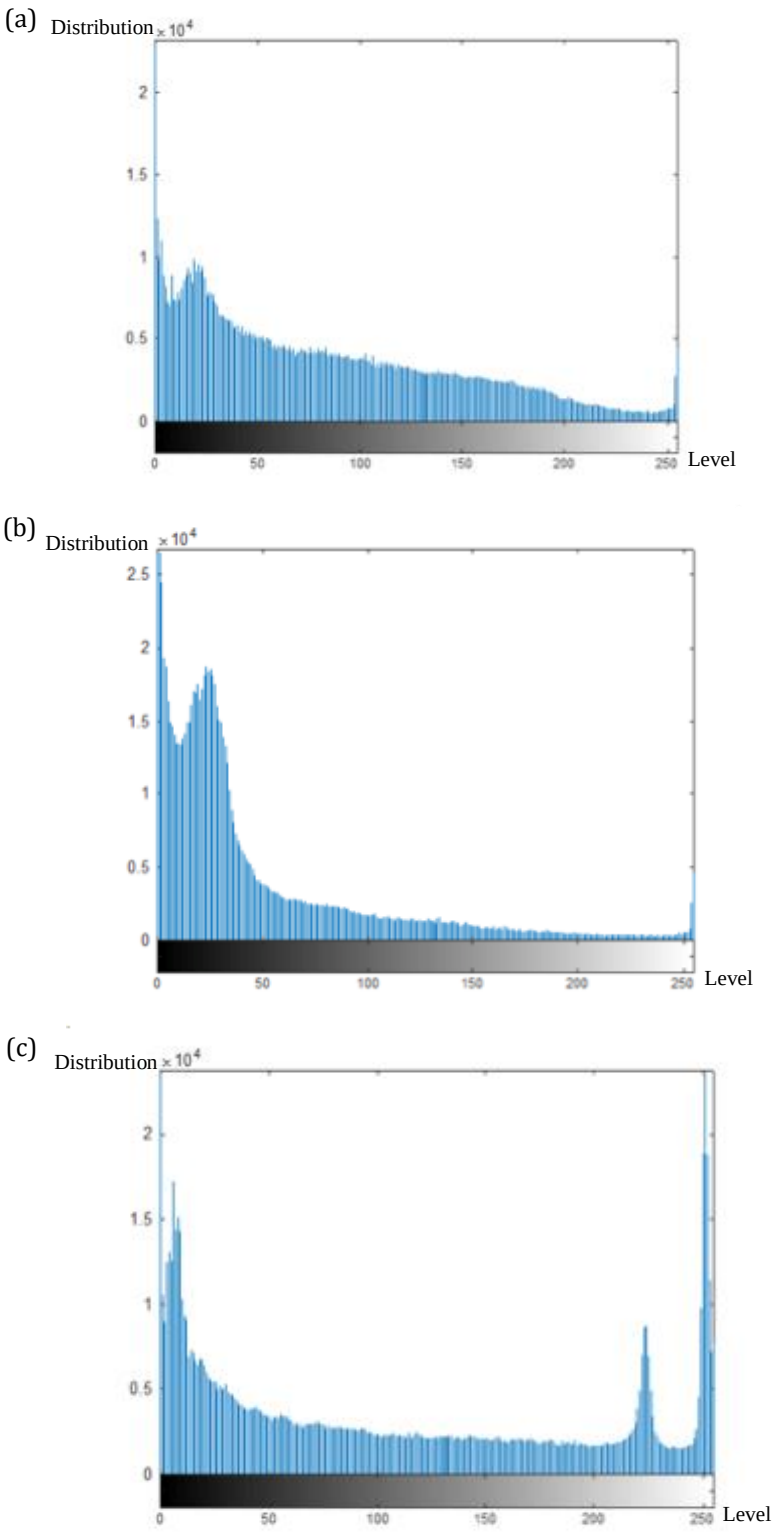


Figure 3.10: (a) Histogram of R component (b) Histogram of G component (c) Histogram of B component

3.3.7 Design of Encryption Algorithm in Combined Spatial and Frequency Domains for Telescope Grayscale and Bayer Images

Images in the RGB colour scheme are made up of three separate images, generally referred to as Red, Green, and Blue. These RGB photos may be transformed to Grayscale images using the approach in Figure 3.11. Any RGB colour image may be converted to a grayscale image using (3.17).

$$Grayscale = \frac{(R+G+B)}{3} \tag{3.17}$$

where R is value in Red component, G is value in Green component and B is value in Blue component.

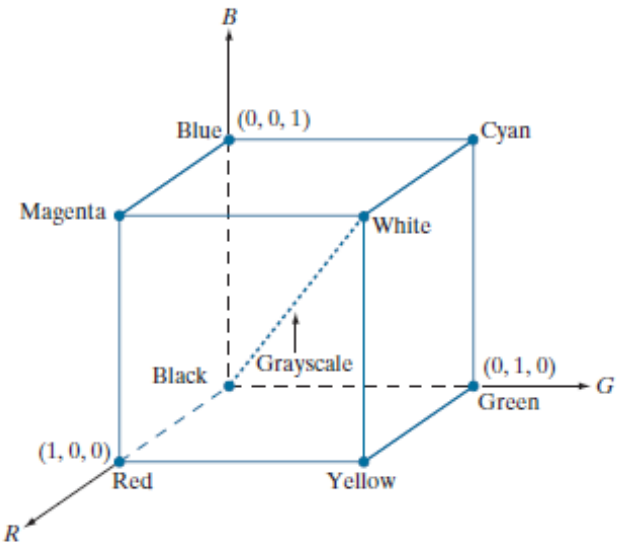


Figure 3.11: RGB Color Model (Gonzalez & Woods, 2018)

R, G, and B are the three main components of a digital colour image, where R stands for red, G for green, and B for blue. A Bayer picture is a colour filtered array with three colour components filtered and organised on a grid of photo sensors. The pattern of a Bayer picture is made up of 50% green, 25%

red, and 25% blue components from the original RGB image. The RGB picture and its Bayer counterpart are shown in Figure 3.12.

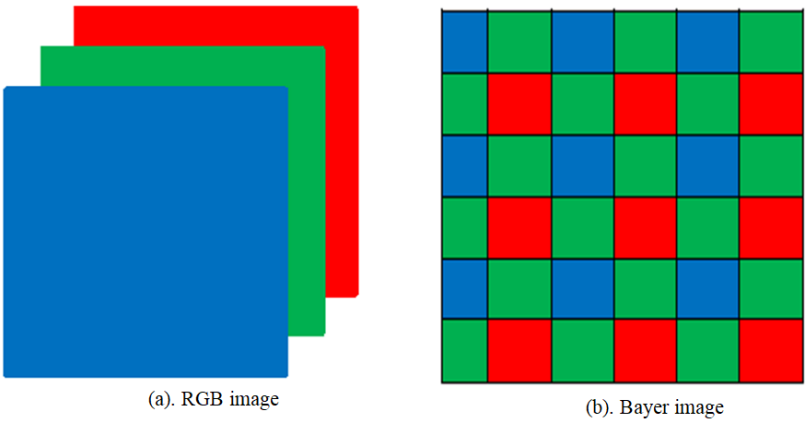


Figure. 3.12: RGB and corresponding Bayer image(Gonzalez & Woods, 2018)

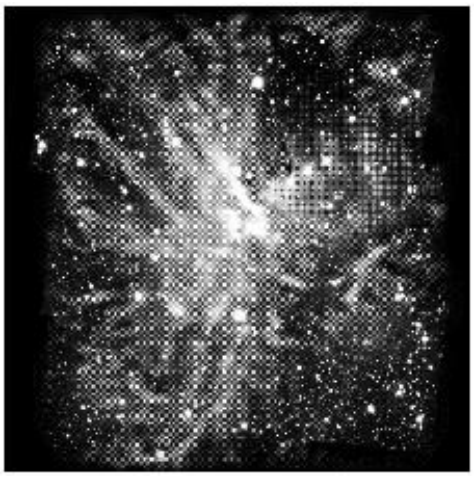


Figure 3.13: Bayer Image

Grayscale and Bayer images will benefit from a combined spatial and frequency domains method. Bit levels decomposition was used in the frequency domain, whereas FT was used in the spatial domain. Figure 3.13 depicts the conversion of an RGB image to a grayscale or Bayer image before to FT. Following that, the grayscale or Bayer image is split into eight levels of bit-planes, numbered from 0 to 7. The algorithm is scrambled twice. The bit-plane is where the first level scrambling takes place. The value of the pixels in each

bit-plane is then arbitrarily jumbled and restructured with random positions to bit-planes. Eight bit-planes reconstruct a new grayscale image.

