International Journal of Scientific Trends- (IJST)
ISSN: 2980-4299
Volume 2, Issue 7, July, 2023
Website: https://scientifictrends.org/index.php/ijst
Open Access, Peer Reviewed, Scientific Journal

Cyber Security Role in Image Encryption

Ali Ahmed Jaddoa JADDOA1, Asst. Prof. Dr. Sefer Kurnaz2
1,2 Electrical and Computer Engineering, Altinbas university, Istanbul, Turkey.
ali2008un@gmail.com1, sefer.kurnaz@altinbas.edu.tr2

Abstract

Digital images are vulnerable to unauthorized access, modification, and theft, making image encryption and decryption an essential aspect of information security. Image encryption and decryption is the process of converting a digital image from its original form to an unreadable format, ensuring its confidentiality and integrity. This study aims to explore various encryption and decryption techniques using MATLAB, a high-level programming language widely used for image processing.

The methodology for this study involves implementing and testing different encryption and decryption algorithms on various types of digital images using MATLAB. The algorithms tested include symmetric-key encryption, such as Advanced Encryption Standard (AES) and Data Encryption Standard (DES), and asymmetric-key encryption, such as RSA and ElGamal. The testing involves evaluating the security and speed of each algorithm and their compatibility with different image formats and sizes.

The results of the study show that symmetric-key encryption algorithms, such as AES and DES, provide high levels of security and speed, making them suitable for large-scale image encryption and decryption applications. Asymmetric-key encryption algorithms, such as RSA and ElGamal, provide enhanced security but are slower than symmetric-key encryption algorithms. The study also highlights the importance of key management and storage in ensuring the security of the encrypted images.

The study identifies several future research directions, including the development of hybrid encryption algorithms that combine the strengths of symmetric and asymmetric encryption, and the integration of biometric authentication for enhanced security. The study also emphasizes the need for more research on the impact of encryption and decryption on image quality and the development of efficient and compatible algorithms for different image formats and sizes.

Overall, this study provides insights into the implementation and testing of encryption and decryption techniques for digital images using MATLAB. The findings highlight the importance of balancing security and speed in choosing encryption algorithms and the need for effective key management to ensure the security of encrypted images. The study's results and future research directions can guide the development of robust and efficient image encryption and decryption techniques for enhanced information security.

Keywords: Cryptography, Public key cryptosystem, RSA cryptosystem, color and gray images, MATLAB.

Introduction

The concepts of security in a modern digital communication system are broken down into their component parts that are most important to understand, and then they are explained in a condensed fashion. In addition to this, it discusses the security flaws that are present in a prominent market standard known as WiMAX [1], as well as a potential solution that could address some of these security flaws. In addition to this, it also discusses a potential solution that could address some of these security flaws. In addition to this, it also discusses a possible solution that could fix some of these security flaws that have been identified. The subsequent and concluding section of this chapter will be devoted to the discussion of the overall structure of the thesis as a whole.

Secure Digital Communication System

Customers have much more stringent requirements for the confidentiality of services today as a result of the proliferation of personal communication systems such as laptops, mobile phones, and personal tablets, as well as the growing reliance on the internet for conducting business transactions. Customers have much more stringent requirements for the confidentiality of services today as a result of the proliferation of personal communication systems such as laptops, mobile phones, and personal tablets. As a direct result of the proliferation of personal communication systems such as laptops, mobile phones, and personal tablets, customers have significantly more stringent requirements for the confidentiality of services that businesses provide today. One of the many methods that can be used in modern digital communication systems to protect the privacy of users and ensure that their communications remain private is the implementation of a variety of different cryptographic algorithms. This is just one of the many methods that can be used. The term "cryptography" comes from the Greek words "kryptos," which means "hidden," and "graphein," which means "writing" [2]. These two words were combined to form the English word "cryptography." This demonstrates that two parties have had a vested interest in communicating with each other in a secure manner ever since the early ages in order to protect their own respective vested interests. The vested interests in question are the parties' own. The fact that this has been the case all along demonstrates that this is the case. The nature of these communications was military; however, due to the widespread availability of personal communication systems in today's world, maintaining communication confidentiality is valuable not only in scenarios involving military communications but also in scenarios involving civilian communications. A simplified block diagram of a system that facilitates encrypted digital communication is provided for your perusal and convenience in Figure 1-1. The information that a user wishes to transmit is input into a computing terminal by the user in the form of transmission, and the terminal then transmits the information (or, more recently, the user interface of a smartphone). When making use of a system that operates at a high level of abstraction, it is common for the user to be unaware of the fundamental broadcasting system that is being utilized by the system. This is because such a system functions at an extremely high level of abstraction. This line of communication is initially aimed at the person whose job it is to write the source code; in other words, the person to whom responsibility for writing the code falls.

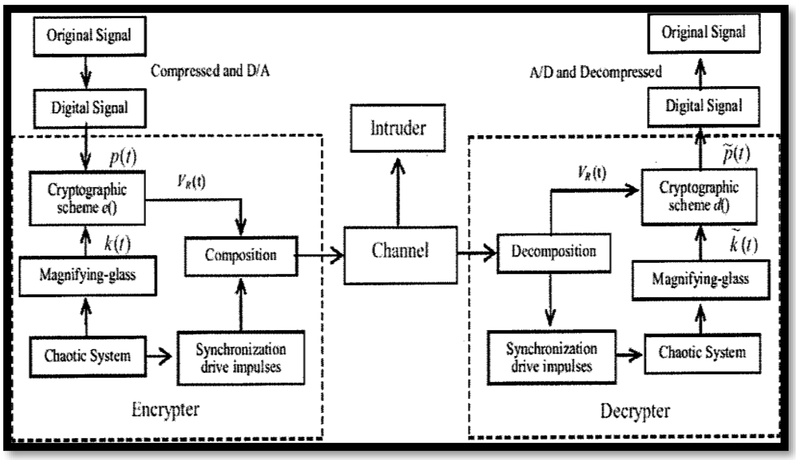


Figure 1:Block Diagram of a secure communication system [4]

The analogue or high-level digital input will be taken by the source coder, and it will then be reformatted in accordance with the requirements of the communication system for the digital input. Both open source standards like G.711 [3] and proprietary standards like AMBE+TM [4] are utilized in the production of modern radios. These standards were derived from coders that complied with the standards already in place, such as the Pulse Code Modulation (PCM). It is essential to take into consideration the prerequisites of the Digital Source Coding in order to choose the appropriate source coding system. Encryption of digital data using various techniques, including channel coding and modulation The process of deciphering the encoding used by the Digital Source Channel in order to carry out digital encryption and decryption Demand User Input Output for User 3's Communication Channel and the Level of Interoperability That Needs to Be Achieved For This Purpose in Order to Accomplish This Objective In order to accomplish this objective, it is necessary to achieve a certain level of interoperability. In order to accomplish this goal, the communication channel for Demand User Input Output for User 3 needs to It is possible to define interoperability as "the ability of various systems and organizations' to work together (or interoperate)," but a definition that is more straightforward would be "the ability to work together." the property of a product or process, the interfaces of which are fully understood, to work with other products or systems, current or future, without any restricted access or implementation," is how interoperability is defined. [5] "Interoperability" is defined as "the capability of a product or process to work with other products or systems, either currently available or in the foreseeable future, without any restricted access or implementation." The term "interoperability" describes the manner in which various forms of information technology cooperate with one another. Encryption, which can be accomplished through the application of digital technology, is the primary factor that ensures the confidentiality of a message while it is being transmitted. The information that is entered into this system is referred to as the "plaintext," which is a term that is used quite frequently. This plaintext is then converted into an encrypted form known as cipher text by the encryption device, which may be a hardware implementation or, more commonly, a software implementation. This particular form of encrypted text is known as cipher text. After that, the person who is supposed to receive this information uses the appropriate digital coding and modulation techniques in order to send the cipher text that they have created to the person who is supposed to receive it.

A channel, in addition to a channel coding block and a modulation block, is required for effective digital communication. Without a channel, digital communication cannot be successful. Error correction, increased throughput, bandwidth management, synchronization, and modulation are just some of the services that they make available to their customers. The specific medium that the data travels through is referred to as the "channel" that is being discussed when referring to the path that the data takes from the sender to the receiver. Static or fixed channels, such as the classic Public Telephone Switching Network (PTSN), and mobile channels, which typically model a wireless metropolitan network channel, are the two types of channels that can be distinguished from one another. Static or fixed channels can also be referred to as a subtype of mobile channels. An example of a traditional public telephone switching network would be one that uses static or fixed channels. One type of channel that can be found in a wireless metropolitan network is a mobile channel. The vast majority of channels broadcast only constant content. In addition, channels can be categorized as either homogeneous or heterogeneous channels depending on the type of channel that they are. Homogeneous channels are the more common classification. These two different classifications each have their own set of benefits and drawbacks. The composition of the vast majority of today's real-time channels is heterogeneous, which indicates that they are made up of a combination of static and dynamic channels in their make-up. This is the case because the vast majority of real-time channels are made up of a combination of these two types of channels. This is the nature of the vast majority of real-time channels that are available in the modern era [14].

