REPUBLIC OF TÜRKİYE

ALTINBAŞ UNIVERSITY

Institute of Graduate Studies

Information Technologies

SURVEILLANCE SYSTEM PROTECTION BY ENCRYPTION TECHNIQUES IMPROVEMENT

Karrar Hamzah Mezher AL-CHAABAWI

Master's Thesis

Supervisor

Asst. Prof. Dr. Timur İNAN

Istanbul, 2023

SURVEILLANCE SYSTEM PROTECTION BY ENCRYPTION TECHNIQUES IMPROVEMENT

Karrar Hamzah Mezher AL-CHAABAWI

Information Technologies

Master's Thesis

ALTINBAŞ UNIVERSITY

2023

The thesis titled SURVEILLANCE SYSTEM PROTECTION BY ENCRYPTION TECHNIQUES IMPROVEMENT prepared by KARRAR HAMZAH MEZHER AL-CHAABAWI and submitted on 09/08/2023 has been **accepted unanimously** for the degree of Master of Science in Information Technologies.

Asst. Prof. Dr. Timur İNAN
Supervisor

Thesis Defense Committee Members:

Asst. Prof. Dr. Timur İNAN	Department of Software Engineering, Altınbaş University	_____
Asst. Prof. Dr. Mesut ÇEVİK	Department of Electrical and Electronics Engineering, Altınbaş University	_____
Asst. Prof. Dr. Vedat ESEN	Department of Electrical and Electronics Engineering, İstanbul Topkapı University	_____

I hereby declare that this thesis meets all format and submission requirements of a Master's thesis. Submission date of the thesis to Institute of Graduate Studies: ___/___/___

I hereby declare that all information/data presented in this graduation project has been obtained in full accordance with academic rules and ethical conduct. I also declare all unoriginal materials and conclusions have been cited in the text and all references mentioned in the Reference List have been cited in the text, and vice versa as required by the abovementioned rules and conduct.

Karrar Hamzah Mezher AL-CHAABAWI

Signature

DEDICATION

First, I thank God Almighty for my success.

My father is my support, my strength, and my companion. My Wife, the woman who trusted me, walked with me, and helped me to the end. My children who bore with me travel and alienation. To my Turkish friends. To all who asked about me and stood by me. I dedicate this research to you and say with gratitude, thank you.

ABSTRACT

SURVEILLANCE SYSTEM PROTECTION BY ENCRYPTION TECHNIQUES IMPROVEMENT

AL-CHAABAWI, Karrar Hamzah Mezher
M.Sc., Information Technologies, Altınbaş University
Supervisor: Asst. Prof. Dr. Timur İNAN
Date: 08/2023
Pages: 64

Systems of surveillance are crucial to the security of your residence or place of business. These systems range from sophisticated alarm systems that notify law authorities at the first sign of a problem to wireless home security cameras. The presence of security cameras can deter would-be robbers, while hidden cameras can defend a property discreetly. Images acquired by the cameras are saved in the storage containers of the surveillance system. Given the sensitivity and importance of photos, the system may be exposed to hacking and penetration to acquire access to the contents of these images and unauthorized usage by unauthorized parties. With the growing volume of data within the monitoring system, data security has become an essential problem in terms of storage and transmission. Images and videos obtained from the monitoring system, in particular, should be forwarded to the designated management rooms for storage and inspection. Cryptographic techniques are used to encrypt the contents of the photos to prevent outsiders from viewing them, and these images are transmitted as encrypted images. To encrypt five different-sized photos, this study used the symmetric and asymmetric techniques RSA, AES, and Blowfish. These algorithms' performance was compared using measures such as histograms, correlation coefficient, entropy, SSIM, elapsed time, and PSNR criterion). Furthermore, RSA and Blowfish outperformed AES in terms of a histogram, SSIM, and PSNR metrics for all five photos, and AES outperformed both Blowfish and RSA. However, while RSA outperforms Blowfish in both picture encryption and decryption, AES techniques outperform the other algorithm in terms of propagation and confusion, as well as resilience to brute force attacks. As a result, their security performance is vastly varied. When the algorithms' time

parameters are examined, AES is determined to be faster than Blowfish and RSA. This work demonstrates that AES is superior to RSA and Blowfish at encrypting images in real-time on computers outfitted with surveillance cameras. After developing the AES algorithm using the Apache Spark platform, it was discovered that the algorithm's execution speed had doubled, implying that the new algorithm might be used to protect big data in the future.

Keywords: Surveillance Systems, AES, RSA, Blowfish, SSIM, PSNR, Apache Spark.

TABLE OF CONTENTS

Pages

LIST OF TABLES

Pages

LIST OF FIGURES

Pages

LIST OF CHARTS

Pages

ABBREVIATIONS

AES	:	Advanced Encryption Standard
RSA	:	Rivest–Shamir–Adleman
SSIM	:	Structural Similarity Index Measure
PSNR	:	Peak Signal-To-Noise Ratio
MLib	:	Machine Learning Library
SMC	:	Sliding Mode Control
KU	:	Public Key
KR	:	Private Key
P	:	Plaintext
CP	:	Cipher Text

1. INTRODUCTION

In the world of today's online, multimedia, and wireless networks, digital images, audio, and video from multi-media sources are becoming an integral aspect of communication. It makes it easier for hackers and assailants to disrupt, use improperly, change sensitive multimedia data, and get unauthorized access to it. As a result, there is an increasing need to create trustworthy and efficient security methods to protect the privacy of digital multimedia data while it is being transferred across wireless networks and the Internet. Using encryption methods to protect sensitive data is a feasible traditional approach Encryption, which is the mathematical transformation of unencrypted data into an incomprehensible form, provides data confidentiality, integrity, authenticity, and non-repudiation. End-to-end secure communication is offered. The primary goal of encryption is to safeguard plaintext. data that only a legitimate recipient with the right secret key will be able to decrypt. A robust encryption method should satisfy the classical Shannon criteria of confusion and diffusion, be resistant to cryptographic assaults, and have excellent statistical characteristics. While diffusion shuffles plaintext bits so that any repetition in the plaintext is dispersed throughout the ciphertext, confusion tries to make the relationship between the key and ciphertext as complicated as possible. Traditional encryption methods include DES, AES, IDEA, RSA, and others. These number-theory-based encryption approaches are effective at generating good confusion and diffusion for encrypting text data, but they are not suitable for encrypting multimedia data.

Multimedia data is typically very huge and bulky; nearby pixels/frames have a high correlation, and there is spatial and temporal redundancy. Encrypting such data with typical techniques requires a lot of computer power, a lot of time, and a lot of money for real-time multimedia applications like video conferencing, picture surveillance, image-based military, and satellite communication, among other things. As a result, stronger solutions are required to successfully address multimedia data security issues. When we perceive the world with our eyes, it should be smooth and pleasant to the eyes, but it might be irritating to the eyes when we see the captured or transmitted images. This is due to image distortion that occurs during the transmission or capture of the image. There are some algorithms and approaches for measuring or analyzing this distortion, such as PSNR and SSIM, which

detect the difference between the distorted image and the original or reference image. The study of these factors provides information about the degree of resemblance to the reference image or original.

1.1 CRYPTOLOGY

The study and application of strategies for safe communication in the face of hostile behavior is known as cryptology[1]. Cryptography is the study and creation of methods that keep the general public or uninvited parties from reading private messages. Modern cryptography prioritizes information security concepts such data secrecy, integrity, authentication, and non-repudiation[2]. Modern cryptography has connections to arithmetic, computer science, electrical engineering, physics, and communication science[3]. Examples of applications for cryptography include e-commerce, chip-based card payments, digital currency, computer passwords, and communication within the military.

Mathematics and computer science have a big impact on modern cryptography. Because cryptographic methods are based on assumptions about computational hardness, it is challenging for an adversary to successfully use them. Although theoretically possible, it is practically impossible to break into a well-designed system.[4]. These plans must be reevaluated and, if required, altered on a frequent basis in light of theoretical advancements (such as improvements in integer factorization algorithms) and faster computing technology. Such systems are said to as "computationally secure" when they are properly understood[5]. The best computationally secure but theoretically breakable approaches are more difficult to use in reality than information-theoretically safe systems, like the one-time pad, which are proven to be impenetrable even with unlimited computer capacity.

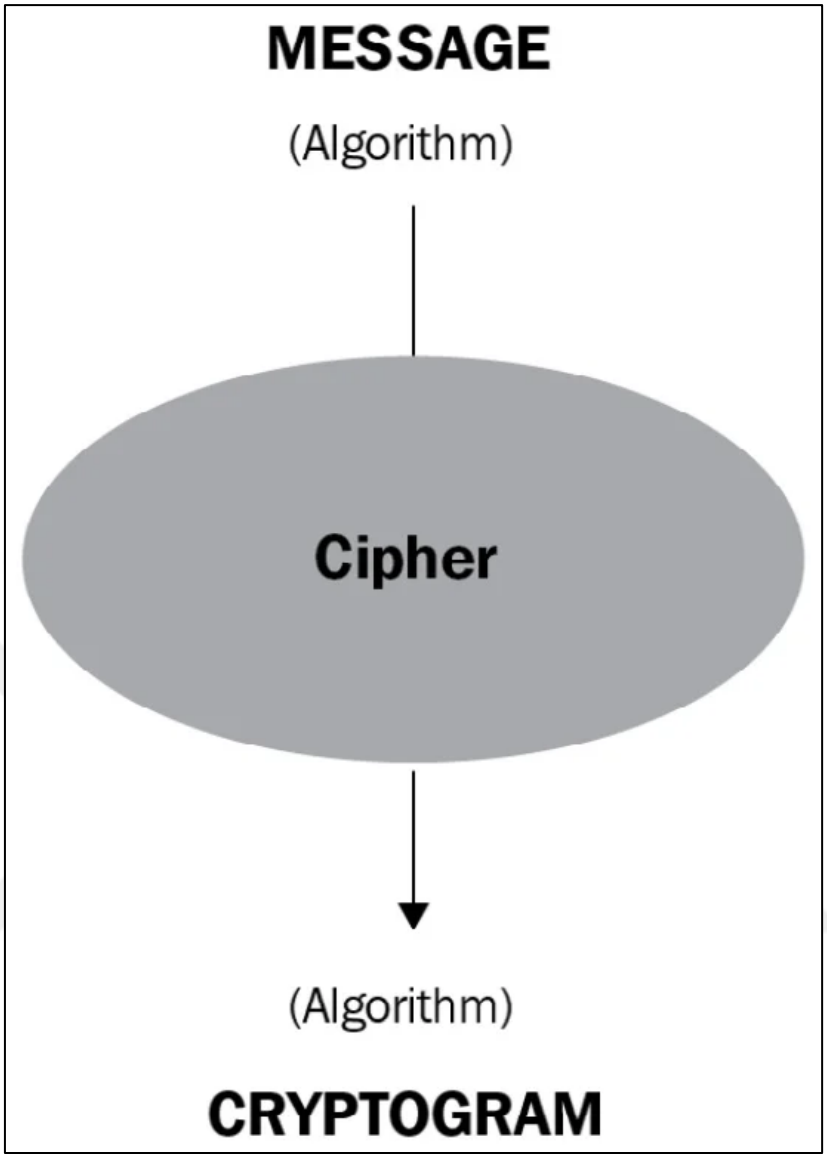


Figure 1.1: Cryptology Operation [6].

Cryptology is divided into two branches:

a. Cryptography is the study and development of cryptographic systems.
b. Cryptographic systems is known as cryptanalysis.

With a third party [6] present, safe communication between two parties (Alice and Bob) is a focus of the computer science and mathematics discipline of cryptography (see Figure 1). Based on techniques like encryption, decryption, signature, and the creation of pseudo-random numbers, among others.

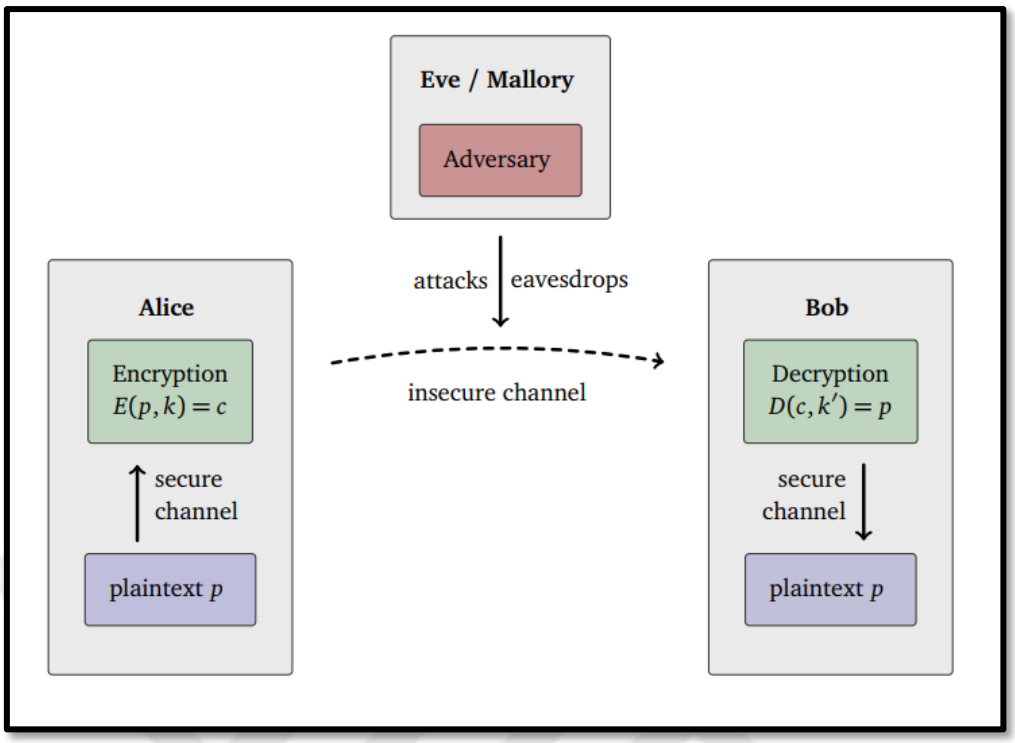


Figure 1.2: A Fundamental Concept for Safe Communication [7].