Scrambling is a technique for swapping pixel positions without affecting their values. On the basis of a random number generation process, it can encrypt and decode grayscale images of any sizes.

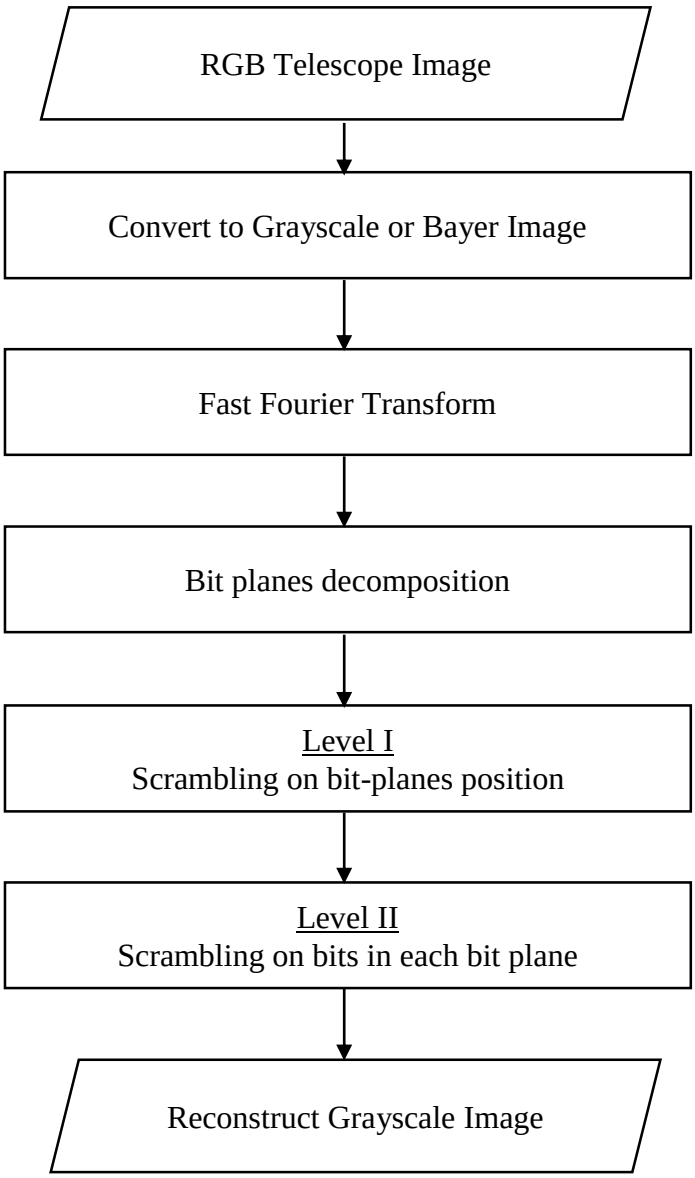


Figure 3.14: Proposed System

3.3.8 Combined Spatial and Frequency Domains in Algorithm of RGB Color Image Security for Telescope Images

A combined spatial and frequency domains technique is proposed in this study. FT is applied in stage of frequency domain, whereas in the stage of spatial domain, bit levels decomposition is used. Figure 3.15 demonstrates how to apply FT to an RGB image before decomposing it into R, G, and B components. Each component will be broken down into eight levels of bit-planes, numbered from 0 to 7. A two-level scrambling method is used. The bit-plane position is used for the first level of scrambling. The value of the pixels in each bit-plane is then randomly jumbled and reorganised with random position to bit-planes position, followed by second level scrambling. R, G, and B components combine to create a new RGB image.

Scrambling is a technique for shifting the location of pixels without affecting their values. It may be used to encrypt and decode grayscale images of any sizes using the random number generation process in the following steps:

Encryption:

Step 1: Image size has been defined as x(i), y(j)

Step 2: The pixel is started with i, j=1, 2,… q

Step 3: Non-repetitive random number is assigned for row (m) and for column (n), where m, n ≤ q

Step 4: New pixel position is generated by replacing i, j with m, n

Step 5: The scrambling process is repeated and record the sequence is recorded

Decryption:

Step 1: Apply the reverse sequence for the encrypted image

Step 2: Repeat the process and get the original image

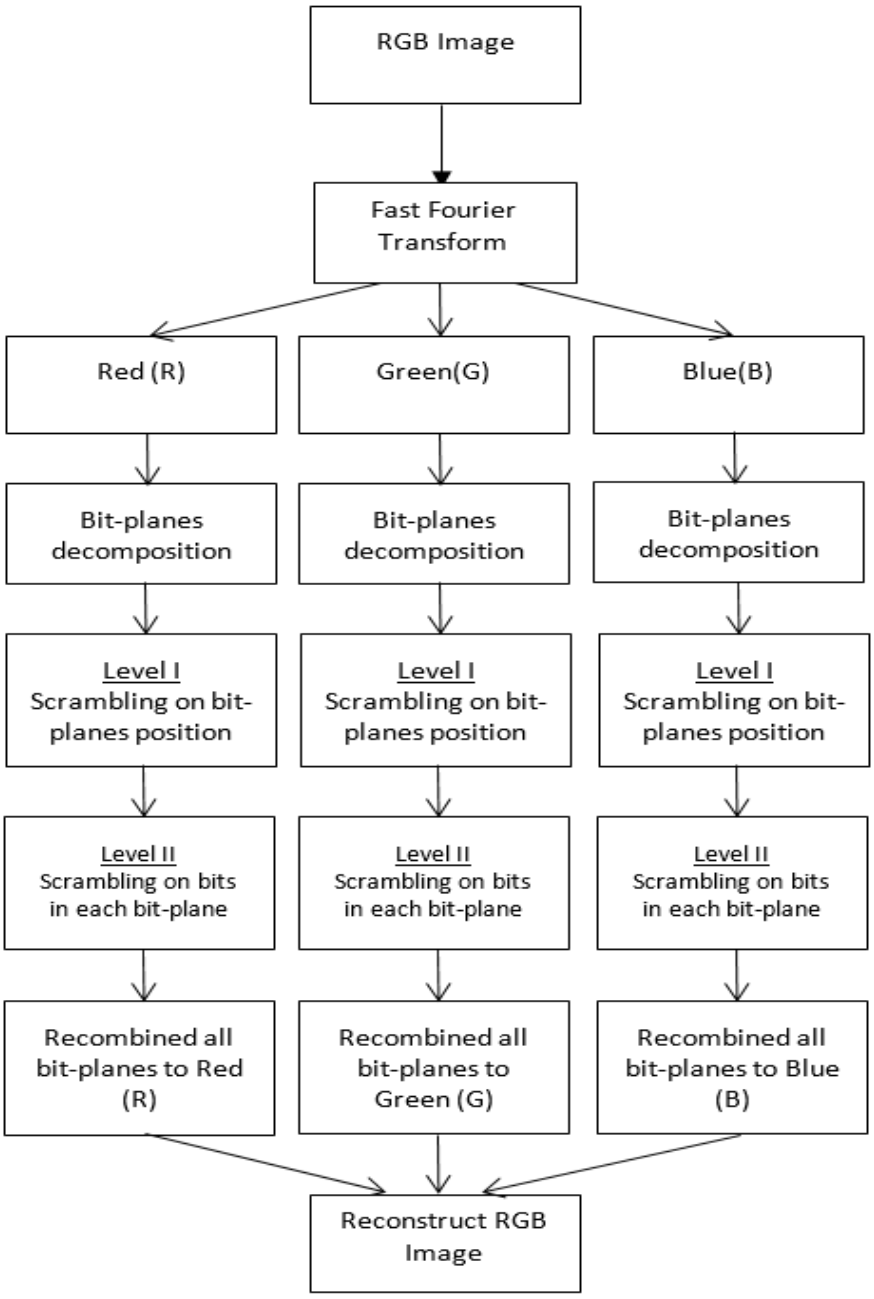


Figure 3.15: Proposed Algorithm

3.4 Summary

This chapter has discussed about the design of radio telescopes with various important parameters which are significant elements in the analysis stages. Besides that, four different design of algorithms had been developed to be evaluated on their outcomes performance of digital image encryption method. The outcomes of the analysis in radio telescope, and performance of the digital image encryption such as encryption scrambling degree, gap between the highest and lowest scrambling degrees, histogram, Number of Pixel Changing Rate, Unified Average Changing Intensity, Peak Signal-to-Noise Ratio, information entropy, and Structural Similarity Index are discussed in the next chapter.