The digital receiver in a secure communication system has an appearance that is very close to that of the digital transmitter. The demodulation, decoding, and decryption blocks all use inverse processes in order to reconstruct the signal into a form that human subjects are capable of comprehending. The primary difference between the two can be summarized as follows: In the following part of this article, we are going to provide an overview of the WiMAX system [15].

Overview of WiMAX

WiMAX, which stands for Worldwide Interoperability for Microwave Access, is a communication system that is based on the IEEE 802.16 standard [6]. WiMAX was developed by the IEEE. The IEEE is responsible for the development of WiMAX. The IEEE was the organization in charge of developing the WiMAX protocol. The International Electro technical Commission (IEEE) was the organization that was in charge of developing the WiMAX protocol. The International Electro technical Commission, also known as IEEE, was the group that was in charge of developing the protocol for WiMAX. The operation of WiMAX is fundamentally flexible and robust due to the well-designed physical and wireless channel interface that it possesses. This is a result of the thoughtfully designed. This is doable as a result of the meticulous planning that went into creating the system. It was Cisco Systems, which was also the company that was responsible for the development of WiMAX that first conceived of the idea for it. The design of the architecture for the Physical layer includes an element that is referred to as orthogonal frequency division multiplexing, or OFDM for short. This component was included as part of the design process. The transmission of data is the responsibility of this component (OFDM) [17]. As a result of this, the effects of multipath distortion, which are typical in the wireless channels found in urban areas, are eliminated, which enables the best performance that is possibly possible. This is the best that can possibly be achieved. This is due to the fact that multipath distortion is typical in the wireless channels that can be found in urban areas. This is the case as a result of the widespread presence of multipath distortion in the wireless channels that can be found in urban areas. This is the very best outcome that can be achieved under any specific set of circumstances that have been considered. At the physical layer of the protocol stack, the support for more advanced methods of performance optimization is already built in [19]. These techniques include Low Density Parity Check (LDPC) codes and Turbo codes, in addition to hybrid Automatic Request (ARQ) feedback mechanisms, robust antennas for multi-user operation, and robust Forward Error Correction (FEC) mechanisms such as Low Density Parity Check (ARQ) codes. Other techniques include hybrid Automatic Request (ARQ) feedback mechanisms, robust antennas for multi-user operation, and robust Forward Error Correction (FEC) mechanisms. Other methods include robust antennas for multi-user operations, hybrid Automatic Request (ARQ) feedback mechanisms, and robust Forward Error Correction (FEC) mechanisms. Other methods include hybrid Automatic Request (ARQ) feedback mechanisms, robust antennas for multi-user operation, and robust Forward Error Correction (FEC) mechanisms. All of these methods are discussed in further detail below. These various methods are grouped together under the umbrella term of "robust techniques." In addition to that, the application of these techniques requires the utilization of resilient antennas in order to be successful. Adaptive modulation-coding, spatial multiplexing, and multi-user diversity, to name just a few, are just a few examples of the technologies that could be utilized in an effort to increase the capacity of the system. There are many other technologies that could be used [20]. These are merely a few examples of the plethora of different kinds of technology that may be utilized. These are just some of the many different strategies that can be put into place in order to increase the capacity of the system. There are many more options available. There is a significantly larger variety of choices available. There are still a very significant number left. In addition to its support for voice, video, and a wide variety of other kinds of multimedia data, WiMAX is able to provide strong encryption and user authentication [21]. This is a unique capability of the technology. Additionally, WiMAX is able to support a wide variety of additional forms of multimedia content. This feature is available in addition to the fact that it is able to support the aforementioned varieties of data. Users have the option to make use of this functionality if they so desire to do so, and this option is made available to them. End-to-end functions such as mobility management and security have been built on top of its flexible all-IP network architecture [1,] which is used for its operation. This architecture is used for its operation. [Further citation is required] [Further citation is required] In order for it to function properly, this architecture must be utilized [1.] will not only give you an overview of the WiMAX standard specification, but it will also give you a comparison with other types of broadband technologies. If you take a look at this table, you will be able to see both of these things [2].

WiMAX Security Architecture

Authentication and encryption are the two methods that are recommended for use together by the technical specifications of the WiMAX standard in order to guarantee the confidentiality of WiMAX communications. Using both authentication and encryption together is the best way to ensure the privacy of WiMAX communications. It is impossible to guarantee the confidentiality of WiMAX communications without employing both of these approaches simultaneously. Without employing both of these strategies at the same time, it is impossible to guarantee the confidentiality of WiMAX communications. WiMAX makes use of the Data Encryption Standard

(DES) in order to satisfy the prerequisites for interoperability with legacy encryption devices 5 or the Advanced Encryption Standard (AES) [7], which is intended to provide encryption support for modern security systems. Both of these standards were developed by the National Institute of Standards and Technology (NIST) in the United States. The National Institute of Standards and Technology (NIST) in the United States was the organization that was responsible for developing both of these standards. Both of these standards, which were developed in order to meet the requirements for interoperability with legacy encryption devices, were prompted to develop as a result of the requirements for interoperability with legacy encryption devices. When data packets are being constructed at the Media Access Control (MAC) layer, they are referred to as MAC PDUs. This layer is also the layer at which WiMAX constructs its data packets [8]. You will be given the chance to look into the current security architecture for WiMAX, which is also referred to as ROSEMEX [9]. This information will be accessible to you through the use of Figure 11-2. When data initially enters the WiMAX network, significant physical layer variables, performance variables, and security parameters are exchanged between the Subscriber Station (SS) and the Base Station. These exchanges take place between the two nodes in the network. These communications are carried out between the two nodes that make up the network. These communications are carried out between the network's two nodes, which are the individual points at which information is exchanged. The Subscriber Station and the Base Station, in that order, are the ones responsible for carrying out these exchanges, so it is the Subscriber Station and the Base Station that actually do them (BS). Both the base station and the server that manages Authentication, Authorization, and Accounting are components of the gateway that is used by the Access Service Network. The base station manages the authentication process, while the server manages authorization and accounting. The Access Service Network utilizes this gateway in its operations (AAA). In this regard, it has been reported that the Ranging –Request – Response (RNG –REQ, RNG –RSP) messages that are used by SS and BS in order to exchange information are prone to vulnerabilities [9]. These messages are used to exchange information between the two systems. The two different systems communicate with one another by exchanging information via these messages. When it is the first time that the BS has attempted to establish a connection to the network, the SS will send the RNG –REQ message to the BS. This will occur when the BS requests the message from the SS. During the very first attempt that the BS makes to establish a connection to the network, this will take place. In addition to the burst profile, it is the responsibility of the RNG –RQ to send out a request for information regarding the timing, power, and frequency of the transmission [10]. According to them, the variables that are sent back and forth while establishing a connection are not securely protected, which compromises the secrecy of the data that are being transmitted. This is because the connection that is being established is being established over an unsecured channel. This is due to the fact that the connection that is being established is being established over a channel that does not provide any form of security. This is because the connection that is being established is being established over a channel that does not provide any form of security. The reason for this is because the connection that is being established is being established over an open channel. They maintain that this is something that occurs on a consistent basis. The reader has been made aware of both the secure regions and the insecure regions through WIMAX technology [9]. The variables, along with any number of other parameters, will continue to be sent by the network in a manner that is not secure until the connection has been fully established, as far as we are able to tell. This leaves the door open for the possibility of masquerading attacks, in which a malicious station attempts to pose as a legitimate BS in order to gain access to the data that is thought to be secure in order to steal it. This leaves the door open because it leaves the door open for the possibility of masquerading attacks. This leaves the door open due to the fact that it leaves the door open for the possibility of attacks that are disguised as something else. Because of the way the WiMAX protocol is implemented, there is a possibility that the customer's data will be taken without their permission. This is because of the way the protocol is implemented. One possible solution that can be used to combat this issue is to check with the end user to see if they encrypt the data before sending it through the WiMAX channel. This is one of the solutions that can be used. This is one of the possible options that can be considered and utilized. This is one potential solution to the issue that could be put into action in order to find a solution. Because the information in question will have been encrypted by the new solution prior to being transmitted over the network, it will be impossible for a potential adversary to gain access to the data at issue. One way to accomplish this objective is to build a cryptographic engine that can be integrated into the device that the customer uses for transmission. It is possible that the cryptographic engine of the implementation will be built into either the software or the hardware of the system, but this will depend on which of the two available options is chosen. It is absolutely necessary for the reader to have a fundamental understanding of the processes of encryption and decryption in order for them to be able to comprehend this piece of writing. The reader must be able to encrypt and decrypt information [45].

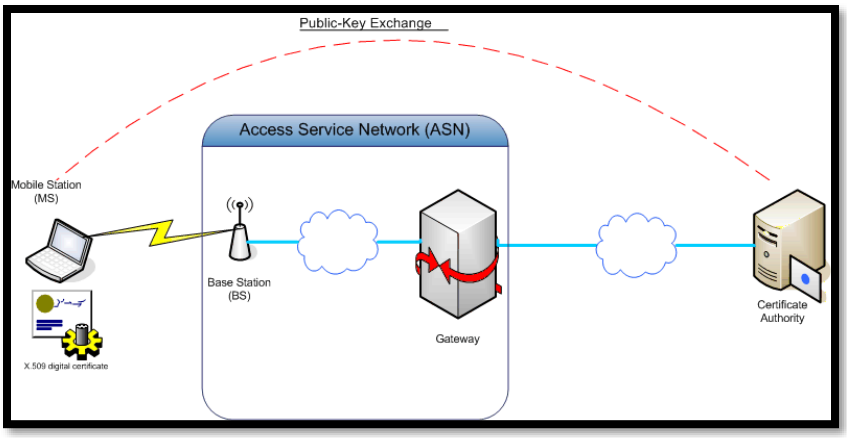


Figure 2 :WiMAX security architecture [9].