1.2 HISTORY OF ALGORITHM

Algorithms have been an idea since ancient times. The oldest examples of algorithms can be found in Babylonian mathematics from ancient Mesopotamia (now Iraq). The first division method was written on a Sumerian clay tablet discovered near Baghdad in Shuruppak approximately 2500 BC[7]. Babylonian clay tablets from the Hammurabi dynasty, which ruled from 1800 to 1600 BC, contained formula computation algorithms[8]. Astronomy under Babylonian theory also made use of algorithms. The time and location of key astronomical occurrences are calculated using algorithms that are described in Babylonian clay tablets.

The Rhind Mathematical Papyrus, which was written in ancient Egypt around 1550 BC, contains mathematical algorithms[9]. The mathematics of the ancient Hellenistic period later employed algorithms. The Euclidean algorithm (originally published in Euclid's Elements around 300 BC) and the Sieve of Eratosthenes (described in Nicomachus' Introduction to Arithmetic)[10].

Dixit Algorizmi ('Thus spake Al-Khwarizmi,' where "Algorizmi" is the translator's Latinization of al-khwarizmi's name) are the first words in the manuscript[11]. Due largely to another of his works, Algebra, Al-Khwarizmi was the most widely read mathematical in Europe in the late Middle Ages. [12]. Algorismus, which became "algorism" in English as a transcription of his name, simply meant "decimal number system" in late medieval Latin. The Latin word algorithm was translated to algorithm in the 15th century as a result of the Greek word (arithmos), which means "number" (cf. "arithmetic"). The term "algorithm" first appeared in print in the 17th century, and the contemporary sense emerged in the 19th century.

1.2.1 Algorithm

An algorithm is a finite collection of explicit instructions used to solve a class of specified problems or carry out a computation in mathematics and computer science. Algorithms are specifications for mathematics and data processing. Algorithms can do automated deductions (also known as automated reasoning) and employ logical and mathematical tests to steer the code in various directions (also known as automated decision-making). Alan Turing utilized figurative terms such as "memory," "search," and "stimulus" to describe machines by evoking human characteristics[13].

Notations for expressing algorithms include natural languages, pseudocode, flowcharts, drakon-charts, programming languages, and control tables (which interpreters parse). Algorithms are rarely expressed in difficult or technical terms using natural language because it is often verbose and unclear[14]. The ambiguity in statements based on plain English is greatly reduced by the methodical expression of algorithms in pseudocode, flowcharts, drakon-charts, and control tables. Despite the fact that they are frequently used to define or explain algorithms, programming languages are primarily designed for expressing algorithms in a way that a machine can execute.

1.2.2 Encryption Ttechniques

There are numerous encryption algorithms and ways to choose from, and the most common encryption systems: Asymmetric encryption vs. symmetric encryption[15].

a. Symmetric Encryption

One key is used for encryption as well as decryption in the symmetrical encryption method. The National Institute of Standards and Technology (NIST) has conducted studies that show the Rijndael algorithm, known as AES, to be the best in terms of security, performance, efficiency, implementation capacity, and flexibility. This information was made public on October 2, 2000. It outperforms all other algorithms currently available[16]. The AES encryption technique is used in this project to encode and decode 5 photos and to test the encryption performance of various data volumes in the Apache Spark environment, where the spark has numerous advantages in processing big amounts of data. Apache Spark offers periodic data streaming and outperforms Hadoop in terms of in-memory computation[17]. The photos will be encrypted using the AES technique, and the time spent encoding and decoding will be calculated in normal mode. Also, the AES algorithm will be customized for use in the Apache Spark environment. The algorithm is applied to the Spark environment inside Clusters with multiple nodes and calculates the elapsed time for encryption and decryption processes to try to gain more time to reach the fastest way to secure surveillance system images in real time.

b. Asymmetric Encryption

In asymmetric key encryption, like that used by RSA and ECC, two keys are used: one to lock or encrypt the plaintext and the other to unlock or decrypt the cyphertext. None of the keys are dual-purpose[18]. Because the public key is used for encryption and the private key is used for decryption, this technique of encryption is more secure. These keys are linked, connected, and have the following operations: A public key can be used by anyone who needs to encrypt data. When it comes to decryption, this key is useless. A user needs the private key, which is a secondary key, to decode this data. In this way, the actor decrypting the data is the only one who keeps the private key, maintaining security when security is scaled[19].

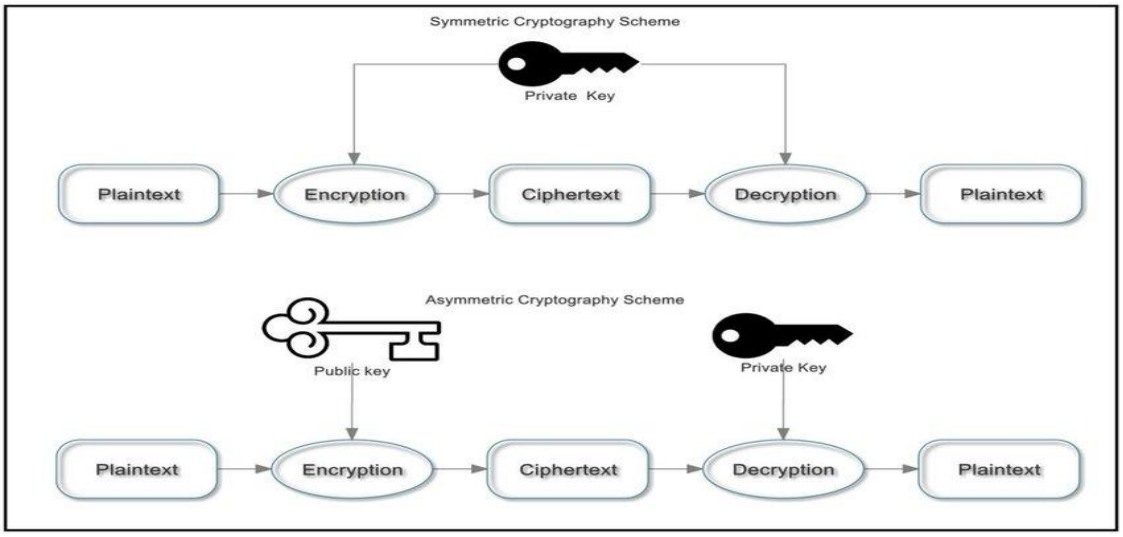


Figure 1.3: Symmetric and Asymmetric Encryption[20].

1.3 APACHE SPARK

Launched in 2009, it is an open-source big data analytics cluster computing project. One of the essential components that provide the MapReduce environment its speed and efficiency is the capability to run computations in memory[21].

The components of Spark is [21, 22]:

a. Basic operations including memory management and communication with storage systems are included in Spark Core.
b. Spark SQL is a collection of Spark packages that includes the tools for managing and arranging data sets.
c. Spark Streaming It is a Spark component that analyzes both log files produced by a web server and live data streams.
d. MLib, or machine learning, it is a library inside of Spark that includes machine learning capabilities and a variety of different machine learning algorithms.
e. GraphX is one of the Spark libraries that focuses on producing and manipulating arbitrary graphs.
f. By increasing the number of mathematical nodes using the techniques of a Spark block manager known as the independent scheduler, the cluster manager is utilized to improve the performance of the Spark environment.

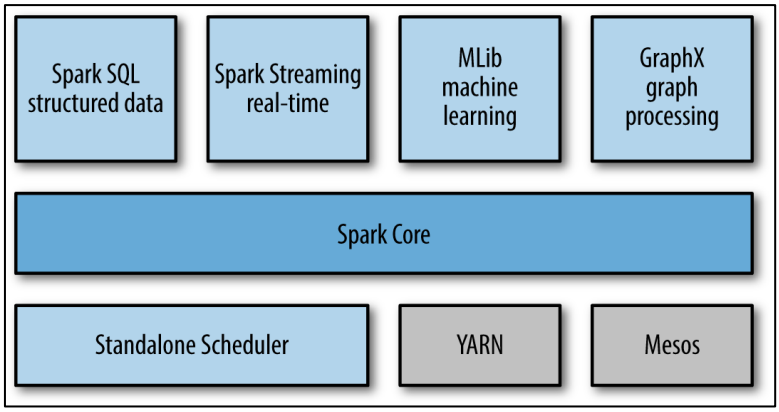


Figure 1.4: Apache Spark Components [21].

1.4 PROBLEM STATEMENT

The term "surveillance system" refers to both overt and covert cameras that record visual pictures while observing activity, behaviour, or data. The interest in securing this system is of significant importance for the data it contains because it is subject to several penetration difficulties and is classified as having weak security. To ensure the high reliability of this system and to guarantee that unauthorized person's access to this data will prevent them from seeing its contents because it is encrypted, the protection of image and video data should go beyond simply preventing them from being accessed.

The following research questions must be answered:

a. Because your system is susceptible, hackers may be able to easily get into it in some circumstances. Hackers can steal camera videos and so track your activities and life from afar. To avoid this, choose a security system that is both redundant and encrypted.
b. Low-Quality Video Surveillance Footage & Alerts.

The quality of the captured images can also be measured to improve the performance of the system. It can use (Entropy, elapsed time, SSIM, Histogram, PSNR, correlation coefficient) criteria for measuring the quality of algorithms and images.

1.5 OBJECTIVES

The long-term purpose of the research is to improve the security of a surveillance system. The process of recognizing, classifying, and modeling data about people in general for a

specific location is characterized here as surveillance systems. The current study's goal is to give a thorough evaluation of the literature and industry practices concerning surveillance systems, as well as to create a conceptual framework for it.

The study has the following sub-objectives in particular:

a. To give a complete assessment of the sources and characteristics of common surveillance systems.
b. Developing a method for protecting collected data by symmetric and asymmetric encryption algorithms.
c. Defining a conceptual framework for the proposed algorithms and encoding the contents of the images captured by the monitoring system with those algorithms.
d. Using image processing and evaluation techniques in order to know the real performance of algorithms and choose the best among them to protect the monitoring system.
e. The algorithm that will be selected as the fastest and most efficient image encryption algorithm is then improved and developed by Apache Spark to reach the highest levels of efficiency in encrypting and protecting the data of the Surveillance systems.
f. This study's findings will be useful to the Surveillance system and related software suppliers in establishing improved methods and tools for surveillance system management and look-ahead scheduling.

1.6 CONTRIBUTION

The contribution to this study is the comparison between algorithms with different encryption techniques and different efficiencies to find the best algorithm for encoding surveillance camera images and to ensure a higher quality of the algorithm, as the best algorithm is improved after the end of the comparison by applying it within the Apache Spark platform. To achieve the method's high real-time execution speed, Apache Spark has modified its use of the AES algorithm to carry out the encryption and decryption operation in standalone mode within the Cluster. Thus, we obtain higher guarantees to protect the storage of surveillance cameras and make the system more secure and effective.

2. LITERATURE REVVIEW

2.1 LITERATURE REVIEW

This portion surveys the scientific literature on the research topic and presents a summary of the state of the science. This allows for the identification of pertinent ideas, approaches, and research gaps that can be later applied to the study thesis.

a. Studies related to the AES algorithm

In this study, Arab, A., Rostami, M.J., et al, suggested using a novel image encryption algorithm built on top of a modified AES algorithm and chaotic sequences. This method uses an Arnold Chaos sequence to create the encryption key. The original image is then encrypted with the help of a modified AES algorithm and round keys generated by the chaos system. The suggested method not only lowers the algorithm's temporal complexity but also gives it the potential to spread, making the images encoded by the suggested algorithm resistant to differential attacks. The major area of the suggested technique is large enough to resist brute force attacks. Since the input image and the initial parameters are crucial to this approach, even minor changes to these values can have a big effect on the encoded image. We demonstrate that this strategy can defend the image against statistical attacks using statistical studies[23]. The results of the entropy test demonstrate that the entropy values are nearly optimal, making the suggested algorithm resistant to entropy attacks. According to the simulation results, the original image cannot be obtained while slight changes to the key and the original image cause significant changes in the encrypted image. The researchers were not able to return the encrypted images to their true state, which prompted us to complete what they started to reach efficient and complete results.

Lin, Chih-Hsueh, et al, discussed the goal of this study to create synchronous dynamic keys based on chaos and an Advanced Encryption Standard (AES) algorithm based on chaos using the suggested synchronous random keys. First, a wavy control scheme is presented based on the sliding mode control (SMC) technique to assure synchronization between the distinct chaotic systems between the master and the slave. In communication systems, synchronization allows for the simultaneous acquisition of the same dynamic random chaos signals from the transmitter and receiver[24]. Then, a novel modified AES cipher scheme

based on chaotic synchronization and featuring dynamic random keys were presented. A static key is utilized in the standard AES encryption method, and it must be rewritten beforehand and kept secure. However, in the suggested design, the static key becomes dynamic and unpredictable and is not required to be retained or broadcast across open channels because the synchronization approach of chaotic systems is used. As a result, key storage issues can be resolved and cryptographic security enhanced. Finally, a novel picture encryption technique was produced using the chaos-based developed AES (CAES) algorithm. To show the effectiveness and optimization of the proposed CAES encryption system, simulated tests were used to generate statistical analysis, graph, information entropy, and correlation indices. Researchers have found that current encryption techniques may be vulnerable to being broken by quantum computers due to their supercomputing speed. Therefore, it is crucial to understand how to protect the security of data flow.

The researchers [25] thought about creating a C-based AES-based picture encryption application in cipher blockchain mode. Using the efficiency of AES-based picture encryption systems, the proposed encryption method was assessed and compared with a few existing chaos-based image encryption systems in terms of encrypting/decryption speed and security. The results of the simulation disprove the generally accepted belief that AES is inappropriate for image encryption. Additionally, the researchers recommended using the performance of AES-based encryption of images as a benchmark for the speed of image encryption algorithms. Image encryption techniques that work at speeds slower than those utilized for real-world communications must be abandoned. Through the aforementioned study, we were inspired to improve the speed of encoding algorithms so they could operate swiftly in real-time and successfully decode the image and restore it to its original form.

Digital picture communication has grown in importance as a mode of information transmission due to the rapid growth of networking and communication technology. Because of this, there is more interest in creating digital picture coding technologies. In this study, we provide a method for encrypting digital images that is based on the MATLAB AES implementation. Then, we combine both methods by processing digital photographs to produce data that can be encrypted with the AES algorithm[26]. After that, the digital

image can be encoded. The results demonstrate that the method can more effectively realize the impact of encryption and decryption when graph analysis and key analysis are compared. Depending on the findings of the inquiry, we may look for novel, effective approaches to assess the encryption strength of an algorithm.

b. Studies Related to the RSA Algorithm

The researchers took precautions to protect the images by transforming them from a comprehensible to an incomprehensible form. In picture encryption, they contrasted Advanced Encryption Algorithms (AES) with Rivest-Shamir-Adleman (RSA). Each method was compared in terms of image coding quality assessment. In addition to examining the graph and correlation results. The results indicated that the AES technique produces higher-quality picture encryption with more closely spaced graph columns. The AES algorithm's correlation coefficient is likewise closer to zero, indicating a stronger link. The study's findings generally demonstrated that the AES method outperforms the RSA technique for image encryption[27].