CHAPTER FOUR

RESULTS AND DISCUSSION

4.1 Background

The performance evaluation takes place after the design or proposed encryption algorithms as mentioned in Chapter Four. The evaluation processes carried out by scrambling degree, gap between highest and lowest scrambling degree, histogram, NPCR, UACI, PSNR, information entropy, and SSIM. As a secured information, it must also be able to resist any kind of attacks attempted on it. In image encryption, two parameters that are mostly used to test the reliability of the encryption techniques to avoid different attacks are, NPCR (Number of Pixel Changing Rate) and UACI (Unified Average Changing Intensity). A high NPCR (>90%) and a good UACI (≈33%) indicate that the image is able to withstand different attacks. Another important key in image encryption is the measurement of the degree of similarity between the original and the encrypted image. This measurement can be done using the mean square error (MSE) and peak-signal-to-noise ratio (PSNR) to compare the squared error between the original image and the encrypted image. A higher PSNR value and a lower MSE value indicate a better quality of the image. Thus, lower value of PSNR index shows no similarity between the two measured images.

4.2 Parabolic Antenna for Radio Telescope

Signals from distant astronomical objects that reach the earth's surface are generally quite weak. As a result, the dimension of a radio telescope must be large in order to receive more signal energy. A parabolic main reflector is used in most radio telescopes. The huge parabolic reflector ensures a large signal gathering aperture and great angular resolution across a broad frequency range for the telescope. The main reflector concentrates the incoming signal onto a feed horn behind or below the parabolic primary reflector. The incoming signal is then connected to a detector in the waveguide, which is subsequently processed to show the spatial data. (Yeap *et al*., 2013).

4.2.1 Performance Analysis of a Cassegrain antenna with different primary reflector focal-length-to-diameter *f*/D ratio

The aperture efficiency is numerically studied, and the design parameters for the Cassegrain antenna configuration's optimal performance are assessed. The essential parameters utilised in the construction of the Cassegrain antenna for the ALMA telescope are listed in Table 4.1 below. The focal length *f* to diameter D ratio of the primary reflector from 0.1 to 1.0 to investigate how it affects the performance of the antenna.

Table 4.1 Parameters for the reflector antennas.

Description	Data
Primary reflector diameter, D	12 m
Distance between foci relative to primary reflector focal length	1.287 m
Secondary reflector eccentricity, e	1.105

Using the GRASP physical optics compiler, the spillover efficiency, ε_s was calculated and the antenna radiation patterns were shown. The following equation is used to calculate the edge taper, T_e, aperture efficiency, ε_a and taper efficiency ε_t (Yeap et al., 2016; Goldsmith, 1998):

$$T_e = \frac{ln(1-\varepsilon_s)}{-0.2303} \tag{4.1}$$

$$\varepsilon_a = \frac{-4\left\{exp\left[0.5\left(\frac{r_s}{r_a}\right)^2 ln(1-\varepsilon_s)\right] - exp[0.5ln(1-\varepsilon_s)]\right\}^2}{ln(1-\varepsilon_s)} \tag{4.2}$$

$$\varepsilon_t = \frac{\varepsilon_a}{\varepsilon_s} \tag{4.3}$$

where r_a and r_s denote the primary and secondary reflector radius, respectively. It is to be noted that r_s is not fixed in this case and it varies in accordance to the *f*/D ratio.

Table 4.2 Performance of the Cassegrain antenna (focal-length-to- diameter ratio f/D, secondary reflector radius rs, edge taper Te, spillover efficiency εs, taper efficiency εt, aperture efficiency εa).

f/D	rs (mm)	Te (dB)	εs (%)	εt (%)	εa (%)
0.1	535	10.43	90.94	87.08	79.19
0.2	399	10.85	91.79	87.38	80.20
0.3	381	10.91	91.90	87.39	80.31
0.4	375	10.86	91.79	87.53	80.34
0.5	372	10.75	91.59	87.74	80.36
0.6	371	10.64	91.36	87.96	80.36
0.7	370	10.50	91.09	88.21	80.35
0.8	369	10.34	90.75	88.51	80.32
0.9	369	10.17	90.39	88.79	80.26
1.0	369	10.00	90.01	89.09	80.19

Table 4.2 lists the design's efficiency and edge tapers. Although there are differences at different *f*/D ratios, the table shows that the spillover, taper, and aperture efficiencies are very similar. Figure 4.1 depicts the overall aperture efficiencies *f*/D varies. Table 4.2 and Figure 4.1 show that when *f*/D is set between 0.5 and 0.6, ε_a reaches a peak at 80.36 percent. When the radius of the secondary reflector is between 371 mm and 372 mm, and the edge taper T_e is between 10.64 dB and 10.75 dB, the antenna's performance is at its best. Figure 4.2 shows the radiation patterns for antenna designs with *f*/D = 0.5 and 0.6. Close examination of the radiation patterns reveals that the magnitudes of the main and side lobes are extremely close to each other.

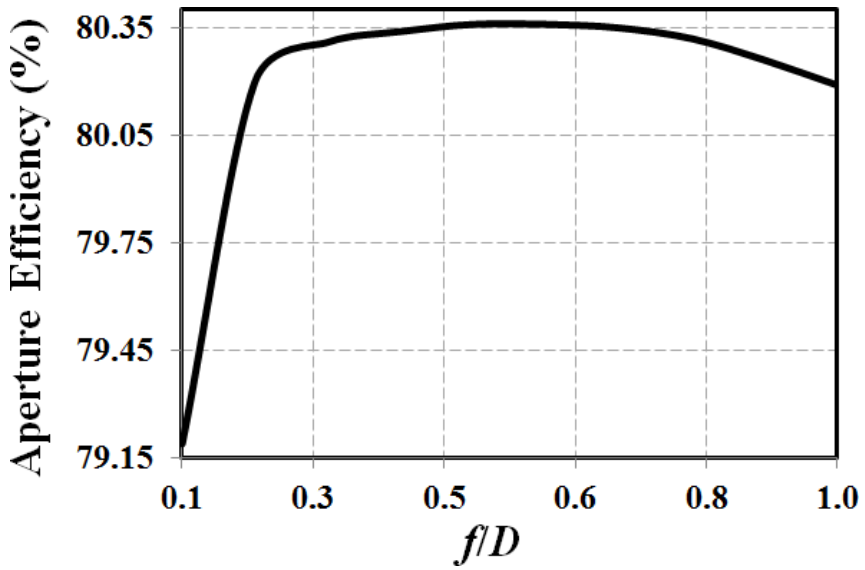


Figure 4.1: Aperture efficiency at different primary reflector *f*/D ratio

When *f*/D is between 0.5 and 0.6, the antenna design achieves an optimal aperture efficiency of 80.36 percent, according to the results. This correlates to the secondary reflector's radius and edge taper, which are 371mm to 372mm and 10.64dB to 10.75dB, respectively.