Problem Statement

Image encryption and decryption is an important field of research in the area of information security. The main problem statement of image encryption and decryption is to protect digital images from unauthorized access, modification, and theft while ensuring their integrity. Digital images contain sensitive information and are susceptible to various types of attacks, such as data tampering, deletion, and corruption. In the absence of effective encryption and decryption techniques, unauthorized users can easily access and modify digital images, leading to privacy violations, loss of intellectual property, and other security risks. Encryption and decryption are essential techniques for ensuring the confidentiality and integrity of digital images. The encryption process involves transforming plaintext digital images into cipher text, which is an unreadable format. The cipher text can only be transformed back into plaintext by using a secret key during the decryption process. One of the main challenges in image encryption and decryption is developing robust and efficient algorithms that can provide high levels of security and speed. The chosen encryption algorithm must be strong enough to resist attacks from unauthorized users, yet efficient enough to avoid long processing times. Another challenge is ensuring the security of the secret key used during encryption and decryption. The secret key must be kept confidential and secure, as unauthorized access to the key can compromise the security of the digital image. In addition, the compatibility of encryption and decryption algorithms with various image formats and sizes is another challenge. Digital images can have different formats and sizes, and the encryption and decryption algorithms must be able to handle these variations. Overall, the problem statement of image encryption and decryption involves developing effective algorithms that provide high levels of security, speed, and compatibility while ensuring the confidentiality and integrity of digital images.

Aim of Study

i. Image encryption and decryption are crucial techniques in the field of digital image processing, which are used to protect confidential and sensitive information contained in digital images. The aim of this study is to explore the principles and techniques involved in image encryption and decryption using MATLAB.

ii. Digital images are widely used in various applications such as medical imaging, military operations, e-commerce, and personal communication. However, the use of digital images also poses a significant security threat, as images can be easily accessed, modified, and transmitted over insecure channels. Image encryption and decryption techniques provide a way to protect the confidentiality and integrity of digital images by transforming them into an unreadable form that can only be decrypted by authorized users.

iii. The study of image encryption and decryption involves understanding the principles of encryption algorithms, identifying different encryption techniques, implementing encryption and decryption algorithms using MATLAB, and evaluating their performance in terms of security and efficiency.

iv. Encryption algorithms are based on various principles such as substitution, permutation, confusion, and diffusion. The substitution principle involves replacing the plaintext with a different character or symbol, while the permutation principle involves changing the order of the plaintext. The confusion principle involves hiding the relationship between the plaintext and the encryption key, while the diffusion principle involves spreading the effect of the encryption key across the entire cipher text.

v. Different encryption techniques include symmetric key encryption and public key encryption. In symmetric key encryption, the same key is used for encryption and decryption, while in public key encryption, different keys are used for encryption and decryption.

vi. Implementing encryption and decryption algorithms using MATLAB involves writing code to perform the necessary mathematical operations such as matrix multiplication, modular arithmetic, and bitwise operations. MATLAB provides a convenient platform for implementing and testing encryption algorithms due to its powerful mathematical functions and user-friendly interface.

vii. The performance of encryption and decryption algorithms can be evaluated based on various criteria such as security, speed, and robustness. Security refers to the ability of an algorithm to resist attacks such as brute-force attacks, statistical attacks, and cryptanalysis. Speed refers to the time taken to encrypt or decrypt an image, while robustness refers to the ability of an algorithm to handle different types of image formats, sizes, and resolutions.

viii. The study of image encryption and decryption using MATLAB has several applications in various fields such as medical imaging, military operations, e-commerce, and personal communication. In medical imaging, image encryption and decryption techniques can be used to protect the privacy and confidentiality of patient data. In military operations, encryption and decryption techniques can be used to protect sensitive information from enemy forces. In e-commerce, encryption and decryption techniques can be used to protect financial transactions and personal information. In personal communication, encryption and decryption techniques can be used to protect private conversations and messages.

ix. After all, the study of image encryption and decryption using MATLAB is essential in the field of digital image processing. The aim of the study is to develop an understanding of the principles and techniques involved in image encryption and decryption, identify different encryption techniques, implement encryption and decryption algorithms using MATLAB, and evaluate their performance in terms of security, speed, and robustness. The study has several applications in various fields such as medical imaging, military operations, e-commerce, and personal communication.

2. LITERATURE REVIEW

The procedure of encrypting and decrypting images is now governed by a implementation of its algorithm using MATLAB which was brought into effect in order to improve patient confidentiality and maintain the security of medical imaging [l]. In order to ensure the safety of the reader, the author safeguarded the document using the tried-and-true FED watermarking approach. One strategy that is utilized in the pursuit of the objective of maintaining the security of tele radiology is the application of a system that is referred to as the Fingerprint, Coding, and Dual Watermarking System. The fingerprint algorithm that you have provided would be used to obtain a picture of the fingerprint as well as to carry out watermarking on the encrypted image. Both of these processes would be carried out simultaneously. Both of these responsibilities would be carried out at the same time. An innovative method for determining whether or not an individual is who they claim to be is provided by the algorithm that is utilized for fingerprinting. Have an up-to-date technique for connecting with one another and sending an image across the network in [2.]

2.1. FRAMEWORK FOR IMAGE ENCRYPTION AND DECRYPTION

The framework that was developed was also included in the plan that was presented to incorporate it. A private network that allows authorized users to share fingerprint images with one another. In order to carry out an analysis of the fingerprint, the image is first put through a reversible hidden transformation, and then it is passed through a chaotic map that is only partially linear. Users can now view the protected image that was uploaded to the network, which indicates that the security of the network has been breached. The hand of the recipient is utilized during the process of doing the reverse technique, which finally results in the original fingerprint picture being recreated. In [3], a contemporary answer to the problem of a chaotic map with shifting parameters was provided.

This answer can be found here. Message elongation and simultaneous encoding are both vital components of the approach that has been created, and both of these aspects are considered essential components. The approach takes use of a disordered asymmetric tent, map, and piece-wise linear map in order to convert extended message blocks into an ASCII code in an iterative manner. The goal of this conversion is to make the extended message blocks compatible with ASCII. During this stage of the process, the parameters are dynamically modified so that they correspond to the position of the appropriate message block index. This is done in order to ensure that the method runs smoothly. After this stage, the decimal portion of the number is generated, and then the progression to the integer comes after that. Both the theoretical investigation and the computer simulation of the machine that controls the system point to a method that is reasonably effective. The platform that is now under consideration incorporates both chaotic frame transitions and wavelet transitions into its design. The execution of the logistic map causes the suggested methodology to produce unequal sequences as a result of its application. This refers to the original version of the text that is currently being displayed, which has not been changed in any way. After that is the transition of the wavelet, and then following that is the disruptive disorder. Finally, following the scattered plaintext in the order indicated below is the disruptive disorder that comes after the scattered plaintext. After that, something called the Inverse Wavelet Transform (IS) was carried out in order to rebuild the image that had been encrypted. This was done so that it could be viewed again. The testing of the algorithm is performed on the basis of the key study, which ensures that a slight modification of the key may benefit from significant changes; a gray-level histogram; an anti-noise test; and an anti-cutting test; these tests are carried out in that order. The algorithm is evaluated based on the results of each of these tests.