The researchers came to the conclusion that information security is a critical concern in data transmission. Encryption has evolved as a solution and is now used extensively in information security systems. An introduction to cryptography is provided, as well as an explanation of the RSA cipher scheme. It also compares the RSA encryption technique to other encryption systems when applied to a grayscale image. The results demonstrated that the time spent using mathematical relations in RSA allows for faster step execution and more secure data than other algorithms and similar systems. However, in RSA, the time spent on key generation increases because it makes it more secure than previously. It was determined that the RSA algorithm has high encryption efficiency and may be compared to other algorithms to find the best[28].

This study suggests a novel chaotic paired system-based picture coding algorithm. They employed the 2D Becker chaotic map to regulate the system parameters and state variables of the logistic chaotic map due to the scalability and weakness of a single chaotic map. A logistic map's parameter changes after control, and the resulting logistic sequence is therefore variable. Complexity research demonstrates that the revised map is random and unpredictable. Furthermore, based on the improved chaotic maps, a new picture coding

algorithm (RSA) with mixing and substitution operations is developed. Numerous statistical tests and security analyses show that this technique provides great security and can compete with certain other recently proposed picture encryption schemes[29].

c. Studies Related to the Blowfish Algorithm

The researchers Singh, P. and Singh, K, focused on how electronic systems communicate data, and how information security has become essential. Security in connection and picture storage has grown in importance with the expansion of multimedia applications. This study focuses on the encryption and decryption of images using the 64-bit Blowfish block cipher, which is intended to boost performance and security. Utilizing a changeable key size of up to 448 bits, this approach will be used. Researchers have found that the Blowfish algorithm outperforms other widely used algorithms and is safe from unwanted attacks[30].

The researchers stated that they are looking for an algorithm to improve the security of long-term color image encryption that is accurate and efficient. By adding a new F function to the conventional Blowfish Algorithm (BA), color picture coding security is raised. To obtain the dynamic S-box and XOR operator from the F function, the number of iterations is significantly reduced from sixteen to four. Secret keys for blocks of different sizes are generated at random. Calculations are performed using Matlab R2008a methods on eight images with a resolution of 512 by 512 pixels that were acquired from the shared USC-SIPI picture collection. The security of the suggested technique significantly increases with larger blocks. According to performance analyses, the entropy is higher than 7.9993 and the correlation coefficient is smaller than -0.0016. Additionally, the Lena image's RGB channel distribution shows notable security advancements. As the entropy ratio rises, the correlation between image pixels declines substantially[31]. The suggested approach outperformed standard BA at coding color images when compared to earlier efforts. The Blowfish algorithm was selected for comparison with other picture encryption algorithms based on the aforementioned results.

This research focused on picture security by increasing the usage of images in most communications, as the information contained in these photos, such as military and medical images, must be safeguarded. Blowfish has been presented as a separate symmetric encryption method with the advantage of being highly resistant to attackers. As a result, it

is frequently used in data coding, however, it is not appropriate for picture coding due to the enormous amount of data, high redundancy, and significant correlation of image pixels. The proposed improved approach utilized a blowfish-based image coding mechanism. To improve the connection between the original image and the processing, the digital image is first separated into a large number of random key-based blocks. Each of these blocks is then subjected to the Blowfish algorithm. The suggested system is built to benefit from strong attachment, which is backed by a chaotic map, leading to increased security and performance[32]. This results in the suggested system having good image coding performance. Both techniques were created for testing purposes in order to improve the Blowfish coding algorithm, which showed that the original image had a flat graph after encoding, reducing correlation between neighboring pixels in all color components, and increasing state entropy. A comparison analysis with the old Blowfish method revealed that the improved technique was superior and that better results could be reached if the encryption algorithms' capabilities were developed and modified [33].

2.2 THE RESEARCH GAP

Based on prior studies, there is a research gap that is essentially an unanswered question and an unresolved problem in cryptography, indicating a lack of existing research in this sector. Despite the fact that there is a lot of current research, the results of studies tug in diverse directions, making it difficult to draw definite conclusions[34]. Where the researchers confirmed their success in encrypting the images with some of the proposed encryption techniques, but it was difficult for them to decrypt the images and return them to their normal state. Some of the researchers succeeded in encoding and decoding images, but without success in developing or improving the techniques. We discover that researchers in this field did not identify the best main algorithms that could be used and tried to develop them, as well as using simple development techniques, and that improving the algorithms depended on modifying the algorithm itself without resorting to external factors.

2.3 DATA SECURITY AND ENCRYPTION

The protection of data against illegal access, use, modification, disclosure, and deletion is known as data security. The process of transferring information from a readable plaintext to an unintelligible encoded representation known as cipher text is known as data encryption. Until it is decoded, encrypted data cannot be read or used by either people or machines. The decryption key must be protected from unauthorized access because it is secret[35].

The method of encrypting data makes it unusable but does not prevent hackers or data theft. Instead, since the hacker or content thief cannot view it in unencrypted format, it prevents the usage of stolen content. Protection is provided through encryption, which scrambles data so that only the holder of the key or password may decode it. This safeguards the data's confidentiality by preventing unauthorized users from accessing the storage system or service and viewing the data. Additionally, it safeguards the data's integrity so that it cannot be altered without the owner's knowledge[36].

Numerous servers connected to the internet are used to manage and store enormous amounts of sensitive data. This is because it is nearly difficult to conduct daily activities, such as dealing with business or personal matters, without your private information being sent and kept by the networked computer systems of many firms[37].

Encryption data techniques encrypt the plaintext so that only the owner of the decryption key may decipher it. This method safeguards the private information users communicate, receive, and save on mobile devices, especially those linked to the Internet of Things[38]. Computer networks are used to transmit digital information, and data encryption technologies protect the cloud. As the internet has changed computers and networks, more recent encryption algorithms (ciphers) have taken the role of the obsolete Data Encryption Standard (DES) to protect IT communications and systems[39].

These algorithms offer privacy protection along with essential security safeguards like non-repudiation, integrity, and authentication. Any communication is first verified as coming from the intended source by the algorithms, and then its integrity is checked to make sure

that nothing was changed in the process of transmission. Additionally, senders are prohibited from downplaying legal actions under the non-repudiation scheme[40].

The two main methods for encrypting data are symmetric encryption and asymmetric encryption. In symmetric encryption, both data encoding and decoding are accomplished using a single, confidential password. Asymmetric encryption encrypts and decrypts data using two unique keys. It is also known as public-key encryption or public-key cryptography. A shared public key must be used to encrypt the data. An unreleased, private, secret key must be used to decode the material[41].

While symmetric-key encryption is faster than asymmetric encryption, the encryption key must be shared between the sender and the recipient for the data to be unlocked. Enterprises now need to securely retain an exponentially greater number of keys as a result of this. Numerous data encryption providers have adapted to asymmetric algorithms as their use has increased[42].

Beyond the distinction between symmetric and asymmetric encryption, there are various techniques for processing secure data in use today. Each data encryption standard was created to address a particular security requirement[18].

2.4 THE PROPOSED ALGORITHM OVERVIEW

The performance of image encryption and decryption using the proposed AES, RSA, and Blowfish algorithms was evaluated in simulations using a specific set of criteria in this work. Five different grayscale images of different sizes were used. Below is an overview of the proposed algorithms and how they work.

2.4.1 Blowfish Algorithm

A symmetrical square assumption that works well for data encryption and security is blowfish. Since it takes keys with different lengths, ranging from 32 bits to 448 bits, it is ideal for data security. The Blowfish Algorithm is a symmetric key square figure for the Feistel Network that typically emphasizes a transparent encryption process. It offers an incredibly high encryption rate. The key can be any size up to 448 bits, and the square size is 64 bits[43]. The actual encryption of data is extremely potent on large microchips, even

though a remarkable presentation arrangement is necessary before any encryption can place. The blowfish algorithm will take substantially longer to process data than the RSA. Better results are produced using the Blowfish algorithm than the RSA[44].

Anyone can encrypt a message using the recipient's open public key in an open public key encryption system, but only the recipient's private key can decrypt it. To be used for encryption and unscrambling, an open and private key match should be easy for a client to create. A framework for open public key cryptography is said to be of high quality if it is computationally challenging to resolve a validly generated private key from its related open key. At that moment, security is only dependent on maintaining the confidentiality of the private key; the open public key may then be shared without compromising security[45].

In an open public key encryption system, anyone can encrypt a message using the recipient's open public key, but only the recipient's private key can decrypt it. To be utilized for encryption and unscrambling, an open and private key match must be straightforward for a client to generate. When it is computationally challenging to resolve a properly created private key from its accompanying open key, an open public key cryptography architecture is said to be of good quality. At that moment, distributing the open public key without affecting security is only possible if the private key's secrecy is preserved[46].

A communication can be encrypted by anybody using the recipient's open public key in an open public key encryption system, but only the recipient's private key can decrypt it. The ability of a client to quickly create an open and private key match is required for encryption and unscrambling to function[47]. An open public key cryptography system is said to be of high quality if it is computationally challenging to resolve a validly generated private key from its corresponding open key. The confidentiality of the private key is then the only need for retaining the open public key without compromising security[48].

a. Fast. Since it uses 32-bit microprocessors with 26 clock cycles per byte to encrypt the data
b. Compact. The Blowfish algorithm can function in memory that is less than 5K.
c. Simple operations like CARs, and database lookups on 32-bit operands are all that the Blowfish algorithm uses. Blowfish design is simple to examine.

d. Modestly Secure. A maximum key length of 448 bits is available for Blowfish. Blowfish is recommended for uses like communications links or automatic file encryptors when the key won't change frequently.

e. The key is more substantial and difficult to crack.

f. The Blowfish would be provided without charge, without a license, and without being patented for all usage[49].

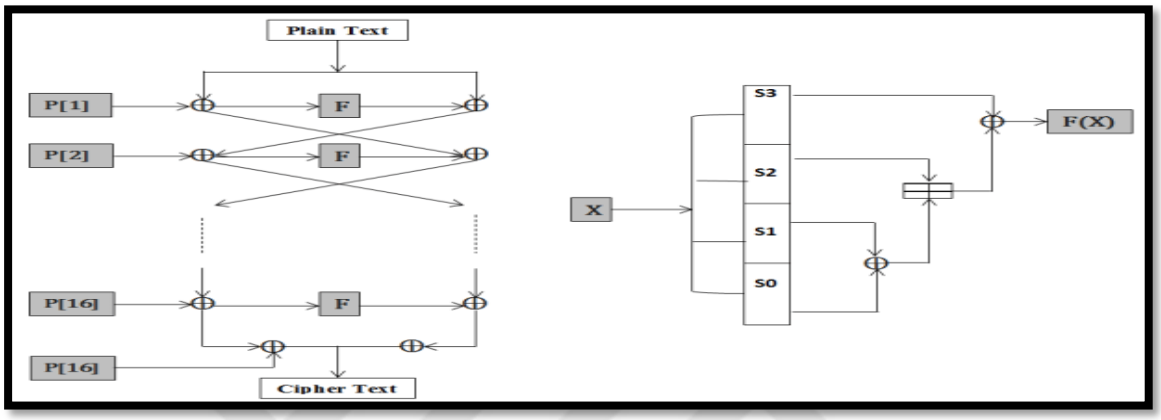


Figure 2.1: The Blowfish Algorithm Working [48].

2.4.2 RSA Algorithm

A popular public-key cryptosystem for safe data transit is (Rivest-Shamir-Adleman). In addition, it is among the oldest. The names of the three people who first made the method publicly known in 1977—Ron Rivest, Adi Shamir, and Leonard Adleman—are the source of the word "RSA". An analogous technique was created in 1973 undercover at GCHQ (the British signals intelligence organization) by English mathematician Clifford Cocks. In 1997, that system became widely known[50].

Asymmetric encryption and decryption were created in 1978 by Rivest, Shamir, and Adleman utilizing two unique keys (public and private). Everyone on the network has access to the encryption key used to encrypt the data, but only the recipient of the data has access to the decryption key. There are three main phases in the RSA algorithm[51].

i. Key Generation: RSA needs two keys, a private key, and a public key. Anyone using the network must be aware of the public key for it to be used to encrypt data.Only the private

key will be able to decrypt material that has been encrypted using the public key. The steps listed below are used to create RSA keys[52, 53].

a. Choose at random p and q, where p and q are both prime.
b. Find the value of n, which has the formula n = p*q and is used as a modulus for both private and public keys.
c. Determine the value of n, where n is the Euler's totient function and n(n) = (p-1) (q-1).
d. Select the integer e, which is used as the exponent for the public key gcd(n),e)=1. This number must be more than 1 and less than (n).
e. If the value of d is less than or equal to the value of, then determine d such that d * e = 1 mod. D is therefore equal to d mod. D must be positive if the value of d is negative, which means that d=(d+).
f. A public key is KU, where KU=e, n.
g. A private key is KR, where KR=d, n.

ii. Encryption

The receiver must maintain the sender's private key secret while sending its public key (n, e) across the channel. Next, the sender wants to deliver message P to the recipient. The sender will first use a padding strategy to convert P into the number m; P1 must be equal to or greater than 0 and less than n.[54].