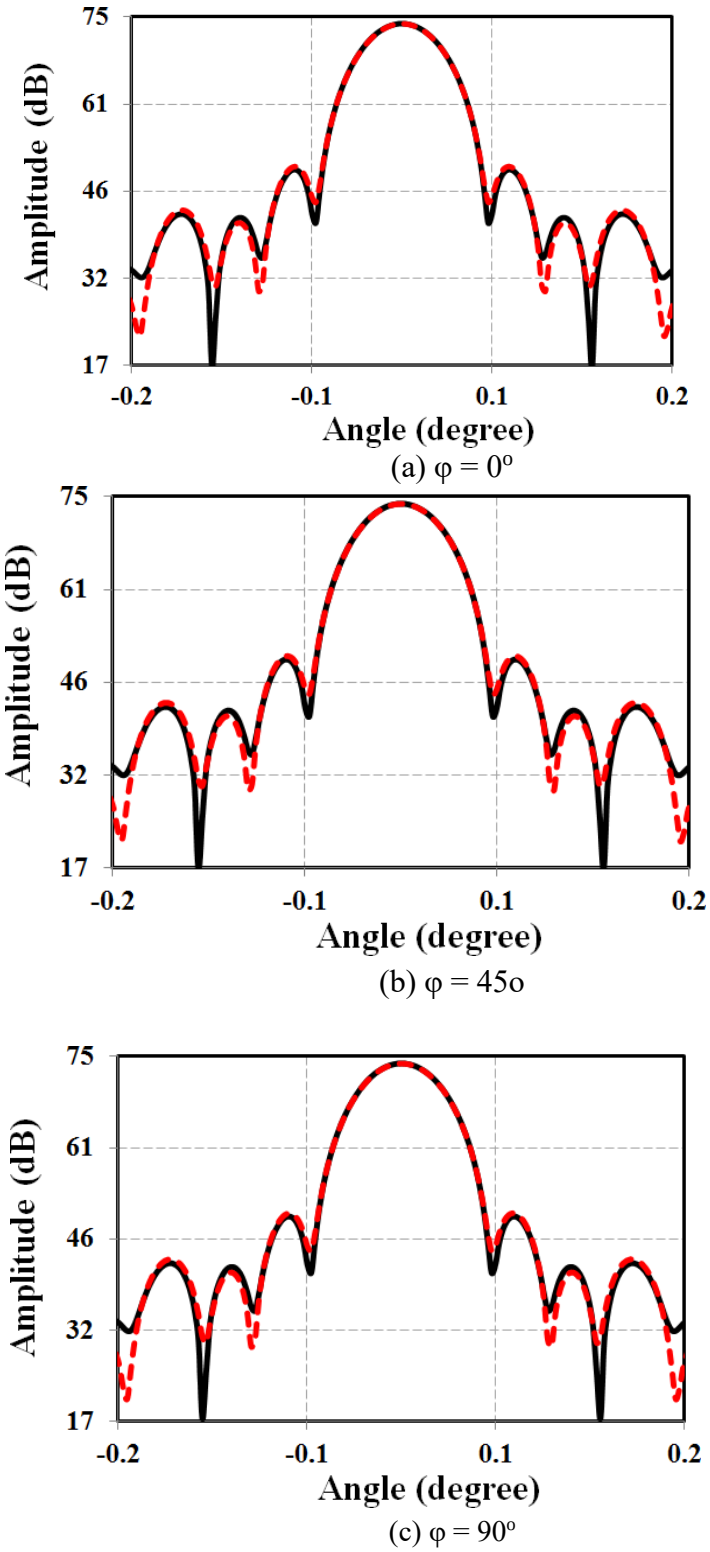


Figure 4.2: The beam patterns of *f*/D = 0.5 (solid line) and 0.6 (dotted line) for a Cassegrain antenna, at *f* = 45 GHz for observations at φ = (a) 0º, (b) 45º, and (c) 90º.

4.3 Encryption Methods for Radio Astronomical Images

Ghadirli *et al.* (2019) mentioned that digital image encryption is the process of hiding images from unauthorized access. In chapter 3, various novel algorithm for digital images had been developed. They are:

i) Development of Bit-level Scrambling Encryption for Radio Telescope Imageries (Proposed Algorithm I)

ii) Bit-levels Encryption for RGB Telescope Images (Proposed Algorithm II)

iii) Design of Encryption Algorithm in Combined Spatial and Frequency Domains for Telescope Grayscale and Bayer Images (Proposed Algorithm III)

iv) Combined Spatial and Frequency Domains in Algorithm of RGB Color Image Security for Telescope Images (Proposed Algorithm IV)

Scrambling degree, histogram distribution, key sensitive analysis, peak signal-to-noise ratio (PSNR), Information Entropy, and SSIM are the measurement used to identify the most reliable algorithm for digital image security.

4.3.1 Scrambling Degree in Algorithm of Bit-level Scrambling Encryption for Radio Telescope Imageries

Arnold transform was incorporated in the assessment for comparison in order to analyse the efficiency of the suggested scrambling method. The scrambling degree for Arnold transform ranges from 0.78 to 0.93, as shown in Table 5.1. The difference between the highest and lowest number is used to establish the range. The higher the scrambling degree, the more away the pixel has been pushed (Makera & Dena, 2015). Despite the fact that Arnold transform may yield a greater degree of 0.93, it also provides a low value of 0.78, making this scrambling approach somewhat unpredictable. For improved scrambling stability, the relatively limited range of degrees for both Level I and Level II scrambling methods, 0.80–0.89 and 0.84–0.89, respectively, is desirable. When Level I scrambling was used, the gap was decreased to 0.09 from 0.15 when Arnold Transform was used. After using Level II scrambling, the disparity was further decreased to 0.05. The second scrambling approach clearly delivers a higher scrambling degree with a lower gap value.

The images are chosen for assessment to further examine the encryption technique on radio telescope imageries, as illustrated in Figure. 4.3(a), 4.4(a) and 4.5(a). After using the Level II scrambling method, the difference between the highest and lowest value is between 0.04 and 0.05, as shown in Figure. 4.3(b), 4.4(b) and 4.5(b). These findings are comparable to those in Table 4.3, which show that using the Level II scrambling approach can improve encryption. Level II scrambling appears to be reliable in the encrypted

transmission of the digital telemetry pictures employed in this investigation, since the average between the greatest and lowest value varies between 0.840 and 0.860.

Table 4.3: Scrambling Degree

Method	**Range**	**Gap between highest and lowest**	**Average between highest and lowest**
Arnold Transform	0.78 -0.93	0.15	0.855
Level 1 Scrambling	0.80-0.89	0.09	0.845
Level II Scrambling	0.84-0.89	0.05	0.865

Table 4.4: Comparison.

Telescope image	Level II	
	Gap between highest and lowest	Average between highest and lowest
Moon	0.04	0.860
Supernova	0.05	0.850
Galaxy	0.05	0.840

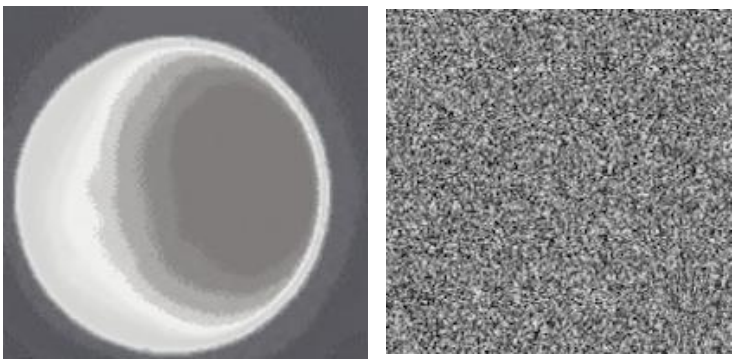


Figure 4.3: (a) Telescope image of moon, (b) After scrambling algorithm

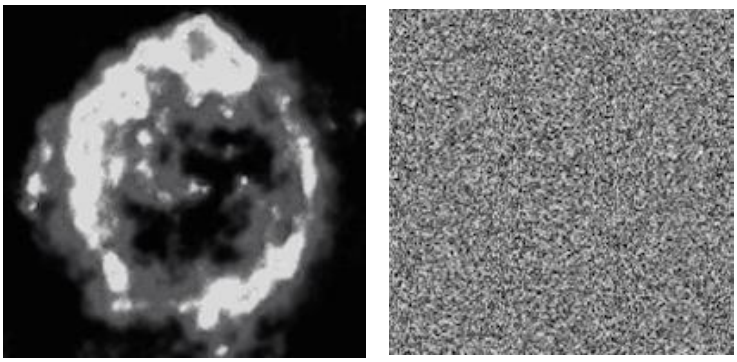


Figure 4.4: (a) Telescope image of supernova, (b) After scrambling algorithm

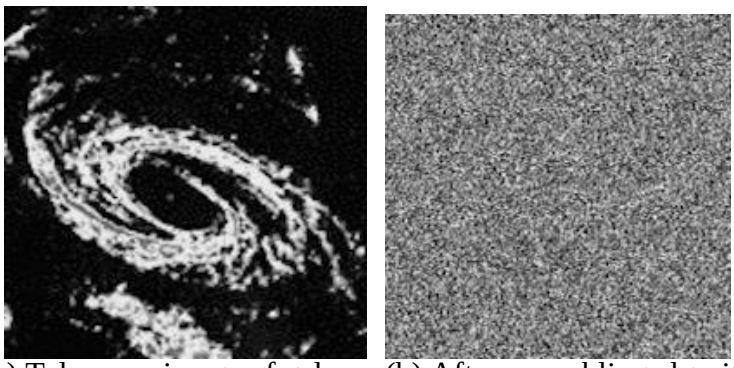


Figure 4.5: (a) Telescope image of galaxy, (b) After scrambling algorithm

4.3.2 Histogram Distribution

The histogram distribution of the pixels can be used to observe the pattern distribution of the image pixels after encryption, then, any reliable encryption algorithm can make the image pixels more uniformly distributed between 0 and 255 in its histogram. (Wang *et al.,* 2020). From Figure 4.7, it is shown the pattern of histogram in proposed algorithm II is amended when compared to the original histogram in Figure 4.6.