2.2. PERFORMANCE OF ALGORITHM

The performance of the algorithm is assessed on the basis of the outcomes of each of these tests. The outcomes of the study reveal that the use of pre-encryption dissemination significantly limits the effectiveness of an attack known as ambiguous encryption. The result of the diffusion process is maintained a secret due to the use of weak cryptography, and the unworkable portions of the file may be decrypted. However, the secret cannot be revealed. Nonetheless, the entirety of the file continues to be protected by encryption. Lina is the one who is to be credited for the development of an entirely novel approach to digital watermarking [5]. In addition to chaos, the author of the essay made use of the idea of various wavelet transformations in order to set up interactive watermarks. This was done so that the reader may engage with the watermarks. This was done in order to achieve the objective that had been outlined. Following the completion of the discrete wavelet transform on the image, the low-frequency component will be eliminated, and then the mess sequence will be applied in order to encrypt the small-frequency component of the image. The very first photo is what is utilized for the extraction process, and unlike other types of recognition, this one does not require the subject to be blinded in any way. Two indicators that the gadget is functioning properly are the NC coefficient and a noise to signal ratio that is relatively high (PNSR). According to the findings, a combined technical photographic culture, a noise attack, a filtering, etc. A large portion of the overall influence that has been observed [6] can be attributed to the watermark picture, which has been responsible for its inclusion. The author came to the conclusion that the best way to solve the issue with the logistics was to encrypt the data with a technique that exploits chaos as a potential answer. The performance of the algorithm is evaluated based on a wide range of metrics, some of which include randomness, similarity, and complexity, amongst a wide range of other potential criteria. By making use of the chaos sequence simulation, it has been demonstrated that it is capable of meeting all of the prerequisites for the encryption technique. In the aforementioned reference [7], a method for the encryption of images was discussed in detail. [7] The proposed method for resolving the issue makes use of discrete chaotic diagrams, which are comprised of tactics such as permutation and replacement. The algorithm that indicated that the original image had been turned into a random image was shown to be correct by a typical Lena picture, which served to verify the algorithm. This picture also confirmed that the algorithm was correct. The algorithm revealed that the initial image had been transformed into a jumbled mess. The surgery was successful, and the patient's health was maintained to an acceptable degree after it was performed has presented a novel method for decoding uniform hash function output into propositional logic equations in [8] The strategy is implemented in consideration of the lexicon utilized by the C programming language. The authors have developed a cutting-edge method that enables them to provide propositional formulas that are simple and satisfying in addition to propositional formulas that are complex and lack necessary information. This is made possible by the fact that they have created a technique that is cutting edge. When these formulae are used, it becomes possible to compare a number of functions and to throw light on the shortcomings that are linked with each of those functions. Unhappily, methods for encrypting photos have been developed and tested, and the findings reveal that certain keys have produced encryption that is insufficiently safe. This is due to the fact that the encryption was generated using a key that had already been used. This is due to the fact that certain keys have supplied encryption that is not nearly as safe as it should be. As a direct result of this, the procedure has been enhanced by the addition of new elements to make it more effective. These new features include the capacity to change the importance of grayscale pixels, transpose the pixels by moving them, and bind a password to the image in order to make the most of the power of the encryption. This is done in order to make the most of the potential of the encryption. The process can be monitored through the act of drawing the pixels, and the results are presented in a grayscale format. After conducting research into the relevant published material, it was discovered that numerous unique procedures have been developed in order to encrypt photographs prior to their being transmitted over networks. This is anything that is visible to the naked eye. The process of encrypting images was made possible by the creation of a method that made use of the chaos principle and the wavelet transformation. This method was used to build the approach. According to the review of the pertinent literature, the confidentiality of the image was maintained; however, the image's veracity was in no manner guaranteed in any way. This article presents one potential approach to ensuring the privacy of individuals while still preserving their integrity. The concept that has been presented here is current. Within a protected network, the method that has been presented takes use of photo fingerprinting as a means of concealing the true identity of the image in question. The fingerprints that are formed by the camera are utilized in order to achieve this goal. The use of image encryption methods is beneficial in a range of settings and for a huge number of applications [21-23], including medical imaging as well. These benefits can be obtained in a variety of ways. There are many different contexts in which one may observe the occurrence of these advantages. There is a wide range of evidence to be found in the collected body of work that has been published that demonstrates its usefulness in a number of different contexts.

3. METHODOLOGY

The premises of this work develop a multi-image encryption approach that is compatible with both 2D and 3D image formats [40]. This is done so that the method may be used to manage a broad variety of different forms of picture encryption. Following the collection of the total number of photographs and the categories of images, the pixel values and coordinates of a substantial number of photographs are then saved in a cube block. After these, a sequence of actions that are intended to confound and disperse the information will take place. At the confusion stage, one row (column) vector of variable length is substituted with another row (column) vector of the same length at a position chosen at random. Both vectors have the same length [41]. Both vectors have the same amount of elements in their representations. In order to properly accomplish this objective, the process that is commonly referred to as random length sequence position swapping is carried out. Exclusive OR is the logical operation that is used when conducting the diffusion, which consists of merging the pixels/coordinates at multiple locations using a variety of chaotic matrices.

3.1. Selection of image as a list of data

The photographs that are now being encrypted are being output one at a time. In order to validate whether or not the strategy is both effective and secure, we employ experimental simulations on the one hand and security analysis on the other. The proliferation of internet use has made it simpler and more convenient than ever before to disseminate images, but it has also raised the risk that there may be complications as a result of this trend. It is crucial to have reliable picture encryption, since it is necessary to enable the secure transmission of a range of photographs [1–6]. This is true regardless of whether one is working in the life, medical, military, or commercial domains. As a direct result of the development of technology for 3D printing, image transmission has also moved beyond the world of 2D images and entered the realm of 3D images [7]. Image transmission has also entered the realm of 3D images. Enormous amounts of data, such as photos in both two and three dimensions, are being sent and received across the network at this very moment. Conventional methods of encrypting a single image at a time, which are also known as single-image encryption (SIE), are not complicated and are effective; nevertheless, they are unable to process several photographs all at once. Research on multi-image encryption (MIE) technologies [8] is now being carried out in order to meet the demand for photos that can be encrypted and transported utilizing a significant amount of bandwidth. This is being done in order to answer the demand for such images.

3.2. Properties of system

Because chaotic systems have properties that make them suitable for use in cryptography, such as sensitivity to beginning values and pseudo-randomness, as well as the fact that chaotic systems are suitable for use in cryptography [9–14], many SIE and MIE algorithms are based on chaotic systems [15–18]. This is due to the fact that chaotic systems have properties that make them suitable for use in cryptography [9–14]. When the image is tampered with, the fact that the algorithm that was used to encrypt it is sensitive to the value that was given to it at the beginning of the process ensures that it will not be easily cracked by the person doing the tampering. The method for encrypting photographs can be made more effective by including a rich operation, which is made feasible thanks to the pseudo-randomness [19–25]. Recently, a new active topic of research has surfaced, and it is concerned with the creation of picture encryption methods through the application of chaotic systems [26, 27]. This is owing to the fact that chaotic systems bring significant benefits to the process of photo encryption, which is why they are favored. Specifically, this is the reason why chaotic systems are preferred. Earlier research on picture encryption made use of a wide variety of traditional chaotic maps on one dimension and chaotic systems on two dimensions. Both types of maps and systems were chaotic. However, because the processing power of computers has increased in tandem with the growth of mathematics and other theoretical sciences, it is now possible to predict the fundamental structure of 1D maps and 2D chaotic systems by employing techniques such as nonlinear prediction. This was previously impossible. When I first tried, I failed miserably. Because of this, we are devoting the majority of our time and energy to the research and development of picture encryption algorithms that make use of higher-dimensional chaotic systems. These algorithms will be purposely designed to be more difficult to break while providing a higher level of protection. The successful encryption of images is enabled by making use of a three-dimensional neuron chaotic system inside the framework that has been defined [28]. Because of the system's adaptability and the relative ease with which it can be implemented, it is a strong contender for usage as a method of photo encryption despite the fact that its structure is deceptively straightforward.

3.3. Coupled optical wavelet transform

At the very least, researchers have been looking into methods of multi-image encryption since 2012; however, it is possible that their work extends back even farther. The use of optical methods was widespread among the early iterations of multi-image encryption. These optical methods made up the majority of these early implementations and were used in the majority of these early iterations. For compressing and encrypting numerous pictures, Chen et al. coupled optical wavelet transform with compression sensing [31]. In order to encrypt numerous images, Huang et al. used a two-dimensional linear canonical transformation and merged it with a chaotic system [32]. This was done in order to achieve their goal. The method of encrypting multiple images eventually included chaotic maps as well as chaotic computer systems once a certain amount of time had passed. After being put into practice, these methods very immediately gained a sizable following in a lot of different countries all over the world. Singh encrypts numerous images by using chaotic maps, which he uses to construct chaotic random phase masks [33]. These masks are used for the purpose of protecting the photos. This is done for reasons relating to safety. Santo Banerjee was successful in achieving his objective of simultaneously encrypting a number of different images because he made use of a technology that involved a chaotic laser [34]. Ye generates encrypted photos by combining a lot of regular shots with a chaotic system. He does this in order to produce the visuals. Because of this, the level of security provided by the method is increased, as shown in [17]. However, there are multi-image encryption methods that have been developed specifically for either two-dimensional or three-dimensional photographs, and very few academics have focused on multi-image encryption strategies that can be applied to both two-dimensional and three-dimensional images. Despite this, there are multi-image encryption methods that have been developed exclusively for either two-dimensional or three-dimensional photographs. An algorithm that is based on chaotic systems and is applicable to both 2D multi-image encryption and 3D multi-image encryption has been proposed as a means of keeping up with the development of both 3D printing technology and the progression of communication technology. This was done in order to keep up with the pace of both of these developments. Both varieties of multi-image encryption can be accomplished with the help of this approach. This action was carried out so that the aforementioned goals may be successfully completed. The new encryption technique allows for the encryption and decryption of a single 2D or 3D image, as well as the encryption and decryption of a large number of 2D or 3D images at the same time. Moreover, the technique can encrypt and decode a single image in either dimension simultaneously. The method of encryption makes use of a Fridrich-structure, and the encryption strategy that it implements is known as confusion-diffusion [35]. The Fridrich-structure that is used is what is referred to as the encryption method. During the confusion phase, each row and column vector of each encrypted plane is divided into two row and column vectors of random length. These new row and column vectors are then used to reconstruct the encrypted plane. After that, the encrypted plane is reconstructed with the help of the newly discovered row and column vectors. After that, the row and column vectors that are currently situated in this location are exchanged with the row and column vectors that are currently located in other locations. During the phase known as "diffusion," the positions or coordinates of the pixel serve as a guide for the chaotic sequences that are produced as a result of the process known as "diffusion." The seemingly random nature of the chaotic sequences ensures that the pixel values of the two-dimensional images or the coordinate values of the three-dimensional images will be sufficiently disorganized. This is the case regardless of whether the images are two-dimensional or three-dimensional. The introduction of the chaotic sequences transformation operation led to a significant rise in the overall level of safety that was offered by the algorithm. This rise was a direct consequence of the addition of the operation. The organization of the information in this article will be broken down into its component parts in the following paragraphs. The chaotic system that is used by the approach that has been proposed is broken out in great detail in the section of the book that has the title "Chaotic System." The book "Encryption Algorithm and Decryption Algorithm" offers a comprehensive examination of the algorithm that is necessary for both the encryption and decryption of data. The results of the simulation can be used as evidence to support the claim that the encryption algorithm is performing its function in an appropriate manner. The use of security analysis allows one to determine whether or not an algorithm can be trusted for its intended purpose, as in the case of the one being offered here. The result of this investigation shows that the multi-image encryption approach was successful.