The sender will do the calculation for the encryption text as the following: -

CP = Pe mod n

P represents plaintext and cipher text is CP , P<n.

iii. Decryption

[55], Using the recipient's own private key exponent d, the original message P can be extracted from the encrypted text CP as displayed below: $P = (C_P)^d \bmod n$

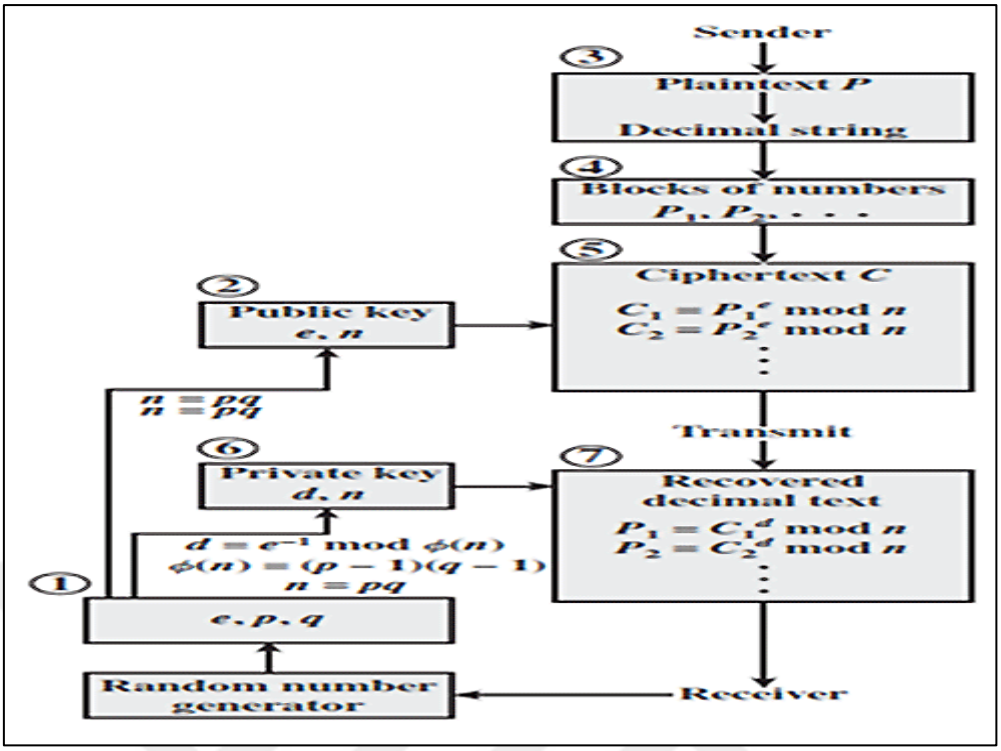


Figure 2.2: RSA Algorithm Working [56].

2.4.3 AES Algorithm

It employs symmetric block cipher technology and is one of the most widely used algorithms today. The National Institute of Standards and Technology (NIST) developed it in response to the need for new cryptographic algorithms to replace ones with security issues. AES features a 128-bit block size and three key sizes of 128, 192, and 256 bits. AES converts each data block several times[57]. The key length for a key value of 128 is 10, 12 for a key value of 196 and 14 for a key value of 256. The block is turned into a 4*4 matrix at the start of the encryption technique, and then the cycles are executed. AES includes mechanisms for clear data content hashing, alternate bytes, row modification, mixed columns, and circular key addition in each round[58]. The technique and stages are reversed during decoding. The pseudo-code for the AES algorithm is shown below[59].

KEY, INPUT STATE

OUTPUT CIPHER

State=AddRoundKey(STATE, KEY[0,…,3]);

```
FOR i =1 to Round
{
STATE = SubstituteBytes (STATE);
STATE = ShiftRows (STATE)
IF (i < Round)
STATE = MixColumns (STATE)
STATE =AddRoundKEY (STATE, KEY [ 4*i, …., 4*i+3]);
}
STATE =CIPHER
```

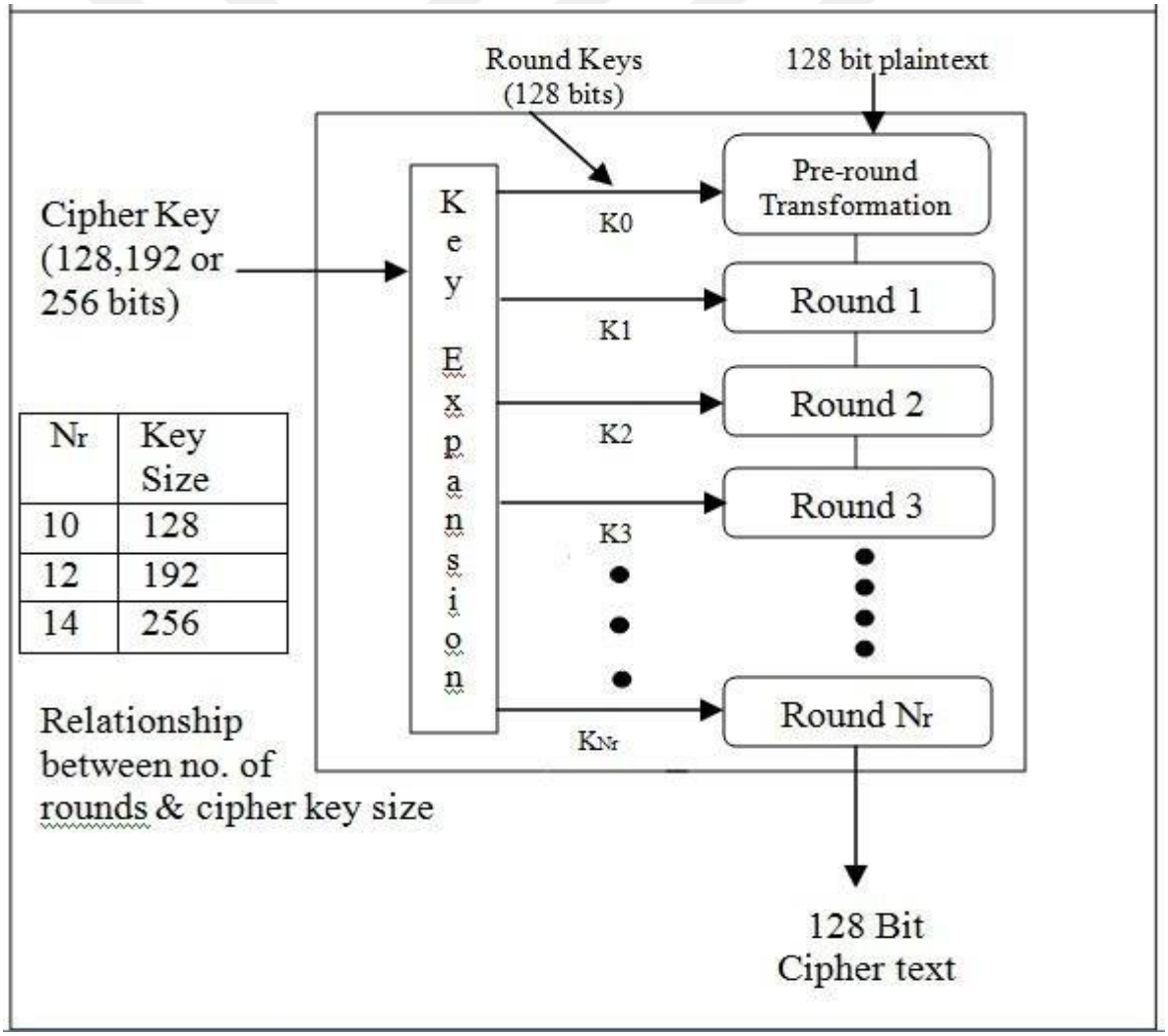


Figure 2.3: AES Algorithm Working [60].

3. METHODOLOGY

3.1 METHODOLOGY

This study used five different grayscale images with sizes ranging from 1920x1080 (as a giant image) to 1600x900 (as a Medium Image), 1600x900 (as a Smedium Image), and 1431x832 (as a small image). The images encrypted with the blowfish, AES and RSA algorithms, and their picture encryption and decryption performance were evaluated using simulations (entropy, elapsed time, SSIM, Histogram, PSNR, and correlation coefficient). The images were taken from Kaggle (https://www.kaggle.com/datasets/aryashah2k/large-scale-multicamera-detection-dataset). Each simulation was created in Python and tested on a machine that met the requirements listed in Table1.

The five photos are displayed in various sizes and forms in Table 1. in addition to their respective byte sizes. As the size in bytes between normal, encrypted, and unencrypted images will differ from the sizes of images processed by the proposed algorithms, the difference in size between normal, encrypted, and unencrypted images will produce different and multiple results if the encryption process is started for both RSA and Blowfish algorithms, AES. This will explain the algorithm's high efficiency in encoding and decoding smoothly and without a significant increase in pixel size. The three algorithms can successfully encrypt all of the photos by masking all of the information and decoding them back to their original form, based on visual judgment. Visual examination alone, however, is insufficient to gauge the effectiveness of encryption techniques; quantitative analysis is also necessary. As a result, (Entropy, elapsed time, SSIM, Histogram, PSNR, and correlation coefficient)are calculated to assess how well the algorithms in the simulation performed at image coding[61].

Table 3.1: Original Images [61].

Image	Original Image
Large Image **(1920x1080)**	 **976,041 bytes**
Big Image **(1920x1080)**	 **796,220 bytes**
Medium Image **(1600x900)**	 **695,555 bytes**
Smedium Image **(1600x900)**	 **675,613 bytes**
Small Image **(1431x832)**	 **289,185 bytes**

3.2 HISTOGRAM ANALYSIS

A simplified illustration of the distribution of numerical data is a histogram. Karl Pearson was the first to use the phrase. When displaying discrete or continuous data, a histogram is utilized. By displaying a percentage of the data points that fall within a given range of values (referred to as "bins"), it provides a visual representation of numerical data. It has a bar chart appearance. Unlike a vertical bar graph, a histogram does not show any gaps between the bars[62]. A histogram shows the frequency of occurrence for each distinct value in a set of data. A histogram is a graph that is used the most frequently to show frequency distributions. Despite how much it resembles a bar chart, there are important differences. This practical data-gathering and analysis tool is one of the seven core quality tools[63]. Examples of histogram analysis include looking at the major local maxima, or simply peaks. Applications determine how exactly to define a significant local maximum. If a local maximum substantially exceeds neigh boring uninteresting values while not being too near to another important local maximum, it is frequently regarded significant. A peak in the histogram is often connected to a particular tissue type in medical imaging data. In the histogram, the tissue types may overlap depending on the imaging modalities and tissue types, resulting in fewer peaks than the actual tissue kinds[64]. A slice of an MRI dataset for the shoulder area is shown in Figure 5, along with the histogram (for the entire dataset).

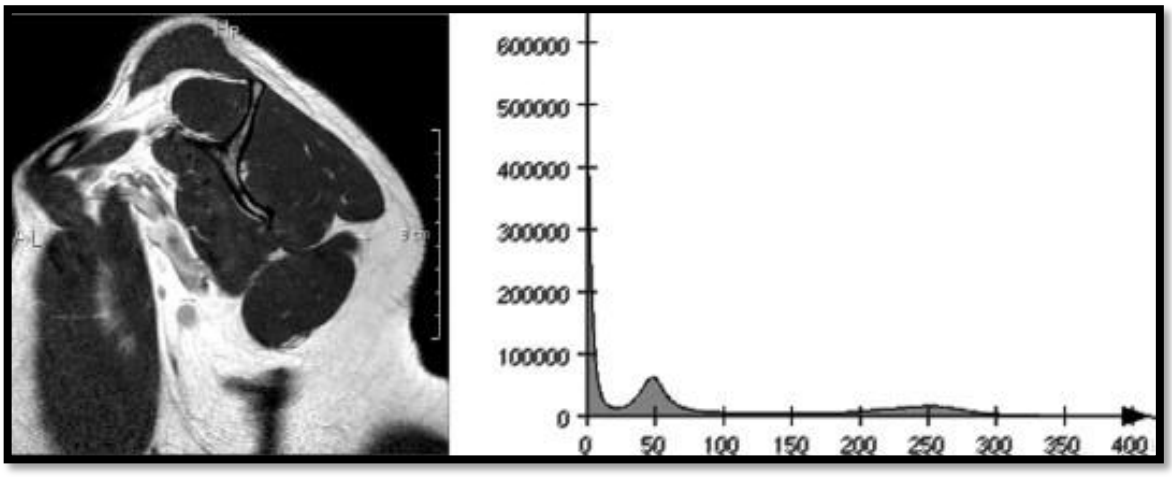


Figure 3.1: An MRI Dataset Slice and A Histogram of the Entire 3D Dataset [65]**.**

The class intervals of the data are shown in rectangles. Rectangular shapes are generated on the X-axis. On the Y-axis, the analyst plots the frequency of the data. Each rectangle represents the number of frequencies that fall inside a particular class interval[66].

Examine the histogram to determine if a normal distribution is depicted. Once all of the frequencies have been plotted on the histogram, the histogram will take on a shape. The frequencies would be evenly distributed if the shape resembled a bell curve. There would be a peak in the histogram. The greatest values in the data are represented by the peak. Both sides of the peak in this type of distribution would have about equal quantities of data frequencies. A normal distribution, for instance, would indicate that the majority of customers are indifferent if a business is utilizing the histogram to understand their preferences between two options[67].

Check the histogram to determine if it shows signs of a skewed distribution. The shape of a skewed distribution histogram is asymmetrical. The histogram's one side is occupied by all of the frequencies. Either the right or left side of the peak is where the distributions are located. The analyst can determine which side of the histogram to focus on using this diagram[68].

With this kind of histogram, the business may observe the most tolerable pricing adjustments, for instance, if it were researching how customers react to price changes.

Examine the histogram to determine if a bi-modal distribution is present. There are two peak spots in these histograms. The highest values are represented by these points. For instance, the business can be evaluating the production levels of the employees throughout the course of the day. The analysis may show that the workers are most productive between the hours of 9 and 4 pm. As a result, the histogram would have two peaks[69].

3.3 CORRELATION COEFFICIENT ANALYSIS

A statistic that describes how closely related the pixels in an image are to one another is the correlation coefficient. The correlation coefficient affects the effectiveness of the encryption procedure as well[70]. Because hackers can utilize correlation data to decode any or all of the ciphered images, an image encryption solution should conceal all features in the plain

image before transforming it into a ciphered image with incompatible pixels and high randomness[71]. Images have correlation coefficients that range from -1 to 1. The degree of a positive relationship (similarity) between pixels in a picture is greatest when the correlation coefficient is one. The negative correlation (contrast) in these pixels is strongest when it equals -1[72]. After encryption, the ciphered image's correlation coefficient should be fairly low. As a result, the plain image and the ciphered image's pixels are no longer correlated. An image may have correlation coefficients in the horizontal, vertical, or diagonal directions. Intensity levels in grayscale for a nxn image are represented by the I matrix[73].

$$I = \begin{bmatrix} I_{1,1} & I_{1,2} & \cdots & I_{1,n} \\ I_{2,1} & I_{2,2} & \cdots & I_{2,n} \\ \vdots & \vdots & \vdots & \vdots \\ I_{n,1} & I_{n,2} & \cdots & I_{n,n} \end{bmatrix} \tag{3.1}$$

The I matrix was split into two submatrices, X and Y, as illustrated in Figs. 1. a, 1. b, and 1. c, to calculate the horizontal, vertical, and diagonal correlation coefficients.