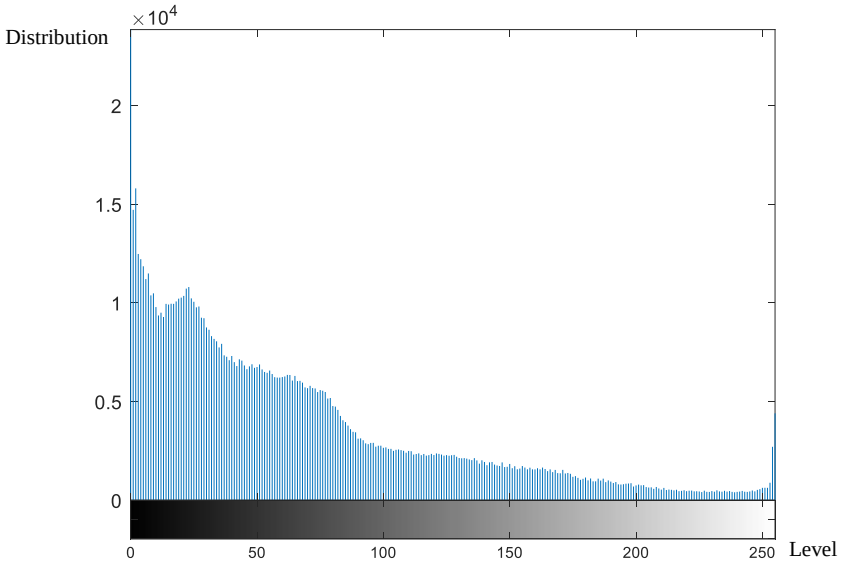


Figure 4.6: Histogram Distribution from Original Image

The histogram distributions for the proposed algorithm III and IV are found to be more uniform in the distribution diagram as shown in Figure 4.8, 4.9 and 4.10. The proposed algorithm IV is divided into two types of histogram distributions which are histogram with spatial domain only and histogram with spatial and frequency domains.