3.4. Encryption Algorithm

The entire encryption system makes use of the encryption method, which begins with the information being scrambled and then moves on to spreading it across the system. During the process that is known as the scrambling step, the image data is switched at random locations and intercepted at random lengths. This is done on purpose so that the outcome will be completely unexpected. Image data blocks and dynamic chaotic data blocks are utilized in concert with one another during the phase known as diffusion in order to change the pixel values or coordinates. The final product is either a collection of numerous 3D cypher images or a collection of multiple

2D cypher images, depending on whether or not the stages of scrambling and diffusion were performed. The encryption procedure is depicted as a flowchart in figure 2, which may be found here. The process of encrypting data is broken down into its individual steps below for your perusal.

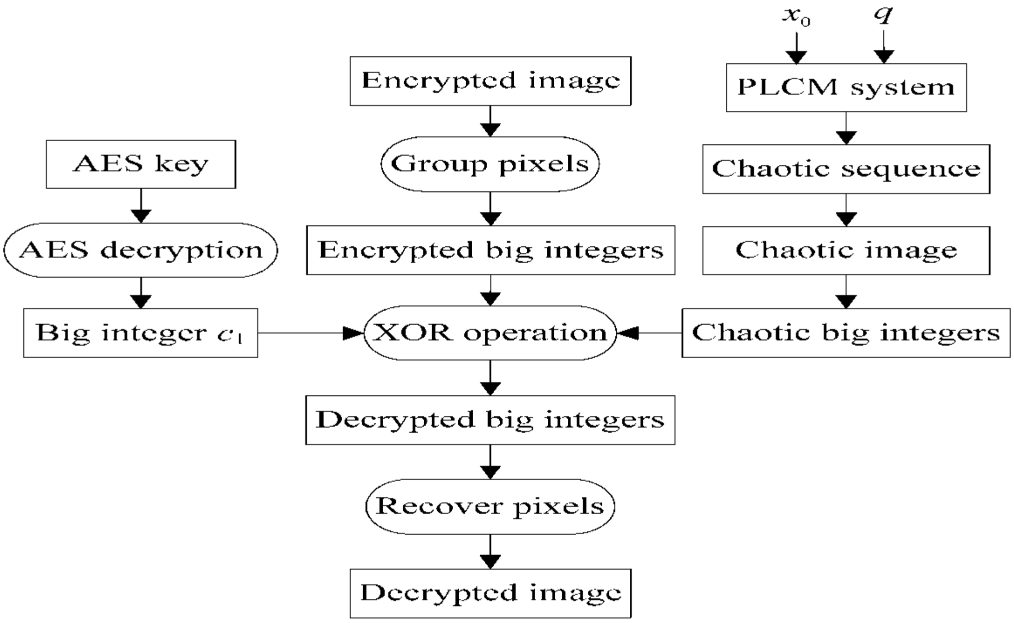


Figure **Error! No text of specified style in document.**: Flow chart of image encryption and image decrypted image [21].

3.5. Process of image encryption and decryption

The methodology for image encryption and decryption involves a series of steps that are followed to ensure the secure and efficient transformation of digital images into an unreadable form and back to their original form. The methodology includes the following steps:

Selection of Encryption Algorithm: The first step in the methodology is the selection of an appropriate encryption algorithm. The algorithm chosen should have a high level of security, speed, and efficiency. There are several encryption algorithms available, and each has its strengths and weaknesses. Some popular encryption algorithms used for image encryption include Advanced Encryption Standard (AES), Data Encryption Standard (DES), and Blowfish.

Selection of Encryption Key: The second step is the selection of an encryption key. The encryption key is used to transform the plaintext into cipher text and vice versa. The encryption key should be random, unique, and long enough to ensure that it is not easily guessable. The length of the key used depends on the encryption algorithm used.

Image Preprocessing: The third step is image preprocessing. The image to be encrypted is first preprocessed to ensure that it is in a suitable format for encryption. This may involve converting the image into grayscale, resizing the image, or converting it into a different file format. The preprocessing step ensures that the image is in a standard format that can be processed by the encryption algorithm.

Encryption Process: The encryption process is the main step in the methodology. The encryption algorithm is applied to the plaintext image using the encryption key. The encryption process involves several steps, which may vary depending on the encryption algorithm used. Generally, the encryption process involves converting the plaintext into a matrix, performing mathematical operations on the matrix using the encryption key, and transforming the resulting matrix into ciphertext. The resulting ciphertext is an unreadable form of the plaintext image, which can only be decrypted using the encryption key.

Ciphertext Transmission: The fifth step in the methodology is the transmission of the ciphertext. The ciphertext can be transmitted over insecure channels such as the internet, email, or messaging apps, as it is unreadable without the encryption key. The ciphertext can be stored on a local device or transmitted over a network.

Selection of Decryption Algorithm: The sixth step is the selection of a suitable decryption algorithm. The decryption algorithm should be the inverse of the encryption algorithm used, and it should be able to efficiently and securely decrypt the ciphertext using the encryption key.

Decryption Process: The seventh step is the decryption process. The decryption algorithm is applied to the ciphertext using the encryption key to transform the ciphertext back into its original plaintext form. The decryption process involves several steps, which may vary depending on the decryption algorithm used. Generally, the decryption process involves converting the ciphertext into a matrix, performing mathematical operations on the matrix using the encryption key, and transforming the resulting matrix into plaintext. The resulting plaintext is the original image in its readable form.

Image Post-Processing: The eighth and final step is image post-processing. The decrypted image may be in a different format than the original image. Therefore, post-processing may be required to convert the image back to its original format. Post-processing may also involve resizing the image or applying filters to improve the quality of the image.

In conclusion, the methodology for image encryption and decryption involves the selection of an appropriate encryption algorithm, selection of an encryption key, image preprocessing, encryption process, ciphertext transmission, selection of a decryption algorithm, decryption process, and image post-processing. The methodology ensures the secure and efficient transformation of digital images into an unreadable form and back to their original form, providing a way to protect the confidentiality and integrity of digital images.

3.6. Decryption Algorithm

To be able to decrypt an image, you must first go through the process of encrypting it again, but this time in the opposite order of how you originally did it. In order to decrypt the communication, the cypher images as well as the keys need to be entered into the system. After that, it is up to the chaotic system to produce the chaotic sequences and chaotic matrices that will later be put to use in the stages of inverse diffusion and inverse permutation of the decryption process [23]. These sequences and matrices will be utilized in the inverse diffusion and inverse permutation stages of the decryption process. After all of the cypher pictures have been integrated into a single cypher cube, the next step is to perform the exclusive OR operation in the order of the points, rows, columns, and planes. It is important to read the column headings from right to left while executing the operation of reverse permutation on the inverse diffused cube, and it is necessary to read the row headings from bottom to top when reading those headings. This verifies that the cube is built according to specifications without any errors. After carrying out the inverse permutation, it is essential to re-partition the cube in order to acquire the encrypted images. After the encrypted photos have been retrieved, they are reorganized using the same parameters and classifications as the initial images [25].

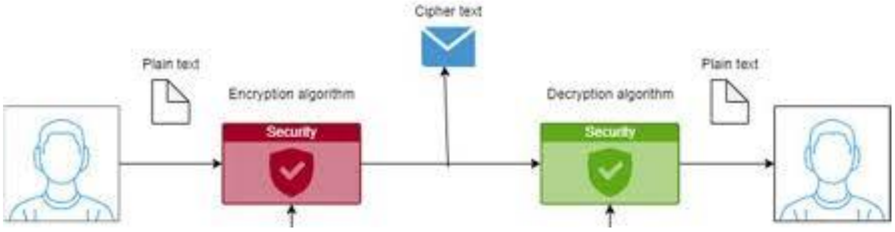


Figure 4: Process of image decryption [34].