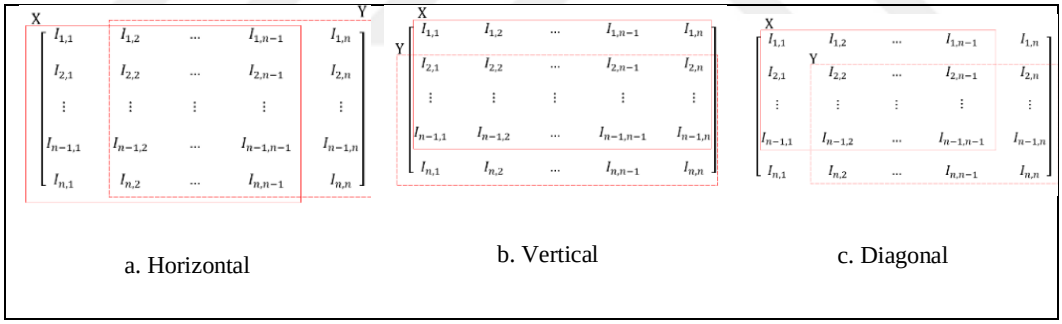


Figure 3.2: I Matrix Splits in the Calculation of the Correlation Coefficient [75].

The correlation coefficient of the I picture is determined using the equivalent elements of the two sub-matrices for a one-to-one comparison[74]. For example, when calculating the [75] The horizontal correlation coefficient is calculated using the variables I_1,1 and I_1,2, the vertical correlation coefficient using the variables I_1,1 and I_2,1, the diagonal correlation coefficient using the variables I_1,1 and I_2,1, and so on. The correlation coefficient of an image is determined mathematically as follows:

$$cc = \frac{\sum_{i=1}^{N}[(x_i - E(x))\,(y_i - E(y))]}{\sqrt{\left[\sum_{i=1}^{N}(x_i - E(x))^2\right]\left[\sum_{i=1}^{N}(y_i - E(y))^2\right]}} \tag{3.2}$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \quad (3.3)$$

$$E(y) = \frac{1}{N}\sum_{i=1}^{N} y_i \quad (3.4)$$

where, correspondingly, x_i from the X matrix and y_i from the Y matrix represent the intensities of two adjacent picture pixels. When computing the horizontal and vertical correlation coefficients, N is equal to (n)x(n-1), while when calculating the diagonal correlation coefficients, it is equal to (n-1)x(n-1)[76].

3.4 PSNR ANALYSING

The PSNR encryption quality indicator displays the pixels that separate plain images from encrypted images[77]. The PSNR analysis accepts the original plain image and the ciphered image as signal and noise, respectively[78]. Lower PSNR values signify better encryption. Here is an example of how PSNR can be calculated:

$$PSNR = 10x\log_{10}\left[\frac{MAX^2}{MSE}\right] \quad (3.5)$$

$$MSE = \frac{1}{nxm}\sum_{i=1}^{n}\sum_{j=1}^{m}[P(i,j) - C(i,j)]^2 \quad (3.6)$$

where MAX represents the maximum value for a pixel can take. MAX is equivalent to 255 if each pixel has eight bits. P stands for the normal image, C represents ciphered image and n, m for the dimensions of the image.

3.5 SSIM (STRUCTURAL SIMILARITY INDEX MEASURE)

By evaluating criteria for brightness, contrast, and structure of anamorphic images, SSIM provides a measure of image quality, the amount of similarity and difference between an image represented via algorithms[79].

$$\text{SSIM}(x, y) = [l(x, y)]^{\alpha}\,[c(x, y)]^{\beta}\,[s(x, y)]^{\gamma} \quad (3.7)$$

Where x and y represent the luminance, contrast, and structure of the deformed pictures in the mathematical model of SSIM above.

3.6 ENTROPY

In the subject of image coding, the entropy or average information of images, refers to a measurement of visual unpredictability. In focused images, entropy is high, whereas in unfocused images, it is low[80]. The entropy image illustrates the robustness and complexity of the coding scheme by showing that the homogeneous regions have a lower share of entropy than the heterogeneous parts. The position of each pixel (i,j) in the image and the corresponding mathematical formula are used to calculate the entropy of the image[81].

$$H1 = \sum_k pk\ log2(pk) \tag{3.8}$$

K stands for the overall number of gray levels, H1 represents entropy, and pk is the probability associated with gray level k.

3.7 THE TIME ELAPSED

Run-time analysis, often known as run-time or execution time, is a theoretical categorization that determines and anticipates an algorithm's increase in running time as its input size (typically denoted by the number n) grows[82]. In computer science, run-time effectiveness is a hotly debated subject: Depending on the algorithm it uses, a program's execution time might range from seconds to years. It is feasible to assess an algorithm's run-time using software profiling techniques however, they are unable to offer time data for all potential inputs[83], by using run-time analysis tools it can only be done theoretically. Other growth rates, such as memory usage, can be predicted using the run-time analysis methodology[84].

The dependability and security of the system will increase when an algorithm completes its operations in real time. The effectiveness of an algorithm is heavily influenced by the speed of encryption and decryption. The properties of the encryption technique being used, as well as the computer's resources like RAM, CPU, and disk, will determine how quickly it can be executed. The implementation of an inefficient algorithm unintentionally or accidentally can have a major negative influence on system performance; hence algorithm analysis is crucial in real-world applications. An algorithm that runs too slowly in time-critical applications may produce results that are no longer relevant or useful. Another factor that can render an

algorithm practically ineffective is if it uses an excessive amount of computational power or storage to run[85].

The dynamics of the signal process and the mechanism of the observation process are frequently merged into a state space model form for use in time series analysis. The ordinary state space model can therefore be used to resolve several fundamental problems in time series analysis, and state space models have been used to create several nonstationary time series models[86]. However, there are numerous circumstances in which a more comprehensive nonlinear or non-Gaussian model is necessary and the regular time series model is insufficient. The use of nonlinear or non-Gaussian time series models is becoming practical with recent advancements in computing capability[87].

4. RESULT

4.1 EXPERMENTAL RESULT

All of the examined outcomes are presented in this section by the goals, which emphasize problem-solving. Results that correspond to levels of statistical significance are presented in this section. it has been offering visual aids for description, such as tables, graphics, figures, and charts. For ease of understanding and clarity, the numerical data are also presented as a bar chart. A bar chart of the scorer's table form, which is also supplied, is shown in the text.

The five photos are displayed in both their encrypted and unencrypted formats in Table 2. Additionally, their size is shown, correspondingly, in bytes. For both the RSA and Blowfish algorithms, the size difference between plain, encrypted, and decrypted images is too similar, in contrast to the AES algorithm, where the size difference in bytes between normal, encrypted, and decrypted images was significantly smaller than the sizes of images processed by other algorithms, indicating the high efficiency of the AES algorithm in smoothly encoding and decoding the images without a significant increase in pixel size. The three algorithms successfully encrypt all photos by obscuring all information, and they successfully decrypt all images to restore them to their original state, according to the visual evaluation. Visual examination alone, however, is insufficient to assess the effectiveness of encryption techniques; quantitative analysis is also necessary. As a result, the picture encryption performance of the algorithms in the simulation is measured using Entropy, elapsed time, SSIM, Histogram, PSNR, and correlation coefficient.

Table 4.1: Visual Forms and Sizes of Original, Encrypted, and Decrypted Images.

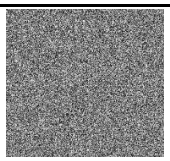
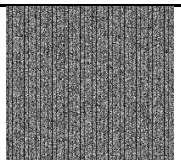
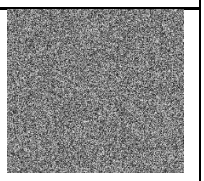
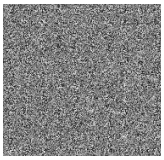
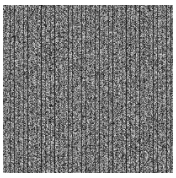
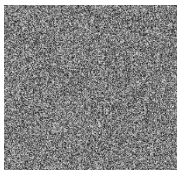
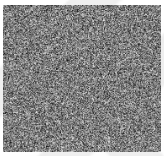
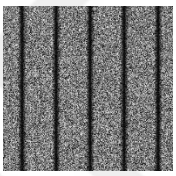
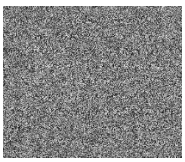
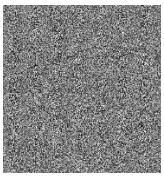
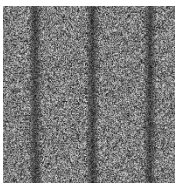
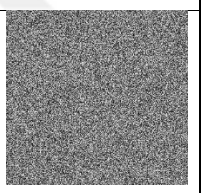
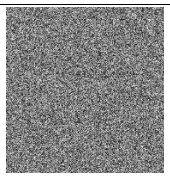
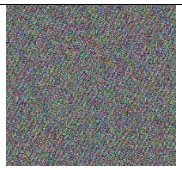
Process	Image	Original Image	AES	RSA	Blowfish
Encryption	Large Image (1920x1080)	 976,041 bytes	 1,152,510 bytes	 2,052,285 bytes	 2,057,450 bytes
	Big Image (1920x1080)	 796,220 bytes	 1,152,540 bytes	 2,061,652 bytes	 2,050,798 bytes
	Medium Image (1600x900)	 695,555 bytes	 803,800 bytes	 1,391,106 bytes	 1,421,572 bytes
	Smedium Image (1600x900)	 675,613 bytes	 803,546 bytes	 1,441,296 bytes	 1,418,612 bytes
	Small Image (1431x832)	 289,185 bytes	 662,519 bytes	 2,472,548 bytes	 3,221,668 bytes
Decryption	Large Image (1920x1080)	 976,041 bytes	 239,097 bytes	 976,041 bytes	

Table 4.1: Visual Forms and Sizes of Original, Encrypted, and Decrypted Images ‘Table Continued’.

Big Image (1920x1080)	 796,220 bytes	 162,132 bytes	 796,220 bytes	 796,220 bytes
Medium Image (1600x900)	 695,555 bytes	 172,657 bytes	 695,283 bytes	 695,283 bytes
Smedium Image (1600x900)	 675,613 bytes	 164,904 bytes	 675,341 bytes	 675,341 bytes
Small Image (1431x832)	 695,555 bytes	 135,721 bytes	 927,897 bytes	 927,897 bytes

4.2 HISTOGRAM ANALYSIS

The ability of an encryption algorithm to cause confusion and diffusion can be assessed using correlation studies and histograms[88]. The intensity levels of each pixel in the image are represented by a frequency distribution in the histogram. The ciphered image is projected to have an even distribution of pixel intensity values, in contrast to the histogram analysis of the plain image, where this is frequently not the case. Because the plain image and the

ciphered image won't look the same in a histogram, hackers won't be able to access your data through a histogram.

For the AES, RSA, and blowfish algorithms, Table 3 displays the histograms of five different sizes of original, encrypted, and decrypted pictures. In contrast to RSA, the blowfish technique successfully encrypts images by dispersing the pixel intensities. Histograms almost uniformly but not entirely obscure all of the statistical information in the source photos. By evenly distributing pixel density values across all encoded images and effectively hiding all statistical information of the source images, AES circumvents Blowfish and RSA in image encryption. Since there is no longer a statistical correlation between the original image and the encrypted image, the encrypted image is far more resistant to intrusion attempts based on statistics.

RSA, AES, and blowfish histograms of original, encrypted, and decrypted photos are displayed in various sizes. Unlike RSA, the blowfish and AES algorithms were successful in encrypting photos by uniformly dispersing and concealing all statistical data from the original photographs, as well as concealing the intensity values of the pixels in the histograms. Because there is no longer a statistical association between the original and encrypted images, the encrypted image is far more resistant to statistically-based infiltration attempts.

Table 4.2: The Histogram of Original, Encrypted, and Decrypted Images.