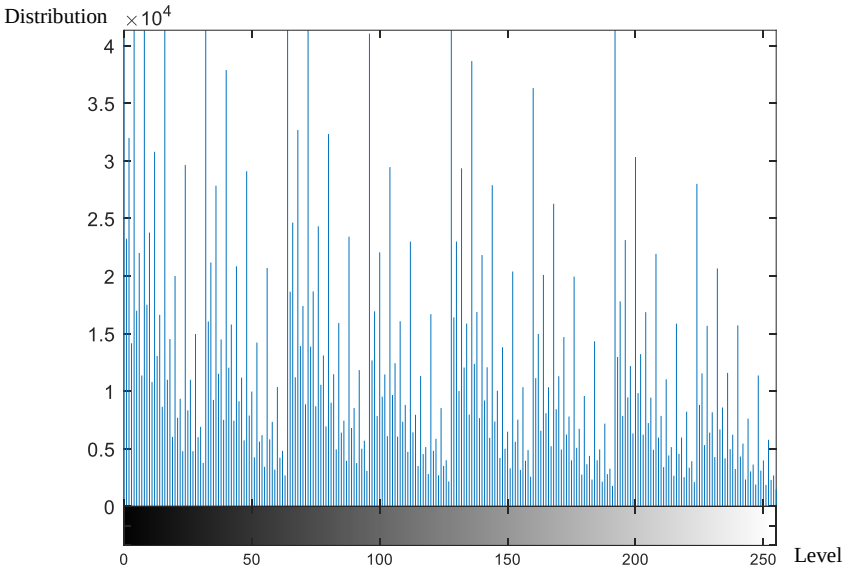


Figure 4.7: Histogram after Proposed Algorithm II

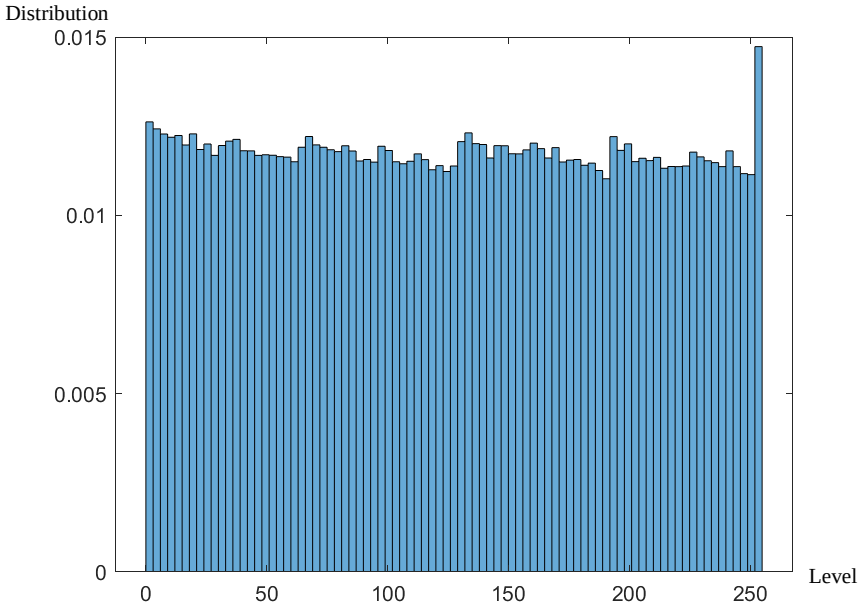


Figure. 4.8: Histogram Distribution after Proposed Algorithm III

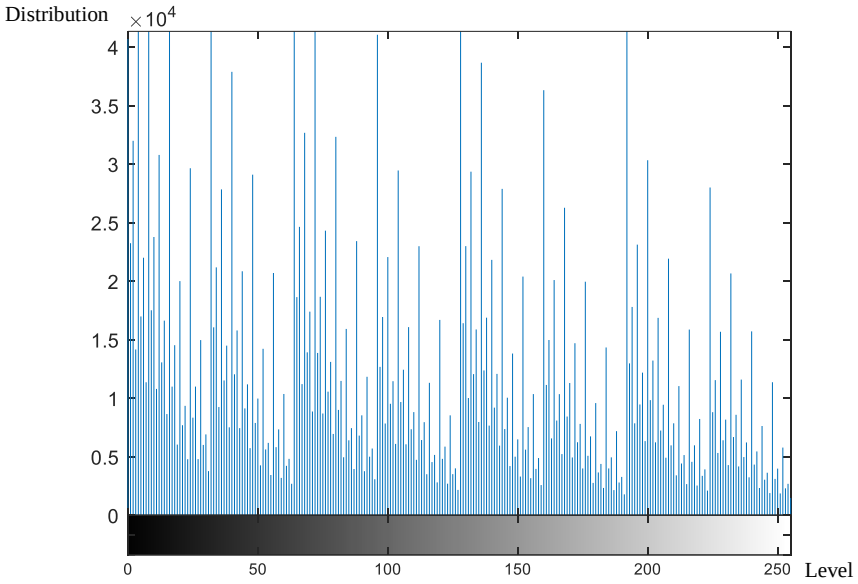


Figure 4.9: Histogram after proposed algorithm IV with spatial domain only

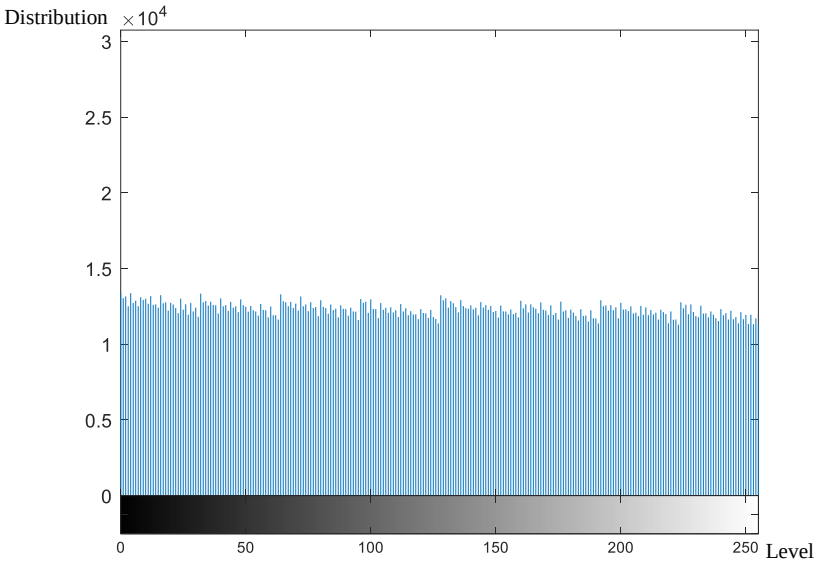


Figure. 4.10: Histogram after proposed algorithm IV with spatial and frequency domains only

When histogram distribution in Figure 4.9 and 4.10 are compared to the original histogram distribution in Figure 4.6, it is evident that the pattern of the histogram has changed. After combining the spatial and frequency domains in

the picture encryption process, Figure 4.10 indicates a significant improvement in histogram distribution.

4.3.3 Key Sensitivity Analysis

Two significant measurements used to analyze the ability of resist from any different attacks are Number of Pixel changing Rate (NPCR) and Unified Average Changing Intensity (UACI). NPCR is rate of change of pixel changes (David, 2009) and its theoretical expectation value is 99.694% (Gao *et al*., 2019). The NPCR is expressed in equation (4.4) as follows:

$$NPCR = \frac{\sum_{ij} D(i,j)}{N \times M} \times 100\% \tag{4.4}$$

$$D(i,j) = \begin{cases} 1, c_1(i,j) \neq c_2(i,j) \\ 0, c_1(i,j) = c_2(i,j) \end{cases} \tag{4.5}$$

where C_1 and C_2 are two encrypted images of dimension *M x N*.

UACI refers to the normalized average intensity of pixels (Wang *et al*., 2020) and its theoretical expectation value of UACI is 33.4635% (Gao *et al.*, 2019). The equation of UACI (Jose, 2019) can be calculated as:

$$UACI = \frac{1}{N \times M} \sum_{ij} \frac{|C_1(i,j) - C_2(i,j)|}{255} \times 100\% \tag{4.6}$$

where C_1 and C_2 are two encrypted images of dimension *M x N*.

Table 4.5: NPCR and UACI values of in different algorithms.

Algorithm	Characteristics	NPCR (%)	UACI (%)
Proposed Algorithm II	Double Scrambling	99.7064	33.4635
Proposed Algorithm III with Grayscale	Combined Spatial and Frequency Domains	99.8792	36.1383
Proposed Algorithm III with Bayer	Combined Spatial and Frequency Domains	99.8782	36.4717
Proposed Algorithm IV	Combined Spatial and Frequency Domains	99.8945	38.6987
Algorithm (Ting, K.C., et al., 2022)	Two Levels scrambling	99.7064	33.4635
Algorithm (Xu & Tian, 2018)	Latin squares	99.6107	33.4232
Algorithm (Kadir et al., 2014)	Skew tent map	99.6062	33.8981
Algorithm (Wei et al., 2012)	DNA sequence	99.2173	33.4055
Algorithm (Wu et al., 2014)	Latin squares	99.6689	33.4055
Algorithm (L. Y. Zhang et al., 2014)	Ciphertext feedback	99.6041	33.4198

It is stated in Gao *et al.* (2019) that the scheme has the power to withstand differential attacks if the NPCR > 90% and UACI ≈33%. The NPCR and UACI values of the proposed algorithms are therefore tabulated in Table 4.5. Proposed algorithms II, III, and IV show that the NPCR rates are above 90% and the UACI rate are in the range of 33.4635 and 38.6987. This is apparent from Table 4.5 that our proposed algorithms can be applied in security transmission for its high NPCR (>90) and good UACI (≈33%).

4.3.4 PSNR

The peak signal-to-noise ratio (PSNR) may be used to assess digital image's quality (Wang et al., 2020) and it can also be used as the index to measure the level of correlation between the encrypted image and the original image. As shown in (4.7), the lower value of the PSNR value implies higher security rank in the encryption algorithm.

$$PSNR = 10log_{10}(\frac{255\times255}{MSE}) \tag{4.7}$$

$$MSE = \frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N}(P(i,j) - C(i,j))^2 \tag{4.8}$$

where M and N is the image dimension, P is original image, and C is encrypted image.

Output of PSNR index with at least 30 should be obtained from two similar images. Therefore, any low PSNR index indicates that the two images being compared are not equal. (Gu *et al.,* 2016) and as the result of the calculation, the entropy value of the proposed algorithm II, III (with Grayscale Images), III (with Bayer Images) and IV are found to be 9.6298, 8.2730, 8.2007

and 7.6817 respectively. All values of PSNR for the proposed algorithms are under value 30 which shows rate of difference between original image and encrypted image are very high. This indicator shows the reliability of the encryption algorithm in our proposed algorithms.

Table 4.6: PSNR for Proposed Algorithms

Algorithm	Value
Proposed Algorithm II	9.6298
Proposed Algorithm III with Grayscale Images	8.2730
Proposed Algorithm III with Bayer Images	8.2007
Proposed Algorithm IV with Combined Spatial and Frequency Domains	7.6817

4.3.5 Information Entropy

The information entropy analysis can be used to measure the complexity of encrypted data. The encrypted images are supposed to be so complex until non original data about the original data can be retrieved out of it. The information entropy analysis can be measured using applying (4.9) below:

$$H(m) = \sum_{i=0}^{M-1}(p(m_i)log\frac{1}{p(m_{i)}}) \qquad (4.9)$$

where m is a set information source, and m_i represents the probability of occurrence.

Wang *et al.* (2020) mentioned that value 8 is the optimum value of information entropy for any image encryption methodology. The quality of encryption becomes higher when the value of information entropy is closer to 8. All results or outputs of the proposed image encryption methods are recorded in Table 4.7. Table 4.7 indicates Entropy value as 7.9253 for proposed Algorithm II, 6.5400 for Proposed Algorithm III (with Grayscale Images), 6.5425 for Proposed Algorithm III (with Bayer Images) and 6.6175 for Proposed Algorithm IV.

From the result shown in Table 4.7, the proposed Algorithm II has the nearest value to 8. Wang *et al.* (2020) indicates that the proposed algorithm has the highest complexity of encrypted image compared to other algorithms. Nevertheless, other proposed algorithms show their entropy value are more than 6.5400, their complexity of encrypted algorithms are in the acceptance level.

Table 4.7: Entropy Value for Proposed Algorithm IV

Algorithm	Value
Proposed Algorithm II	7.9253
Proposed Algorithm III with Grayscale Images	6.5400
Proposed Algorithm III with Bayer Images	6.5425
Proposed Algorithm IV with Combined Spatial and Frequency Domains	6.6175

4.3.6 SSIM

The Structural Similarity Index Measure algorithm is used to calculate the similarity index between original and encrypted images. If the SSIM value is low, the amount of dissimilarity will be raised. A lower SSIM score implies that the difference between two digital pictures is greater (Wang *et al*., 2020). The calculation of the SSIM index between the original and encrypted image is:

$$SSIM(I,E) = \frac{(2\mu_I\mu_E+J_1)(2\sigma_{IE}+J_2)}{(\mu_I^2+\mu_E^2+J_1)(\mu_I^2+\mu_E^2+J_2)} \quad (4.10)$$

where μ_I and μ_E are mean of the original and encrypted image pixels respectively, σ_I and σ_E are the standard deviation of the original image pixels and encrypted image pixels respectively, σ_{IE} is the covariance between the original and encrypted image pixels. $J_1 = (s_1P)^2$, $J_2 = (s_2P)^2$ and s1=0.01, s_2=0.03 and P= 2number of bits per pixel – 1. Table 4.8 shows a low SSIM values for the proposed algorithms. This indicates that the proposed algorithms indeed have the efficacy for encryption.