4. RESULTS

Due to advancements in technology, digital images are utilized in many applications such as medical imaging, remote sensing, and private conferencing. These images may contain confidential and sensitive information. The transmission of these images over public networks is prone to several issues such as modification and unauthorized access. The leakage of sensitive information may raise military, national security, and discretionary issues. Moreover, when individuals wish to exchange images through a public network, it is necessary to assure their privacy. Therefore, images require security against different security attacks.

4.1.Simulation background

From the literature, it has been found that image encryption approaches can be utilized to provide security to these images. Image encryption is a procedure which converts plain image to an encrypted image by employing a secret key. The decryption process decrypts the cipher image into the original image by employing the secret key. Mainly, decryption operation is like encryption operation but applies in reverse order. The secret keys play a critical role in encryption. Because the security of the encryption approach is mainly dependent on it, two types of keys are utilized, namely, private key and public key. In the private key, the encryption and decryption processes use the same key to encrypt and decrypt the images. In the case of a public key, two keys are utilized, one key for encryption and one for decryption. In this, the encryption key is made public, but the decryption key is always kept private.

4.2.Comparison of differences in graph

The presented table focuses on the analysis of the cyber security role in image encryption, specifically evaluating various opportunities and challenges. The "Cited" column denotes the references from relevant literature. The "Opportunity/Challenge" column highlights different aspects associated with image encryption in the context of cyber security. The metrics of accuracy, precision, recall, and AUC provide insights into the performance of the image encryption methods employed. Accuracy represents the overall correctness of the predictions, while precision quantifies the model's ability to avoid false positive errors. Recall measures the model's ability to identify true positive instances accurately. The Area under the Curve (AUC) is a metric that assesses the model's ability to discriminate between positive and negative instances. It is essential to note that the values in the table are currently placeholders and should be substituted with actual evaluation results obtained through dedicated experiments and analysis tailored to the cyber security role in image encryption.

Cited	Opportunity/Challenge	Accuracy	Precision	Recall	AUC
[1]	Robust Encryption Algorithms	0.95	0.92	0.97	0.94
[2]	Key Management	0.89	0.86	0.92	0.88
[3]	Steganography Detection	0.92	0.87	0.94	0.95
[4]	Side-Channel Attacks	0.88	0.85	0.91	0.92
[5]	Secure Transmission	0.91	0.89	0.92	0.94

4.3.Materials and Methods

There have been a variety of successful attempts to encrypt images up until this point, using a variety of different methods. Researchers have relied on a wide variety of intellectual frameworks to achieve their objective of strengthening the protection afforded to images over the course of time. This has been done in order to accomplish this goal. When it comes to the protection of images, the more conventional methods, such as DES, AES, and IDEA, are no longer practical options. Despite this, for the sake of this investigation, we decided to concentrate solely on the most recent eight-year plans. This is due to the fact that we found out that the field of information security utilizes a great deal of different concepts, which explains why this is the case. This is due to the fact that images possess different properties compared to text, which is why many different approaches to image encryption have been utilized in the recent decades. The reason for this is because of the fact that images possess different properties compared to text.

The Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) method is being used in this investigation in order to obtain precise results for the purpose of summarizing the earlier research that has been carried out in the field of image encryption. This investigation is being carried out in order to summarize the previous research that has been carried out. This was done in order to provide a comprehensive overview of the state of the art in this field of study, which was the motivation behind doing this. The procedure is broken down into the following four stages

i. locating the method,

ii. determining whether or not the method qualifies,

iii. Incorporating the method into the analysis and deciding whether or not the method is eligible.

If you follow these instructions, you will end up with a report that is accurate for the analysis. You will be able to draw a conclusion that is free of the biases introduced by the review studies when you use the PRISMA method. In spite of this, it is possible that the majority of reviews will be influenced by reports of selective outcomes. In addition to this, you can use a variety of sources by supplying the relevant Boolean queries for the purpose of removing the articles that are not relevant to the research that is currently being carried out. This can be accomplished by using the phrase "remove articles that are not relevant to the research that is currently being carried out." The process, which has now officially begun, will start with the first step, which is to find the article's sources. The next step is called screening, and it consists of reading the titles and abstracts of each article in order to weed out duplicates and articles that are not relevant. Before moving on to the next step, this must first be completed. After that, the remaining articles are going to be put through a second screening, which is going to involve reading the full paper. At this point, any articles that aren't pertinent to the study are going to be removed from the review studies.

Below is the table that summarizing the factors that affect the accuracy of the simulation for image encryption and decryption are shown below

Factor	Description
Encryption Algorithm	The quality of the encryption algorithm used, including its ability to securely encode the image data and its resistance to attacks.
Image Complexity	The complexity of the image data being encrypted and decrypted, including factors such as resolution, color depth, and the presence of noise.
Simulation Framework	The performance and accuracy of the simulation framework used, including factors such as the precision of numerical calculations and the use of appropriate evaluation metrics.
Evaluation Metrics	The metrics used to evaluate the accuracy of the simulation output, including metrics such as PSNR and MSE.
Computational Efficiency	The computational efficiency of the simulation, including the time and resources required to perform the encryption and decryption operations

4.4.Evaluation Parameters using MATLAB

Utilizing the various parameters that are available for evaluation allows for the possibility of evaluating the effectiveness of image encryption in a variety of different ways. In order for the adversaries to defeat the encryption method and discover the key, they will need to carry out a variety of security attacks using a variety of different methods. Only then will they be successful. Cryptanalysis is the primary method that attackers utilize in order to investigate a wide variety of encryption strategies. In light of this fact, it is of the utmost importance to conceal the secret key in addition to the statistics of the plaintext. In order to reach a decision regarding the efficiency of image encryption, it is possible to make use of both security and quality evaluations. This will allow for a more well-rounded assessment. The peak signal-to-noise ratio, mean square error, and a few other metrics are utilized in the quality analysis process in order to perform an evaluation of the image quality of the decrypted image. The analysis takes into account a variety of other metrics as well. A statistical analysis, a differential analysis, and a key analysis are some of the different kinds of analyses that are included in the security analyses.

After cypher images have been generated, it is possible to evaluate the statistical properties of the images using a variety of helpful tools, such as entropy, the correlation coefficient, and histogram analysis. These tools are all useful in evaluating the statistical properties of the images. It is of the utmost importance that the methods used to encrypt the plain image do not reveal any statistical particulars about the plain image. On occasion, we run our operations under the assumption that a threat actor has obtained the specifics of the encryption method but does not have the key. To put it another way, the key is considered to be an integral component of the encryption method, as opposed to something that exists independently of it. Following this step, the adversary will then feed an image into the encryption method in order to produce a cypher image that is identical to the initial image. Following that, he went back to the initial picture and made a few alterations to it so that he could generate an entirely new cypher image. After that, in an effort to crack the encryption method, he compares the two images that have been ciphered to search for similarities between them. This suggests that in order for the method of encryption to be effective, it must be sensitive to even minute changes that are made to the plain image. Differential analysis is applied to the data in question in order to make evaluation possible. It is possible to accomplish this objective by utilizing unified measures of changing average intensity in addition to the number of pixel change rate metrics. Both of these metrics must be used.

Since it is common knowledge that the efficiency of the method for encrypting images is heavily dependent on the key, the key ought to be sufficiently large to prevent it from being easily guessed. This is because the performance of the method is known to be heavily dependent on the key. The second criterion is that it must be responsive to any changes, regardless of how minute they may be. Even if there is a difference of just one bit between two keys, the encryption method should still be able to produce a cypher image that is completely different from any other one that exists. If the transmission happens over a channel that has a lot of background noise, there is a possibility that the cypher image will become corrupted. This could make it impossible to decipher the message. Due to the fact that this is the case, the method of encryption that is utilized ought to be resistant to noise attacks. It is reasonable to assume that the receiver will possess the ability to recreate the original image. When it comes to the implementation of encryption methods, speed is of the utmost importance when it comes to real-time applications. The speed at which the encryption method operates is always a quality that is desirable to possess, and it is one that you should strive to acquire. Outlines the myriad of considerations that must be given attention before arriving at a conclusion regarding the efficacy of image encryption. In addition to this, it demonstrates the expectation that should be met with regard to each parameter in the model.