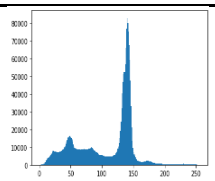
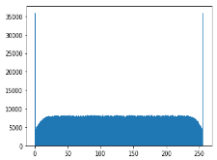
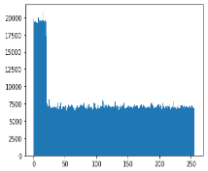
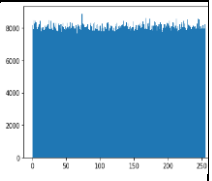
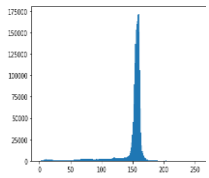
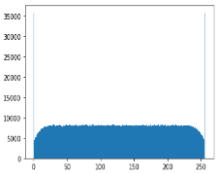
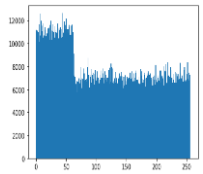
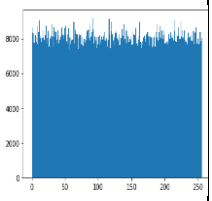
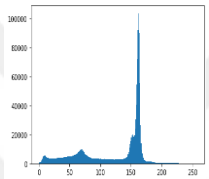
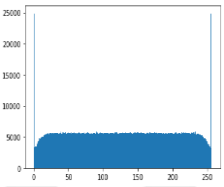
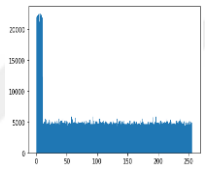
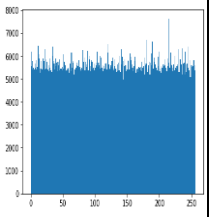
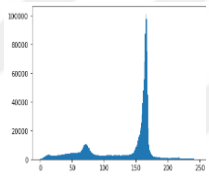
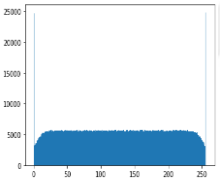
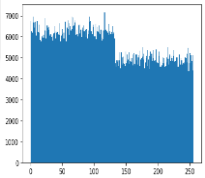
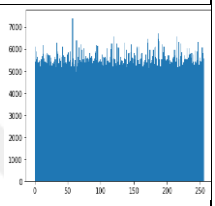
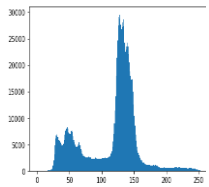
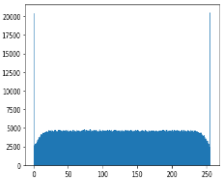
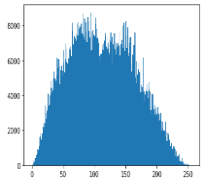
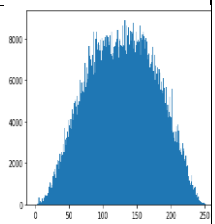
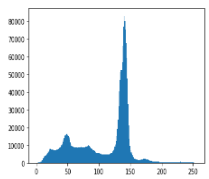
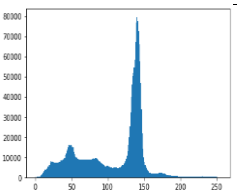
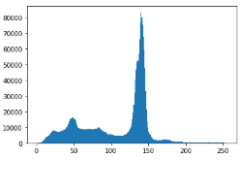
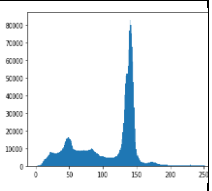
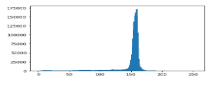
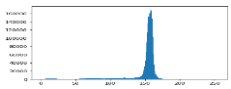
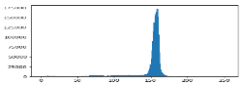
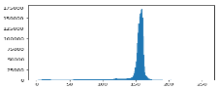
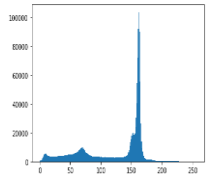
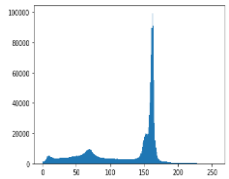
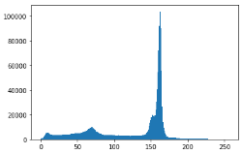
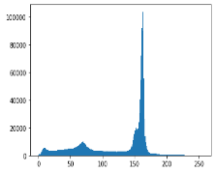
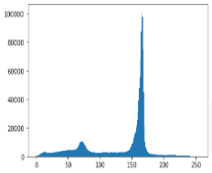
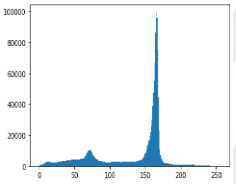
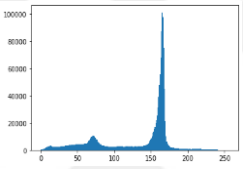
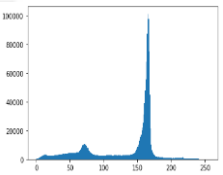
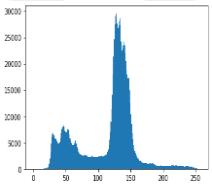
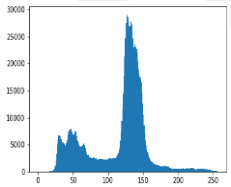
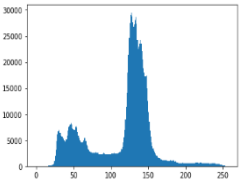
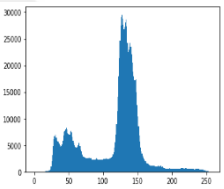
Process	Image	Original Image	AES	RSA	Blowfish
Encryption	Large Image (1920x1080)				
	Big Image (1920x1080)				
	Medium Image (1600x900)				
	Smedium Image (1600x900)				
	Small Image (1431x832)				
Decryption	Large Image (1920x1080)				

Table 4.2: The Histogram of Original, Encrypted, and Decrypted Images' Tables Continued'.

Big Image (1920x1080)				
Medium Image (1600x900)				
Smedium Image (1600x900)				
Small Image (1431x832)				

4.3. CORRELATION COEFFICIENT

The correlation coefficient is a statistic for characterizing the relationship (measuring how closely pixels are related to one another) between pixels in an image. The correlation coefficient also has an impact on how well the encryption process works. Hackers can read parts of or the full ciphered image using correlation data, hence image encryption solutions should mask all features in the plain image before generating a ciphered image with pixels that are uncorrelated and have a high level of randomness[89].

Tables 4 and 5 show the horizontal, vertical, and diagonal correlation coefficients for the original and encrypted images, respectively. The horizontal, vertical, and diagonal correlation coefficients of the original photographs are all more than 0.92, showing that the pixels there are tightly associated to one another. The output values for all horizontal, vertical, and diagonal poles of Table 5's images after they have been encrypted with AES and Blowfish show that all correlation coefficients are very close to zero. These results suggest that, in terms of correlation analysis, both techniques perform very similarly, as opposed to RSA, whose output exhibited no variance in values. Both AES and Blowfish are capable of high amounts of confusion and dispersion.

Table 4.3: Original Image for Correlation Coefficients.

Image	Horizontal	Vertical	Diagonal
Large	0.9814	0.9771	0.9575
Big	0.9780	0.9521	0.9295
Medium	0.9803	0.9765	0.9633
Smedium	0.9817	0.9715	0.9609
Small	0.9811	0.9760	0.9643

Table 4.4: Encrypted Image for Correlation Coefficients.

Image	Horizontal			Vertical			Diagonal		
	AES	RSA	Blowfish	AES	RSA	Blowfish	AES	RSA	Blowfish
Large	-0.0044	-0.0302	-0.0015	-0.0059	0.2399	0.0151	-0.0007	-0.0328	0.0015
Big	-0.0052	-0.0293	-0.0009	-0.0064	0.1757	0.0169	0.0009	-0.0250	0.0011
Medium	-0.0043	-0.0358	-0.0005	-0.0073	0.2542	0.0200	0.0003	-0.0320	-0.0015
Smedium	-0.0058	-0.0059	0.0018	-0.0072	0.0763	0.0213	0.0008	-0.0116	-0.0007
Small	-0.0052	-0.0870	-0.0117	-0.0061	-0.0915	-0.0017	-0.0004	0.2240	0.0171

4.4 PSNR ANALYSIS

The PSNR is a statistic used to assess encryption performance that counts the number of pixels that differ between the encrypted and normal images. The initial, plain image is categorized as noise in the PSNR analysis, but the ciphered image is categorized as signal. A lower value of PSNR indicates a stronger level of encryption[90].

Table 4.5: PSNR Analysis.

Image	PSNR Value for AES	PSNR Value for RSA	PSNR Value for Blowfish
Large	9.1550	8.9496	9.1819
Big	9.8854	9.2989	9.9008
Medium	8.9887	8.4927	9.0190
Smedium	9.1071	9.1151	9.1480
Small	9.3850	11.5298	11.6630

The PSNR values for five photos from surveillance cameras are shown in Table 6 for the AES, RSA, and Blowfish algorithms. Better picture encryption is indicated by lower PSNR values. In a PSNR examination, the RSA and Blowfish algorithms were unable to surpass one another because their values were comparable to and greater than those of the AES method. The AES method, on the other hand, outperformed the others, notably in the small image, with lower and more steady results. Comparing AES to the other proposed algorithms, It can be stated that AES can sufficiently obfuscate picture details from intrusion attacks.

4.5 SSIM (STRUCTURAL SIMILARITY INDEX MEASURE)

By comparing criteria for brightness, contrast, and structure of anamorphic images, SSIM provides a measure of image quality, the amount of similarity and difference between an image that has been encoded using algorithms[91].

In Table 7,8 the degree of similarity and difference between the original images and the encrypted, decrypted images was measured through the criteria of luminance, a contrast in pixels, and image structure to analyze the quality of algorithms.

Table 4.6: SSIM Values for Original & Encrypted Images.

Image	Similarity Value of AES	Similarity Value of of RSA	Similarity Value of Blowfish
Large	0.0092	0.0079	0.0079
Big	0.0101	0.0091	0.0091
Medium	0.0083	0.0074	0.0074
Smedium	0.0092	0.0093	0.0093
Small	0.0096	0.0179	0.0179

Table 4.7: SSIM Values for Original & Decrypted Images.

Image	Similarity Value of AES	Similarity Value of of RSA	Similarity Value of Blowfish
Large	0.9741	1.0	1.0
Big	0.9774	1.0	1.0
Medium	0.9761	1.0	1.0
Smedium	0.9767	1.0	1.0
Small	0.9725	1.0	1.0

The Structural Similarity Index, which ranges in value from -1 to +1, is calculated using this system between two provided images. The number +1 denotes that the two photographs are identical or extremely similar, whereas a value of -1 denotes that the two images are highly dissimilar. These numbers are frequently modified to fall inside the range (0, 1), where the extremes have the same significance.

The results in Table 7 indicate the great similarity of the encryption process between each of the proposed algorithms, with a slight superiority of the AES algorithm in some images, where the values were closer to 0, and thus the value of the difference between the encrypted image and the original is higher. For Table 8, the values for all three algorithms were close to 1, so the decrypted images were very similar to the original images, with a slight superiority for both the RSA algorithm and the blowfish algorithm. We conclude from these criteria that the three algorithms have close encryption ability and hide the details of the original images by 95% with a slight superiority of the AES algorithm. As for the similarity of the original and decrypted images, the three algorithms succeeded in restoring the details of the encrypted images as they are slight superiority to RSA and the Blowfish algorithm.

4.6 ENTROPY

In the context of picture coding, the entropy of images is a measurement of visual unpredictability. In concentrated images, entropy is high, while in unfocused images, it is low. The entropy graphic demonstrates the power and intricacy of the coding method by demonstrating that homogeneous regions have less entropy than heterogeneous areas[92].

Table 4.8: Entropy for Original Images.

Image	Image Processing	Entropy
Big		
Medium		
Smedium		
Small		

Table 4.9: Entropy for Encrypted Images by AES, RSA &Blowfish.

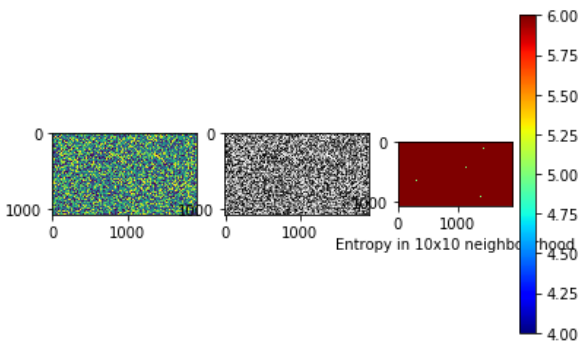
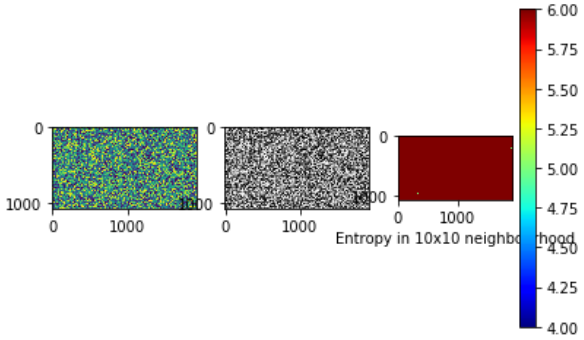
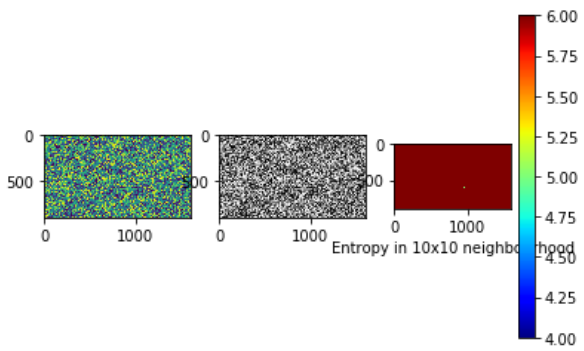
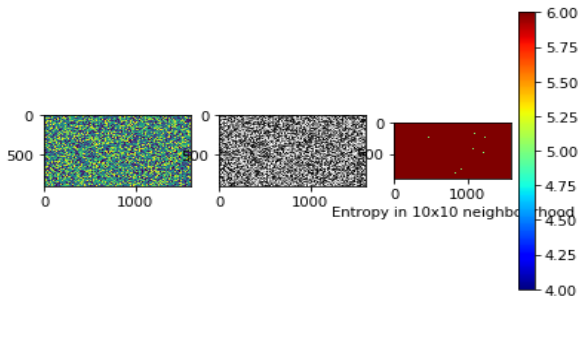
Image	Image Processing	Entropy
Large	**AES Encrypted**	
Big	**AES Encrypted**	
Medium	**AES Encrypted**	
Smedium	**AES Encrypted**	

Table 4.9: Entropy for Encrypted Images by AES, RSA &Blowfish 'Table Continued'.

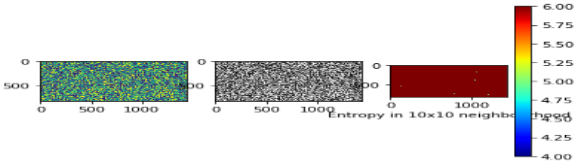
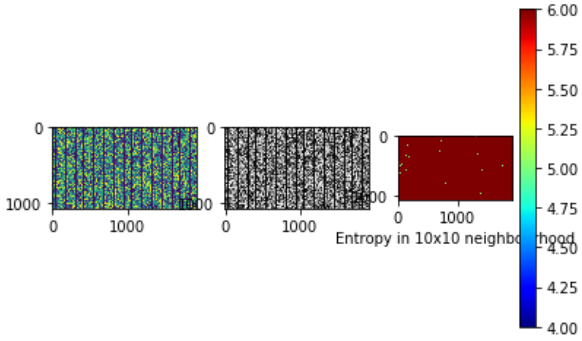
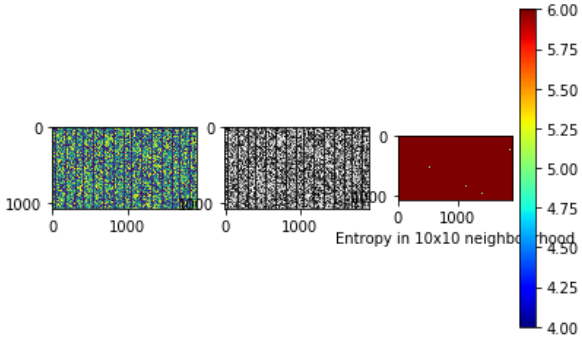
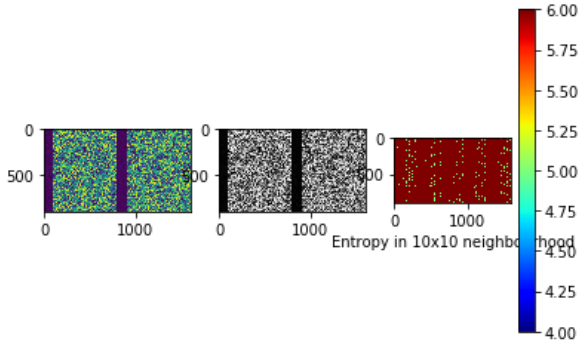
Small	**AES Encrypted**	
Large	**RSA Encrypted**	
Big	**RSA Encrypted**	
Medium	**RSA Encrypted**	

Table 4.9: Entropy for Encrypted Images by AES, RSA &Blowfish 'Table Continued'.