Table 4.8: SSIM for Proposed Algorithms

Algorithm	Value
Proposed Algorithm II	0.0309
Proposed Algorithm III with Grayscale Images	0.0289
Proposed Algorithm III with Bayer Images	0.0284
Proposed Algorithm IV	0.0273

4.3.7 Security Index Mapping Table (SIMT)

Table 4.9: Summary Results of Proposed Algorithm I, II, III, and IV

Algorithm	I	II	III (gray Image)	III (Bayer Image)	IV
Histogram	4	3	2	2	1
NPCR	-	99.7064	99.8792	99.8782	99.8945
UACI	-	33.4635	36.1383	36.4717	38.6987
PNSR	-	9.6298	8.2730	8.2007	7.6817
Information Entropy	-	7.9253	6.5400	6.5425	6.6175
SSIM	-	0.0309	0.0289	0.0284	0.0273

The outcomes of proposed algorithms I, II, III and IV had been compared with each other to identify the most suitable algorithm. The summary of outcomes are shown in Table 4.9 above. This table has been converted to index mapping format which is shown in Table 4.10 below. Table 4.10 shows that the proposed algorithm with the lowest value in the Total Index will be classified the most suitable algorithm among the proposed algorithm I, II, III and IV. From this table, it shows that proposed algorithm IV has the lowest total index value. Therefore, it is considered the most suitable encryption algorithm for RGB telescope imaginaries.

Table 4.10: Security Index Mapping (SIMT)

Algorithm	**I**	**II**	**III** (Gray Image)	**III** (Bayer Image)	**IV**
Histogram	4	3	2	2	1
NPCR	5	4	2	3	1
UACI	5	1	2	3	4
PNSR	5	4	3	2	1
Information Entropy	5	1	3	2	4
SSIM	5	4	3	2	1
Total index	29	17	15	14	12

4.5 Summary

The performance Analysis of a Cassegrain antenna with different primary reflector focal-length-to-diameter *f*/D ratio has been performed in this chapter. Besides that, evaluation of various telescope's images encryption methods also have been discussed in this chapter. In the discussion, strengths and weaknesses of each algorithm have been identified.

CHAPTER FIVE

CONCLUSION AND RECOMMENDATION

5.1 Background

The work has extended the knowledge from existing telescope designs to analyse the performance of parabolic antennas for radio telescopes. Besides that, various development of encryption methods for radio astronomical images have been studied. Any optimization processes in the parabolic antennas can provide optimal quality of signal to be transformed into digital images. Therefore, encryption methods play a significant role to ensure high rate of digital image security during signal transmission.

5.2 Conclusion

The performance of a Cassegrain antenna with varied main reflector focal-length-to-diameter f/D ratios was examined and assessed. When f/D = 0.5 to 0.6, the antenna design achieves an optimal aperture efficiency of 80.36 percent, according to the results. This corresponds to the secondary reflector's radius and edge taper, which are 371 mm to 372 mm and 10.64 dB to 10.75 dB, respectively. Therefore, objective to optimize the telescope aperture efficiency by performance analysis on current telescope design have been achieved.

In this study, several development of encryption methods for radio astronomical images have been studied and proposed. The proposed algorithms include

i) Development of Bit-level Scrambling Encryption for Radio Telescope Imageries

ii) Bit-levels Encryption for RGB Telescope Images

iii) Design of Encryption Algorithm in Combined Spatial and Frequency Domains for Telescope Grayscale and Bayer Images

iv) Combined Spatial and Frequency Domains in Algorithm of RGB Color Image Security for Telescope Images

The security performance and reliability of the proposed algorithms have been evaluated using several analysis processes, such as histogram distribution, NPCR, UACI, PNSR, information Entropy, and SSIM. Security Index Mapping Table (SIMT) is used to compare the performance of the security algorithm among these four novel encryption algorithms. The outcomes of SIMT show Combined Spatial and Frequency Domains in Algorithm of RGB Color Image Security for Telescope Images is the novel algorithm for optimal security in telescope images. This novel encryption algorithm is a reliable methodology for Digital Image Security too.

3. Recommendations

A more in-depth investigation on the optimized parameters for the radio telescope can be performed. Various different kinds of bands of the ALMA telescope should be taken into consideration as well when computing the aperture efficiencies of the telescope. Besides that, the performance of the telescope aperture efficiency in other ground-based observatories is suggested for future study too.

Even though the development of encryption methods for radio astronomical images in this study showed an encouraging and positive outcomes improvement process should continue to ensure better algorithms can be developed in the near future. Artificial Intelligence (AI) agents such as artificial neural network (ANN), fuzzy logic, Genetic Algorithm (GA), and etc. are to be integrated into the encryption algorithms. Therefore, the selection of a suitable AI agent and the employment of AI in the encryption methods are going to be the significant agenda in further research recommendation.

BIBLIOGRAPHY

About ALMA - ALMA. (n.d.). ALMA NAOJ. https://alma-telescope.jp/en/about

Andrecut, M. (1998). Logistic Map as a Random Number Generator. *International Journal of Modern Physics B, 12*(09), 921–930. https://doi.org/10.1142/s021797929800051x

Artiles, J. A., Chaves, D. P., & Pimentel, C. (2019). Image encryption using block cipher and chaotic sequences. *Signal Processing: Image Communication*, *79*, 24–31. https://doi.org/10.1016/j.image.2019.08.014

Bong, D.B.L., Lai, K.C., Joseph, A. (2009). Automatic Road Network Recognition and Extraction for Urban Planning. *Int. J. Appl. Sci., Eng. Technol*. 5 54–59

Chapeau-Blondeau, F., & Belin, E. (2020). Fourier-transform quantum phase estimation with quantum phase noise. *Signal Processing*, *170*, 107441. https://doi.org/10.1016/j.sigpro.2019.107441

Chen, G., Mao, Y., & Chui, C. K. (2004). A symmetric image encryption scheme based on 3D chaotic cat maps. *Chaos, Solitons & Fractals*, *21*(3), 749–761. https://doi.org/10.1016/j.chaos.2003.12.022

David, B.L.B., Ting, K.C., Wang, Y.C.(2009). Novel Face Recognition Approach using Bit-Level Information and Dummy Blank Images in Feedforward Neural Network. Appl. Soft Comput. 483-490

El-Samie, F. E. Abd., Ahmed, H. H., Elashry, I. F., Shahieen, M. H., Faragallah, O. S., El-Rabaie, E. M. & Alshebeili, S. A. (2014).Image encryption: a communication perspective. Australia: Taylor & Francis Group, LLC.

Fares, K., Amine, K., & Salah, E. (2020). A robust blind color image watermarking based on Fourier transform domain. *Optik*, *208*, 164562. https://doi.org/10.1016/j.ijleo.2020.164562

Gehani, A., LaBean, T., Reif, J.: DNA-Based Cryptography. In: Jonoska, N., Păun, G., Reozenberg, G. (2003). Aspects of Molecular Computing. *Lecture Notes in Computer Science, 2950*, 167–188

Ghadirli, H. M., Nodehi, A., & Enayatifar, R. (2019). An overview of encryption algorithms in color images. *Signal Processing*, *164*, 163–185. https://doi.org/10.1016/j.sigpro.2019.06.010

Gonzalez, R., & Woods, R. (2017). *Digital Image Processing* (4th ed.). Pearson.

Goldsmith, P.F. (1998) Quasioptical Systems: Gaussiam Beam Quasioptical Propagation and Applications. IEEE Press: Piscataway.