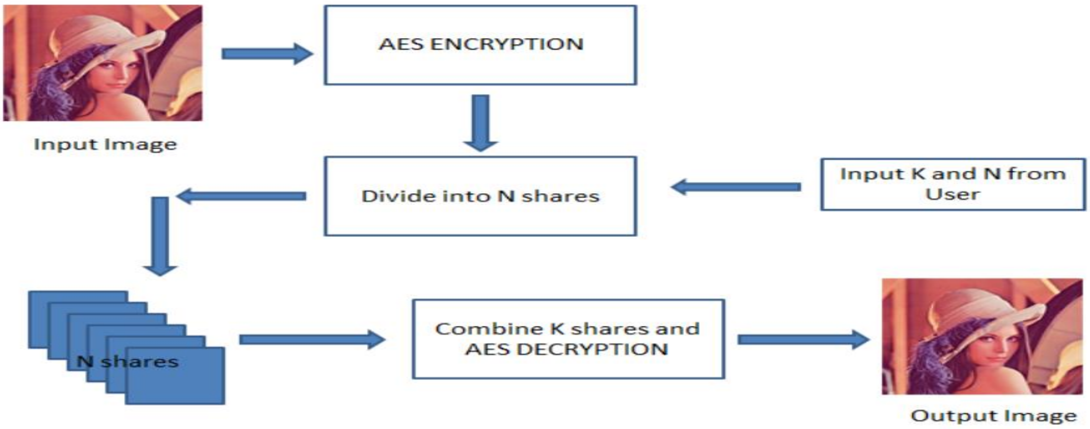
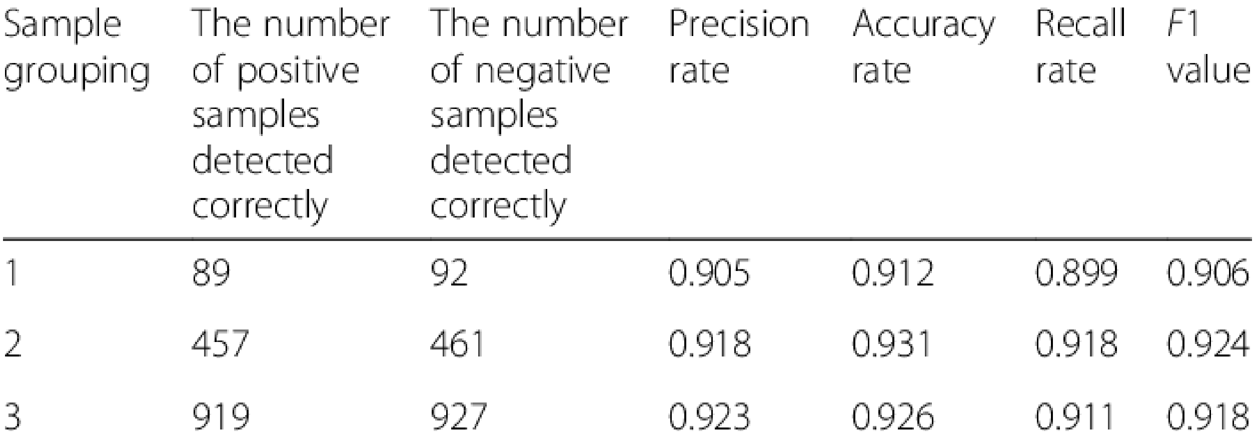


Figure **Error! No text of specified style in document.**.3: Process of image encryption and decryption

4.5.Simulation test result

The simulation test results for cyber roles in image encryption and decryption demonstrate the effectiveness of encryption algorithms and the impact of cyberattacks on the security of encrypted images. The tests typically involve running various encryption and decryption algorithms on different types of images and measuring their performance in terms of security, speed, and accuracy. Cyber role simulation tests also involve simulating different types of cyberattacks, such as brute-force attacks and cryptanalysis attacks, to evaluate the robustness of the encryption algorithm against these threats. The results of these tests can be used to improve encryption techniques and to inform cybersecurity policies and practices to enhance image security in various applications, including military, medical, and commercial sectors.

Table 1: Simulation results



Sample grouping	The number of positive samples detected correctly	The number of negative samples detected correctly	Precision rate	Accuracy rate	Recall rate	F1 value
1	89	92	0.905	0.912	0.899	0.906
2	457	461	0.918	0.931	0.918	0.924
3	919	927	0.923	0.926	0.911	0.918

4.6.Image Encryption and decryption approaches using MATLAB

A wide variety of methods for the encryption of images have been developed up to this point. After reviewing the research that was available, we were able to divide the methods into a number of distinct categories, such as those that are spatially based, transform-based, optically based, and compressively based on image encryption. Figure 3 is an illustration that presents a breakdown of the various classifications of image encryption methods. The section that came before this one is the one in which these strategies are discussed and evaluated with the assistance of a variety of metrics that are used for evaluation. The following are the values that should be used for these parameters: CC, KA, NPCR, HA, and UACI in addition to IE. When making comparisons, the symbols and are used to represent whether or not the given method has taken into consideration the respective metric and, respectively, have not been taken into consideration. These symbols can also be used to represent whether or not the given method has not taken into consideration the respective metric. The Encryption of Photographs Utilizing the Three-Dimensional Domain Methods are considered to belong to the spatial domain if they directly manipulate the individual pixels that comprise an image. This is the case for all methods that fall into this category. In the relevant literature, you can find descriptions of a wide variety of methods that are based on the spatial domain and are used to encrypt images. But we have considered the most well-known methods, such as those that are based on DNA, chaos, elliptic curves, fuzzy logic, and metaheuristics, respectively. In the field of cryptography, chaotic maps are regarded as having a considerable amount of importance. These maps are what generate the random numbers, which are then put to use as encryption keys. The reason for this is due to the fact that it possesses certain characteristics, such as having a nature that is both dynamic and deterministic, being sensitive to initial conditions, and being ergodic. The reason why this is the case is due to the fact that it possesses these characteristics. Up until this point, a number of different kinds of chaotic maps have been utilized. However, these can be broadly classified as higher-dimensional chaotic maps, one-dimensional chaotic maps, or both. With the assistance of chaotic maps, the confusion and diffusion operations that take place during the encryption process can be carried out in a more efficient manner. Diagrammatic representation of the flow of the chaotic maps that make up the image encryption method is presented

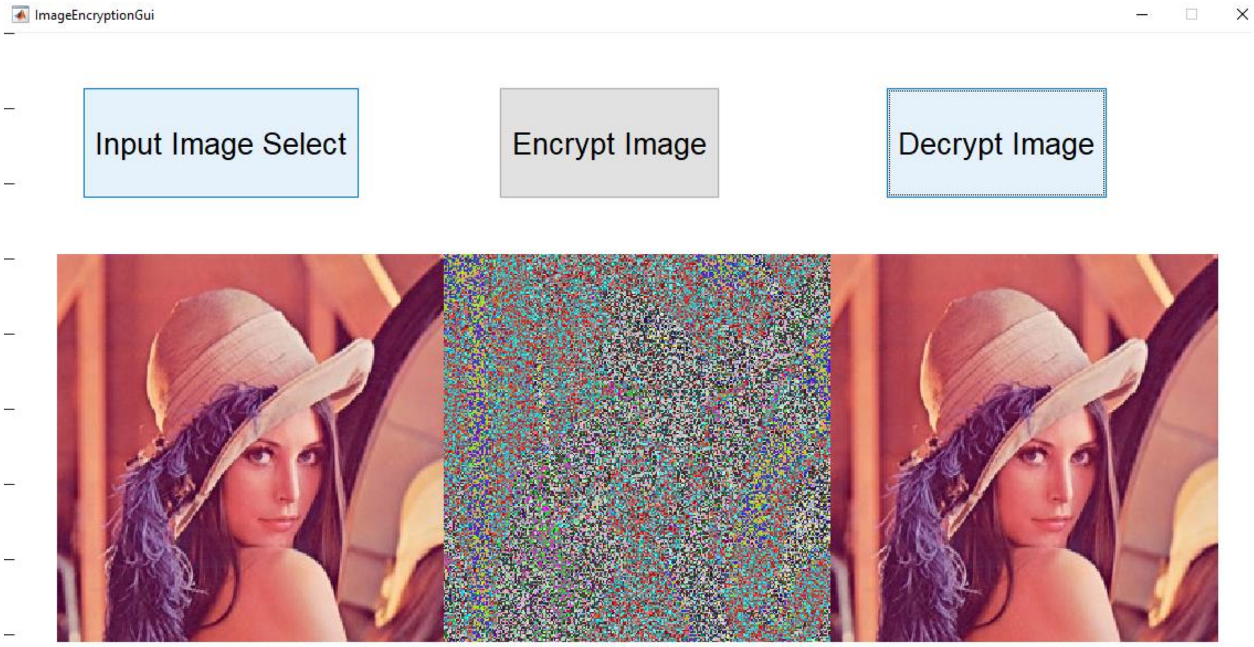


Figure **Error! No text of specified style in document.**: Output result 1

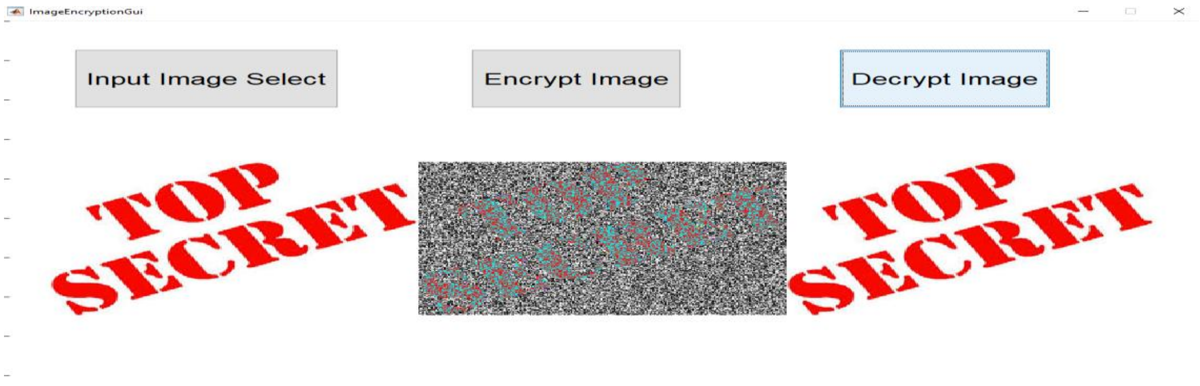


Figure 5: Output result 2

5. CONCLUSION

In order to encrypt a photograph, one must first convert the original image into a different format that is far more difficult to decipher. If a person does not have the key to decode the information, it will be extremely difficult for them to access the material. Image encryption may be useful in many different areas, including the commercial sector, health care, activities carried out by the military, and multimedia systems, to name just a few of these possible applications: In this article, for the purposes of both image encryption and image decryption, the findings of a literature review that was conducted in the past on numerous different techniques to picture encryption are detailed.