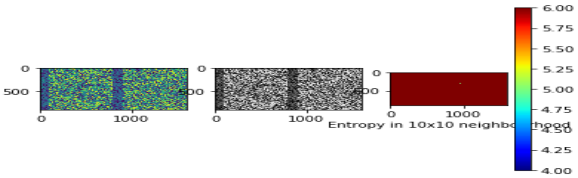
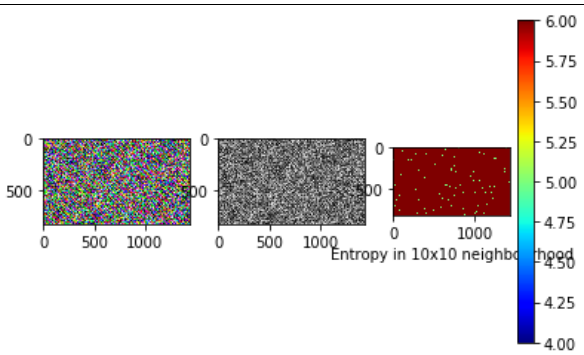
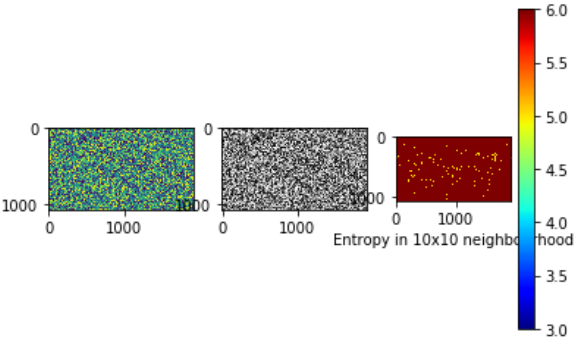
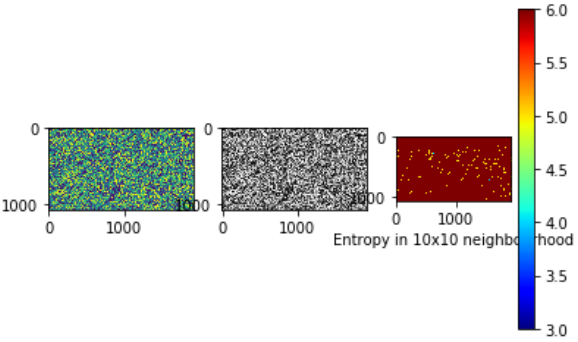
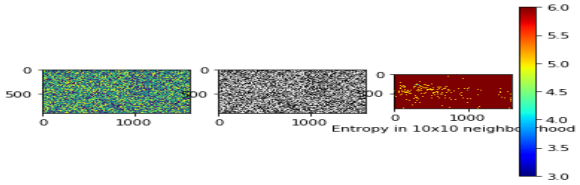
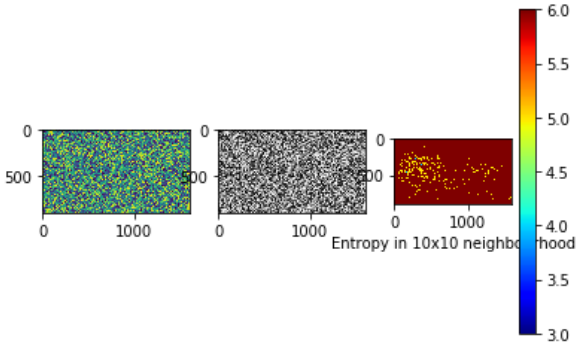
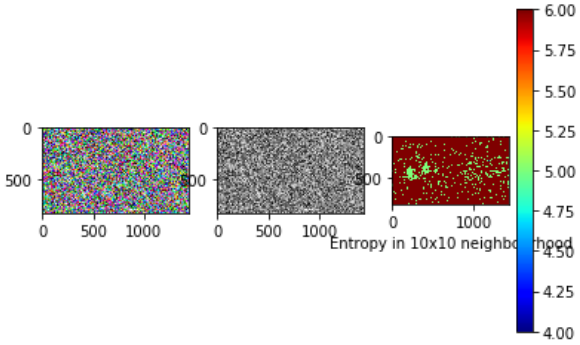
Smedium	**RSA Encrypted**	
Small	**RSA Encrypted**	
Large	**Blowfish Encrypted**	
Big	**Blowfish Encrypted**	

Table 4.9: Entropy for Encrypted Images by AES, RSA &Blowfish 'Table Continued'.

Medium	**Blowfish Encrypted**	
Smedium	**Blowfish Encrypted**	
Small	**Blowfish Encrypted**	

The aforementioned data revealed that images encoded using the AES technique had a high degree of homogeneity, in contrast to images encoded with the RSA and Blowfish algorithms, which had huge entropy values. Due to the intricacy of its coding scheme and the homogenization of pixel coordinates in encrypted images, the AES technology has a higher entropy than the other system.

4.7 ELAPSED OF TIME

The amount of time that elapses between the start and finish of an event is known as elapsed time. Simply put, it is the difference between the two times given[93].

Table 4.10: Elapsed Time For AES, RSA and Blowfish Encryption, Decryption Processes.

Image	The Encryption Time of AES	The Decryption Time of AES	The Encryption Time of RSA	The Decryption Time of RSA	The Encryption Time of Blowfish	The Decryption Time of Blowfish
Large	0.0002	0.0028	6.8599	12.7739	15.1916	30.3832
Big	0.0001	0.0010	6.6928	13.3856	19.6631	39.3263
Medium	0.0059	0.0029	4.9113	9.8227	6.6435	13.2870
Smedium	0.0002	0.0089	3.7261	7.4523	6.0893	12.1786
Small	0.0001	0.0010	5.0098	10.0196	10.6241	21.2483

Table 10 displays the elapsed time for encoding and decoding operations per second for the AES, RSA, and Blowfish algorithms. According to a wide range of tests, the AES algorithm outperformed competing algorithms in the encryption and decryption procedures. The encoding and decoding speed of the AES algorithm is 40% faster than the RSA encoding ability and the Blowfish algorithm by more than 60%.

5. DISCUSSION AND CONCLUSION

5.1 DISCUSSION AND CONCLUSION

The most popular cryptographic algorithms, AES, RSA, and blowfish, have each undergone a thorough performance analysis in this study in terms of security and speed when used to encrypt images from surveillance cameras. Analyses have been conducted using satellite pictures in five distinct sizes. The two algorithms have produced remarkably diverse results in terms of security-related factors. It is advised to use the AES algorithm in cipher operations when the time parameter matters because it performs faster than RSA and Blowfish in both encryption and decryption operations.

In terms of the (histogram, correlation coefficient, entropy, SSIM, elapsed time, and PSNR criteria), AES, RSA, and blowfish achieved substantially varied results while ciphering images. Moreover, the results are unaffected by the image size. These findings demonstrate that the AES algorithms outperform the other algorithm due to their capabilities for diffusion and confusion as well as their resistance to Brute Force attacks. Their security performance differs greatly as a result. Comparing the algorithms based on time criteria, however, reveals that AES is quicker than RSA and Blowfish. This outcome demonstrates that AES is suitable for real-time picture encryption on onboard surveillance camera processors than RSA and Blowfish.

5.2 ADOPTION THE AES ALGORITHM WITH APACHE SPARK

After finding the best algorithm for encrypting surveillance camera images, and to ensure a higher quality of the algorithm, its ability is further improved by applying it within the Apache Spark platform Apache Spark uses the AES method to carry out standalone encoding and decoding operations within Cluster. This is accomplished by installing the PySpark library on the Jupiter platform. The command also needs to set up the latest versions of Java on the PC, jre1.8.0_271, and spark-3.0.1-bin-hadoop2. As in the preceding method, after the AES algorithm's successful adaptation within Apache Spark. Within Spark, a dataset snapshot is encrypted and decrypted, and the elapsed time for both operations is calculated as shown in Table 11.

The encoding and decoding of the five images of different size (Large, Big, Medium, Smedium, Small) were tested using the AES algorithm as normal and the elapsed time was calculated. After that, the AES algorithm was applied inside Apache Spark, and the five images were encrypted. After calculating the elapsed time, a difference in time is shown in (table 12), which proves the improvement of the AES algorithm.

Table 5.1: Normal AES vs AES Apache Spark.

Normal AES Encryption	AES Encryption with Apache Spark
3.3999	2.01

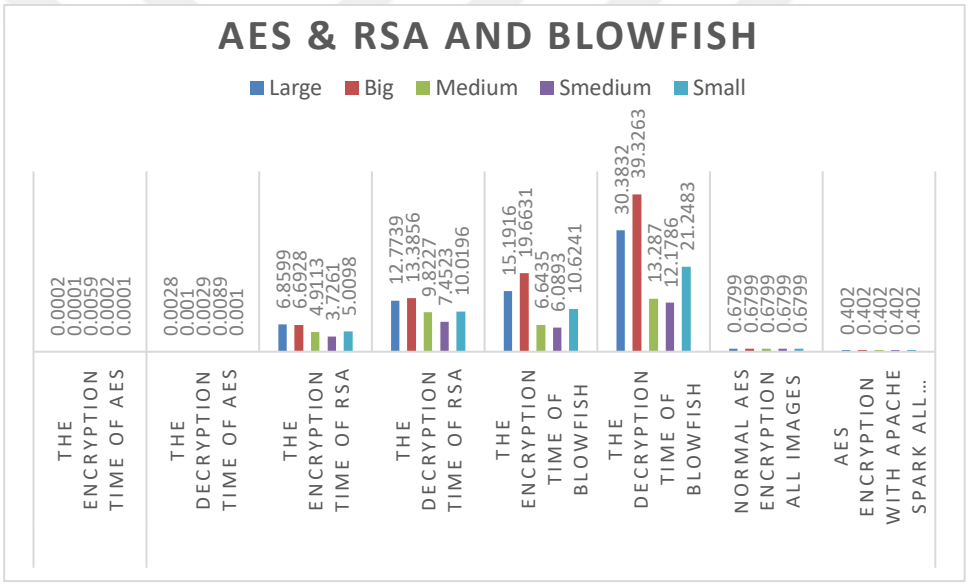


Chart 5.1: AES & RSA and Blowfish Elapsed Time.

The chart shows the superiority of the AES algorithm over the rest of the proposed algorithms in the time elapsed in the normal case when encoding and decoding individual and group images. After developing the algorithm using Apache Spark, the developed algorithm with the speed of execution outperformed itself in the normal state by 20 percent in the calculated times.

5.3 FUTURE PART

The market benchmark for big data analytics has been established by Apache Spark. It has transformed how businesses use data by processing massive volumes of data at breakneck speeds. But with the changing market trends, the future of Apache Spark is not without challenges. Plans must be developed to deal with big data by adapting different algorithms in the field of encryption by working with the Spark platform to develop the capabilities of different encryption technologies to accommodate the huge amount of data, whether it is an image or a video, and others. The real goal of the plan is to expand the range of symmetric and asymmetric encryption algorithms using Apache Spark technology to encrypt huge data of all kinds and give high efficiency to secure data in the monitoring systems of companies, homes, and international agencies and ensure the security of huge data during the process of transmission, storage, and monitoring to prevent falling into The risk of unauthorized entry.

REFERENCES

[1] H. C. Van Tilborg, *An introduction to cryptology*. Springer Science & Business Media, 2012.

[2] G. C. Kessler, "An overview of cryptography," 2003.

[3] S. Pirandola *et al.*, "Advances in quantum cryptography," *Advances in optics and photonics,* vol. 12, no. 4, pp. 1012-1236, 2020.

[4] J. Katz and Y. Lindell, *Introduction to modern cryptography*. CRC press, 2020.

[5] M. T. Gençoğlu, "Importance of cryptography in information security," *IOSR J. Comput. Eng,* vol. 21, no. 1, pp. 65-68, 2019.

[6] M. Gupta, M. Gupta, and M. Deshmukh, "Single secret image sharing scheme using neural cryptography," *Multimedia tools and applications,* vol. 79, pp. 12183-12204, 2020.

[7] M. Bullynck, "Histories of algorithms: Past, present and future," *Historia Mathematica,* vol. 43, no. 3, pp. 332-341, 2015.

[8] V. J. Katz and B. Barton, "Stages in the history of algebra with implications for teaching," *Educational studies in mathematics,* vol. 66, pp. 185-201, 2007.

[9] E. Barbin *et al.*, *A history of algorithms: from the pebble to the microchip*. Springer Science & Business Media, 2012.

[10] M. Kharrich, L. Abualigah, S. Kamel, H. AbdEl-Sattar, and M. Tostado-Véliz, "An Improved Arithmetic Optimization Algorithm for design of a microgrid with energy storage system: Case study of El Kharga Oasis, Egypt," *Journal of Energy Storage,* vol. 51, p. 104343, 2022.

[11] C. B. Boyer and U. C. Merzbach, *A history of mathematics*. John Wiley & Sons, 2011.

[12] B. Note and S. Putty, "In Wikipedia, the free encyclopedia," *Retrieved November,* vol. 19, p. 2007, 2007.

[13] E. Akyürek, D. Schuurmans, J. Andreas, T. Ma, and D. Zhou, "What learning algorithm is in-context learning? investigations with linear models," *arXiv preprint arXiv:2211.15661,* 2022.

[14] L. Dogruel, "What is algorithm literacy? A conceptualization and challenges regarding its empirical measurement," *75898,* vol. 9, pp. 67-93, 2021.