Gu, G., Ling, J., Xie, G., & Li, Z. (2016). A chaotic-cipher-based packet body encryption algorithm for JPEG2000 images. *Signal Processing: Image Communication*, *40*, 52–64. https://doi.org/10.1016/j.image.2015.06.009

Jithin, K., & Sankar, S. (2020). Colour image encryption algorithm combining Arnold map, DNA sequence operation, and a Mandelbrot set. *Journal of Information Security and Applications*, *50*, 102428. https://doi.org/10.1016/j.jisa.2019.102428

Kadir, A., Hamdulla, A., & Guo, W. Q. (2014). Color image encryption using skew tent map and hyper chaotic system of 6th-order CNN. *Optik*, *125*(5), 1671–1675. https://doi.org/10.1016/j.ijleo.2013.09.040

L07: Reflectors. (n.d.). PHY217. http://slittlefair.staff.shef.ac.uk/teaching/phy217/lectures/telescopes/L07/index.html#top

Liu, X., Song, Y., & Jiang, G. P. (2019). Hierarchical Bit-Level Image Encryption Based on Chaotic Map and Feistel Network. *International Journal of Bifurcation and Chaos*, *29*(02), 1950016. https://doi.org/10.1142/s0218127419500160

Makera M.A., and Dena, R.A. (2015). Simple image scrambling algorithm based on random numbers generation. International Journal of Advanced Research in Computer Science and Software Engineering (5), 434-438.

M. Carter, et al., "ALMA Front End Optics Design Report (FEND-40.02.00.00-035- B-REP)," 2007.

Murphy, J. A. (1987). Distortion of a simple Gaussian beam on reflection from off-axis ellipsoidal mirrors. *International Journal of Infrared and Millimeter Waves*, *8*(9), 1165–1187. https://doi.org/10.1007/bf01010819

National Radio Astronomy Observatory - Legacy Content - ALMA (CV). (2022). National Radio Astronomy Observatory. http://legacy.nrao.edu/alma.shtml

Olbrys, J., & Mursztyn, M. (2019). Measuring stock market resiliency with Discrete Fourier Transform for high frequency data. *Physica A: Statistical Mechanics and Its Applications*, *513*, 248–256. https://doi.org/10.1016/j.physa.2018.09.028

Reflecting Telescopes. (2020). PH217. Retrieved October 30, 2021, from http://slittlefair.staff.shef.ac.uk/teaching/phy217/lectures/telescopes/L07/index.html

Tercero, F. (2008). Radio Telescopes. *Proceedings of Science: 2nd MCCT-SKADS Training School Radio Astronomy: fundamentals and the new instruments Siguenza(Spain)*

Tham, C.Y., Withington, S., & Yassin, G. (2007) Optimisation of ALMA Feed Optics.

Ting, K. C., Tan, J. Y. B., Lee, T. Z., & Bong, D. B. L. (2013). Face Recognition by Neural Network Using Bit-planes Extracted from An Image. *Journal of Information and Computational Science*, *10*(16), 5253–5261. https://doi.org/10.12733/jics20102079

Ting, K.C., Yeap, K.H., Teh, P.C., Lai, K.C.: Bit-Levels Encryption for RGB Telescope Images. In: Isa K. et al. (eds) Proceedings of the 12th National Technical Seminar on Unmanned System Technology 2020. Lecture Notes in Electrical Engineering, Vol 770. Springer, Singapore (2022)

Two-mirror telescopes: Cassegrain, Gregorian and variants. (n.d.). Telescope-Optics. https://www.telescope-optics.net/two-mirror.htm

Wang, S., Wang, C., & Xu, C. (2020). An image encryption algorithm based on a hidden attractor chaos system and the Knuth–Durstenfeld algorithm. *Optics and Lasers in Engineering*, *128*, 105995. https://doi.org/10.1016/j.optlaseng.2019.105995

Wang, X., Li, Y., & Jin, J. (2020). A new one-dimensional chaotic system with applications in image encryption. *Chaos, Solitons & Fractals*, *139*, 110102. https://doi.org/10.1016/j.chaos.2020.110102

Wotten, A. (2008). ALMA capabilities for observations of spectral line emission. *Astrophysics and Space Science*, 313, 9 – 12.

Wu, Y., Zhou, Y., Noonan, J. P., & Agaian, S. (2014). Design of image cipher using latin squares. *Information Sciences*, *264*, 317–339. https://doi.org/10.1016/j.ins.2013.11.027

Wu, Y., Noonan, J. P., & Agaian, S. (2011). Dynamic and implicit latin square doubly stochastic S-boxes with reversibility. *2011 IEEE International Conference on Systems, Man, and Cybernetics*. https://doi.org/10.1109/icsmc.2011.6084188

Wei, X., Guo, L., Zhang, Q., Zhang, J., & Lian, S. (2012). A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system. *Journal of Systems and Software*, *85*(2), 290–299. https://doi.org/10.1016/j.jss.2011.08.017

Wei, X., Guo, L., Zhang, Q., Zhang, J., & Lian, S. (2012). A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system. *Journal of Systems and Software*, *85*(2), 290–299. https://doi.org/10.1016/j.jss.2011.08.017

Xu, M., & Tian, Z. (2018). A novel image encryption algorithm based on self-orthogonal Latin squares. *Optik*, *171*, 891–903. https://doi.org/10.1016/j.ijleo.2018.06.112

Yeap, K. H., Lai, K. C., Ting, K. C., Teh, P. C., Nisar, H., & Yeo, W. L. (2017). Optimization of reflector antennas in radio telescopes. *Malaysian Journal of Fundamental and Applied Sciences*, *13*(3). https://doi.org/10.11113/mjfas.v13n3.552

Yeap, K. H., Tham, C. Y., Nisar, H., & Loh, S. H. (2013). Analysis of Probes in a Rectangular Waveguide. *Frequenz*, *67*(5–6). https://doi.org/10.1515/freq-2012-0117

Yeap, K. H., Yiam, C. Y., Lai, K. C., Loh, M. C., Lim, S. K., & Rizman, Z. I. (2016). Analysis of Offset Antennas in Radio Telescopes. *International Journal on Advanced Science, Engineering and Information Technology*, *6*(6), 997. https://doi.org/10.18517/ijaseit.6.6.1071

Yun-Shik, L. (2008). Principles of Terahertz Science and Technology. New York, NY: Springer.

Zhang, G., & Liu, Q. (2011). A novel image encryption method based on total shuffling scheme. *Optics Communications*, *284*(12), 2775–2780. https://doi.org/10.1016/j.optcom.2011.02.039

Zhang, L. Y., Hu, X., Liu, Y., Wong, K. W., & Gan, J. (2014). A chaotic image encryption scheme owning temp-value feedback. *Communications in Nonlinear Science and Numerical Simulation*, *19*(10), 3653–3659. https://doi.org/10.1016/j.cnsns.2014.03.016

Zhou, Y., Bao, L., & Chen, C. P. (2014). A new 1D chaotic system for image encryption. *Signal Processing*, *97*, 172–182. https://doi.org/10.1016/j.sigpro.2013.10.034

LIST OF PUBLICATIONS

1. Ting, K.C., Yeap, K.H., Teh, P.C., Lai, K.C.: Bit-Levels Encryption for RGB Telescope Images. In: Isa K. et al. (eds) Proceedings of the 12th National Technical Seminar on Unmanned System Technology 2020. Lecture Notes in Electrical Engineering, Vol 770. Springer, Singapore (2022)

2. Ting, K.C., Yeap, K.H., Teh, P.C., Lai, K.C. & Francis-Lothai, F. (2022). Development of Bit-level Scrambling Encryption Algorithm for Radio Telescope Imageries. *Borneo Journal of Sciences & Technology*, *4*(1). https://doi.org/10.35370/bjost.2022.4.1-08

3. Ting, K.C., Yeap, K.H., Teh, P.C., Lai, K.C., Francis-Lothai, F. (2022). Combined Spatial and Frequency Domains in Algorithm of RGB Color Image Security for Telescope Images. In: Ghazali, R., Mohd Nawi, N., Deris, M.M., Abawajy, J.H., Arbaiy, N. (eds) Recent Advances in Soft Computing and Data Mining. SCDM 2022. Lecture Notes in Networks and Systems, vol 457. Springer, Cham. https://doi.org/10.1007/978-3-031-00828-3_18

4. Ting K.C., Yeap K.H., Teh P.C., Lai, K.C. & Francis-Lothai, F. (2022) Design of Encryption Algorithm in Combined Spatial and Frequency Domains for Telescope Grayscale and Bayer Images.J Adv Res Sig Proc Appl 2021; 3(2): 1-5

5. Yeap, K. H., Lai, K. C., Ting, K. C., Teh, P. C., Nisar, H., & Yeo, W. L. (2017). Optimization of reflector antennas in radio telescopes. *Malaysian Journal of Fundamental and Applied Sciences*, *13*(3). https://doi.org/10.11113/mjfas.v13n3.552