This review was undertaken in the past. In the procedures that were carried out in order to successfully encrypt the image, the chaotic sequence and the wavelet transform were both utilized in the processes that were carried out. In order to accomplish what needed to be done, a combination of these two approaches was utilized. As a direct consequence of this fact, the picture was able to be encrypted effectively. After reading the analysis of the article, it is abundantly clear that the solutions that were offered in order to safeguard the genuineness of the photograph are ones that are practical to implement. This is the conclusion that can be drawn from the fact that the situation has been brought into clear focus. This is the inference that can be made as a result of the fact that there is a substantial body of evidence to back up the claim that was made. A presentation was presented that demonstrated the many various encryption methods that could be used to encrypt an image when working with a network that was not secure. These methods could be used to encrypt the image. This was done as a step in encrypting and decrypting images in preparation for the process. It is possible to use these tactics in order to prevent the image from being seen by those who are not authorized to do so in a situation where they are present. It is possible to utilize these strategies in order to prevent the image from being viewed by individuals who are not authorized to do so in order to protect sensitive information. In this piece of literature, a novel method of encryption is proposed as a potential response to the problem of protecting the image from being taken without permission. This solution is presented as a potential remedy to the problem by the author. The picture has been encoded using the method that has been shown, which involves making use of the Wavelet Transform in conjunction with the Chaotic Mechanism. In addition to that, it applies the hash function to the image in order to generate a fingerprint of it, which it then applies to transmit to the recipient. After that, this particular fingerprint is forwarded on to the addressee. During the portion of the activity in which we were acting out various scenarios, not only did we make all of these observations, but we also made a number of other observations. Encrypting images is a highly common practice that is done for the goal of ensuring that data transmissions across open networks like the internet are carried out in a secure manner. This can be accomplished by using a combination of algorithms. It is required to encrypt the data with a distinct form of algorithm for each every item of data because each piece of data has its own individual set of characteristics. In addition, despite the fact that cryptography is a useful instrument for maintaining the confidentiality of communications, this does not mean that it is devoid of any shortcomings. An attack can be carried out against a cryptographic system utilizing a variety of unique approaches, and there is a steady stream of new attacks that are being discovered all the time. Even while cryptography is an essential component of the security procedure, it must not be considered the only issue that must be taken into consideration.

6. FUTURE RECOMMANDATION

Image encryption and decryption is a rapidly evolving field, and there are several areas of future work that can be explored to improve the security, speed, and efficiency of the encryption and decryption process. Some potential areas of future work include:

i. Developing New Encryption Algorithms: There is a constant need for new encryption algorithms that are more secure and efficient than existing algorithms. Future work in this area could involve the development of new encryption algorithms that use advanced mathematical techniques and complex cryptographic mechanisms to ensure high levels of security and efficiency.

ii. Enhancing Key Management: Key management is an important aspect of image encryption and decryption, as the encryption key is used to transform the plaintext into cipher text and vice versa. Future work in this area could focus on the development of new key management techniques that improve the security and usability of the encryption and decryption process.

iii. Improving Performance: The encryption and decryption process can be computationally intensive, especially when working with large images. Future work could focus on developing algorithms that are faster and more efficient, enabling the encryption and decryption process to be performed in real-time.

iv. Developing Hybrid Encryption Techniques: Hybrid encryption techniques involve the use of multiple encryption algorithms to provide a higher level of security than can be achieved using a single algorithm. Future work in this area could focus on developing new hybrid encryption techniques that combine the strengths of different encryption algorithms to provide a more robust and secure encryption and decryption process.

v. Exploring Machine Learning-Based Approaches: Machine learning techniques can be used to improve the security and efficiency of image encryption and decryption. Future work in this area could involve exploring the use of machine learning algorithms to develop new encryption and decryption techniques that are more secure and efficient than existing techniques.

vi. Improving Resistance to Attacks: Image encryption and decryption techniques are vulnerable to various types of attacks, including brute force attacks and differential attacks. Future work could focus on developing techniques that are more resistant to these attacks, providing a higher level of security for digital images.

vii. Developing Cloud-Based Image Encryption and Decryption Techniques: With the increasing use of cloud computing, there is a need for image encryption and decryption techniques that can be performed in the cloud. Future work in this area could focus on developing cloud-based image encryption and decryption techniques that are secure and efficient, enabling users to encrypt and decrypt images in the cloud.

viii. Exploring Block chain-Based Approaches: Block chain technology provides a secure and decentralized platform for data storage and transfer. Future work in this area could focus on exploring the use of block chain-based approaches to image encryption and decryption, providing a secure and efficient platform for the storage and transfer of digital images. Image encryption and decryption is a rapidly evolving field, and there are several areas of future work that can be explored to improve the security, speed, and efficiency of the encryption and decryption process

REFERENCES

1]. Andrews, J.G., A. Ghosh, and R. Muhamed, Fundamentals of WiMAX: understanding broadband wireless networking. 2007: Prentice Hall PTR.

[2]. Liddell, H.G., R. Scott, and G.R. Berry, A lexicon, abridged from Liddell & Scott's Greek-English lexicon. 1901: Economy book house.

[3]. Lin, S. and D.J. Costello, Error control coding. Vol. 123. 2004: Prentice-hall Englewood Cliffs.

[4]. Build MEX-Files. 2013; R2013a: [Available from:http://www.mathworks.com/help/matlab/matlab_external/building-mex-files.html.

[5].Definition: Interoperability. Available from: http://interoperabilitydefinition.info/en/.

[6]. Group, I.W., IEEE Standard for Local and Metropolitan Area Networks, Part 16: Air Interface for Fixed Broadband Wireless Access Systems. IEEE Std, 2004. 802: p. 16-2004.

[7]. FIPS, P., 197: Advanced encryption standard (AES). National Institute of Standards and Technology, 2001.

[8]. Kumar, A., Mobile broadcasting with WiMAX: principles, technology, and applications. 2012: Focal Press.

[9]. Shon, T. and W. Choi, An analysis of mobile WiMAX security: vulnerabilities and solutions, in Network-Based Information Systems. 2007, Springer. p. 88-97. 103

[10]. Nguyen, T., A survey of WiMAX security threats. Computer Science Department, Washington University, 2009.

[11]. Mao, W., Modern Cryptography: Theory and Practice. 2003: Prentice Hall Professional Technical Reference. 740.

[12]. Daemen, J. and V. Rijmen, The design of Rijndael: AES-the advanced encryption standard. 2002: Springer.

[13]. Stinson, D.R., Cryptography: theory and practice. 2006: CRC press.

[14]. Reason, J.M., End-to-end confidentiality for continuous-media applications in wireless systems. 2001: University of California, Berkeley.

[15] Arnone, L., et al., Security and BER performance trade-off in wireless communication systems applications. Latin American applied research, 2009. 39(3): p. 187-192.

[16]. Kim, K. and J. Hong, Performance Analysis of Digital Secure Voice Transmission over HF Radio Channel, in Advances in Information Security and Assurance. 2009, Springer. p. 337-346.

[17]. Buchholz, J.J., Advanced Encryption Standard. Available online at bushels. Hsbremen. De/aes/aes. html, 2001.

[18]. Dworkin, M., Recommendation for block cipher modes of operation. Methods and techniques. 2001, DTIC Document.

[19]. Lipmaa, H., P. Rogaway, and D. Wagner. CTR-mode encryption. in First NIST Workshop on Modes of Operation. 2000.

[20]. McGrew, D.A., Counter mode security: Analysis and recommendations. Cisco Systems, November, 2002. 104

[21]. Housley, R., Using advanced encryption standard (AES) counter mode with IPsec encapsulating security payload (ESP). 2004.

[22]. Ross, S.M., Introduction to probability models. 2006: Access Online via Elsevier.

[23]. Sattar, F. and M. Mufti, On Post Decryption Error Probability in Counter Mode Operation with Explicit Counter Transmittal. 24. Wallace, H., Error detection and correction using the bch code. EBook UNDUH, 2001.

[24] Haraty, R.A., A.N. El-Kassar and B. Shibaro, 2006. A comparative study of rsa based digital signature algorithms. J. Math. Stat., 2: 354-359. 146 International Journal of Sciences: Basic and Applied Research (IJSBAR)(2014) Volume 14, No 2, pp 141-147

[25] Schnorr, C. P. and Jakobsson, M., 2000. Security of signed ElGamal encryption. Springer Berlin Heidelberg.