[15] Q. Zhang, "An overview and analysis of hybrid encryption: the combination of symmetric encryption and asymmetric encryption," in *2021 2nd international conference on computing and data science (CDS)*, 2021: IEEE, pp. 616-622.

[16] P. Karthigaikumar and S. Rasheed, "Simulation of image encryption using AES algorithm," *IJCA special issue on "computational science-new dimensions & perspectives" NCCSE,* pp. 166-172, 2011.

[17] C. Li, Y. Zhou, Y. Shen, and C. Yang, "A video selective encryption strategy based on spark," in *2016 IEEE Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC)*, 2016: IEEE, pp. 757-760.

[18] S. Farah, Y. Javed, A. Shamim, and T. Nawaz, "An experimental study on performance evaluation of asymmetric encryption algorithms," in *Recent Advances in Information Science, Proceeding of the 3rd European Conf. of Computer Science,(EECS-12)*, 2012, pp. 121-124.

[19] M. Agoyi and D. Seral, "SMS security: an asymmetric encryption approach," in *2010 6th International Conference on Wireless and Mobile Communications*, 2010: IEEE, pp. 448-452.

[20] A. Alwan and S. Albermany, "Novel Design of RADG Automata In CRNs," 03 2016.

[21] H. Karau, A. Konwinski, P. Wendell, and M. Zaharia, *Learning spark: lightning-fast big data analysis*. " O'Reilly Media, Inc.", 2015.

[22] M. Zaharia, "An Architecture for Fast and General Data Processing on Large Clusters April 2016 https://doi. org/10.1145/2886107.2886114."

[23] A. Arab, M. J. Rostami, and B. Ghavami, "An image encryption method based on chaos system and AES algorithm," *The Journal of Supercomputing*, vol. 75, pp. 6663-6682, 2019.

[24] C.-H. Lin, G.-H. Hu, C.-Y. Chan, and J.-J. Yan, "Chaos-based synchronized dynamic keys and their application to image encryption with an improved AES algorithm," *Applied Sciences*, vol. 11, no. 3, p. 1329, 2021.

[25] Y. Zhang, "Test and verification of AES used for image encryption," *3D Research*, vol. 9, pp. 1-27, 2018.

[26] Q. Zhang and Q. Ding, "Digital image encryption based on advanced encryption standard (AES)," in *2015 Fifth International Conference on Instrumentation and Measurement, Computer, Communication and Control (IMCCC)*, 2015: IEEE, pp. 1218-1221.

[27] D. M. Alsaffar *et al.*, "Image encryption based on AES and RSA algorithms," in *2020 3rd International Conference on Computer Applications & Information Security (ICCAIS)*, 2020: IEEE, pp. 1-5.

[28] S.-H. Shin, W. S. Yoo, and H. Choi, "Development of modified RSA algorithm using fixed mersenne prime numbers for medical ultrasound imaging instrumentation," *Computer Assisted Surgery*, vol. 24, no. sup2, pp. 73-78, 2019.

[29] Y. Luo, J. Yu, W. Lai, and L. Liu, "A novel chaotic image encryption algorithm based on improved baker map and logistic map," *Multimedia Tools and Applications*, vol. 78, pp. 22023-22043, 2019.

[30] P. Singh and K. Singh, "Image encryption and decryption using blowfish algorithm in MATLAB," *International Journal of Scientific & Engineering Research,* vol. 4, no. 7, pp. 150-154, 2013.

[31] L. M. Jawad and G. Sulong, "Chaotic map-embedded Blowfish algorithm for security enhancement of colour image encryption," *Nonlinear Dynamics,* vol. 81, no. 4, pp. 2079-2093, 2015.

[32] A. H. Jassem, A. T. Hashim, and S. A. Ali, "Enhanced Blowfish algorithm for image encryption based on chaotic map," in *2019 First International Conference of Computer and Applied Sciences (CAS)*, 2019: IEEE, pp. 232-237.

[33] I. Landge, B. Contractor, A. Patel, and R. Choudhary, "Image encryption and decryption using blowfish algorithm," *World Journal of Science and Technology,* vol. 2, no. 3, pp. 151-156, 2012.

[34] J. Sócrates-Dantas, R. M. Silveira, D. Careglio, J. R. Amazonas, J. Solè-Pareta, and W. V. Ruggiero, "A study in current dynamic fragmentation-aware rsa algorithms," in *2014 16th International Conference on Transparent Optical Networks (ICTON)*, 2014: IEEE, pp. 1-4.

[35] D. Chen and H. Zhao, "Data security and privacy protection issues in cloud computing," in *2012 international conference on computer science and electronics engineering*, 2012, vol. 1: IEEE, pp. 647-651.

[36] R. Bhanot and R. Hans, "A review and comparative analysis of various encryption algorithms," *International Journal of Security and Its Applications*, vol. 9, no. 4, pp. 289-306, 2015.

[37] J. Wu, L. Ping, X. Ge, Y. Wang, and J. Fu, "Cloud storage as the infrastructure of cloud computing," in *2010 International conference on intelligent computing and cognitive informatics*, 2010: IEEE, pp. 380-383.

[38] A. Nadeem and M. Y. Javed, "A performance comparison of data encryption algorithms," in *2005 international Conference on information and communication technologies*, 2005: IEEE, pp. 84-89.

[39] X. Li, "Application of data encryption technology in computer network communication security," in *Journal of Physics: Conference Series*, 2020, vol. 1574, no. 1: IOP Publishing, p. 012034.

[40] M. Gruteser and X. Liu, "Protecting privacy, in continuous location-tracking applications," *IEEE Security & Privacy*, vol. 2, no. 2, pp. 28-34, 2004.

[41] M. B. Yassein, S. Aljawarneh, E. Qawasmeh, W. Mardini, and Y. Khamayseh, "Comprehensive study of symmetric key and asymmetric key encryption algorithms," in *2017 international conference on engineering and technology (ICET)*, 2017: IEEE, pp. 1-7.

[42] D. S. Abd Elminaam, H. M. Abdual-Kader, and M. M. Hadhoud, "Evaluating The Performance of Symmetric Encryption Algorithms," *Int. J. Netw. Secur.*, vol. 10, no. 3, pp. 216-222, 2010.

[43] V. Poonia and N. S. Yadav, "Analysis of modified Blowfish Algorithm in different cases with various parameters," in *2015 International Conference on Advanced Computing and Communication Systems*, 2015: IEEE, pp. 1-5.

[44] V. P. Bansal and S. Singh, "A hybrid data encryption technique using RSA and Blowfish for cloud computing on FPGAs," in *2015 2nd international conference on recent advances in engineering & computational sciences (RAECS)*, 2015: IEEE, pp. 1-5.

[45] M. N. Khatri–Valmik and V. Kshirsagar, "Blowfish algorithm," *IOSR Journal of Computer Engineering (IOSR-JCE)*, vol. 16, no. 2, pp. 80-83, 2014.

[46] T. Nie, C. Song, and X. Zhi, "Performance evaluation of DES and Blowfish algorithms," in *2010 International conference on biomedical engineering and computer science*, 2010: IEEE, pp. 1-4.

[47] J. Thakur and N. Kumar, "DES, AES and Blowfish: Symmetric key cryptography algorithms simulation based performance analysis," *International journal of emerging technology and advanced engineering*, vol. 1, no. 2, pp. 6-12, 2011.

[48] T. Nie and T. Zhang, "A study of DES and Blowfish encryption algorithm," in *Tencon 2009-2009 IEEE Region 10 Conference*, 2009: IEEE, pp. 1-4.

[49] B. Srinivas, A. Shanbhag, and D. S. Austin Solomon, "A comparative performance analysis of DES and BLOWFISH symmetric algorithm," *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 2, no. 5, pp. 77-88, 2014.

[50] Ç. K. Koç, F. Özdemir, Z. Ödemiş Özger, Ç. K. Koç, F. Özdemir, and Z. Ödemiş Özger, "Rivest-shamir-adleman algorithm," *Partially Homomorphic Encryption*, pp. 37-41, 2021.

[51] H. T. Sihotang, S. Efendi, E. M. Zamzami, and H. Mawengkang, "Design and implementation of Rivest Shamir Adleman's (RSA) cryptography algorithm in text file data security," in *Journal of Physics: Conference Series*, 2020, vol. 1641, no. 1: IOP Publishing, p. 012042.

[52] N. Gilboa, "Two party RSA key generation," in *Annual International Cryptology Conference*, 1999: Springer, pp. 116-129.

[53] H. M. S. Rani, D. H. Mittal, and S. Director, "A Compound Algorithm Using Neural and AES for Encryption and Compare it with RSA and existing AES," *J. Netw. Commun. Emerg. Technol. JNCET*, vol. 3, no. 1, 2015.

[54] D. Boneh, A. Joux, and P. Q. Nguyen, "Why textbook ElGamal and RSA encryption are insecure," in *International Conference on the Theory and Application of Cryptology and Information Security*, 2000: Springer, pp. 30-43.

[55] X. Zhou and X. Tang, "Research and implementation of RSA algorithm for encryption and decryption," in *Proceedings of 2011 6th international forum on strategic technology*, 2011, vol. 2: IEEE, pp. 1118-1121.

[56] M. N. A. Wahid, A. Ali, B. Esparham, and M. Marwan, "A comparison of cryptographic algorithms: DES, 3DES, AES, RSA and blowfish for guessing attacks prevention," *Journal Computer Science Applications and Information Technology,* vol. 3, no. 2, pp. 1-7, 2018.

[57] A. M. Abdullah, "Advanced encryption standard (AES) algorithm to encrypt and decrypt data," *Cryptography and Network Security*, vol. 16, no. 1, p. 11, 2017.

[58] R. Lavanya and M. Karpagam, "Enhancing the security of AES through small scale confusion operations for data communication," *Microprocessors and Microsystems,* vol. 75, p. 103041, 2020.

[59] P. Pandey, R. Tyagi, and D. R. K. Bharti, "Encryption Technique for Secure Password Authentication Scheme at Application Layer," *IOSR Journal of Computer Engineering,* vol. 19, pp. 23-25, 07 2017, doi: 10.9790/0661-1904022325.

[60] M. T. Elkandoz and W. Alexan, "Image encryption based on a combination of multiple chaotic maps," *Multimedia Tools and Applications,* vol. 81, no. 18, pp. 25497-25518, 2022.

[61] K. J. Dana and S. K. Nayar, "Histogram model for 3d textures," in *Proceedings. 1998 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (Cat. No. 98CB36231)*, 1998: IEEE, pp. 618-624.

[62] B. B. Rad and M. Masrom, "Metamorphic virus variants classification using opcode frequency histogram," *arXiv preprint arXiv:1104.3228,* 2011.

[63] H.-D. Cheng and X. Shi, "A simple and effective histogram equalization approach to image enhancement," *Digital signal processing,* vol. 14, no. 2, pp. 158-170, 2004.

[64] T. Arici, S. Dikbas, and Y. Altunbasak, "A histogram modification framework and its application for image contrast enhancement," *IEEE Transactions on image processing,* vol. 18, no. 9, pp. 1921-1935, 2009.

[65] Y.-C. Chang and C.-M. Chang, "A simple histogram modification scheme for contrast enhancement," *IEEE Transactions on Consumer Electronics,* vol. 56, no. 2, pp. 737-742, 2010.

[66] R. Blomley, M. Weinmann, J. Leitloff, and B. Jutzi, "Shape distribution features for point cloud analysis–A geometric histogram approach on multiple scales," *ISPRS Annals of the Photogrammetry, Remote Sensing and Spatial Information Sciences*, vol. 2, pp. 9-16, 2014.

[67] S. Dean and B. Illowsky, "Descriptive Statistics: Histogram," *Retrieved from the Connexions Web site: http://cnx. org/content/m16298/1.11*, 2009.

[68] B. Dzyubak *et al.*, "Automated liver stiffness measurements with magnetic resonance elastography," *Journal of Magnetic Resonance Imaging*, vol. 38, no. 2, pp. 371-379, 2013.

[69] A. G. Asuero, A. Sayago, and A. González, "The correlation coefficient: An overview," *Critical reviews in analytical chemistry*, vol. 36, no. 1, pp. 41-59, 2006.

[70] E. W. Weisstein, "Correlation coefficient," *https://mathworld. wolfram. com/*, 2006.

[71] B. Ratner, "The correlation coefficient: Its values range between+ 1/− 1, or do they?," *Journal of targeting, measurement and analysis for marketing*, vol. 17, no. 2, pp. 139-142, 2009.

[72] Y. Ortakci and M. Y. Abdullah, "Performance analyses of aes and 3des algorithms for encryption of satellite images," in *Innovations in Smart Cities Applications Volume 4: The Proceedings of the 5th International Conference on Smart City Applications*, 2021: Springer, pp. 877-890.

[73] M. Kumari, S. Gupta, and P. Sardana, "A survey of image encryption algorithms. 3D Research 8 (4): 1–35," ed, 2017.

[74] M. Kohrangi, A. N. Papadopoulos, P. Bazzurro, and D. Vamvatsikos, "Correlation of spectral acceleration values of vertical and horizontal ground motion pairs," *Earthquake Spectra*, vol. 36, no. 4, pp. 2112-2128, 2020.

[75] M. Ahmad and O. Farooq, "Secure satellite images transmission scheme based on chaos and discrete wavelet transform," in *International Conference on High Performance Architecture and Grid Computing*, 2011: Springer, pp. 257-264.

[76] Y. Jain, R. Bansal, G. Sharma, B. Kumar, and S. Gupta, "Image encryption schemes: a complete survey," *International Journal of Signal Processing, Image Processing and Pattern Recognition*, vol. 9, no. 7, pp. 157-192, 2016.

[77] M. Kumari, S. Gupta, and P. Sardana, "A survey of image encryption algorithms, 3D Research 8 (4)(2017), 37," ed.

[78] I. Bakurov, M. Buzzelli, R. Schettini, M. Castelli, and L. Vanneschi, "Structural similarity index (SSIM) revisited: A data-driven approach," *Expert Systems with Applications*, vol. 189, p. 116087, 2022.

[79] B. Bein, "Entropy," *Best Practice & Research Clinical Anaesthesiology*, vol. 20, no. 1, pp. 101-109, 2006.

[80] J. Aczél, "Entropies old and new (and both new and old) and their characterizations," in *AIP Conference Proceedings*, 2004, vol. 707, no. 1: American Institute of Physics, pp. 119-126.

[81] P. A. Dinda, "Online prediction of the running time of tasks," *Cluster Computing*, vol. 5, pp. 225-236, 2002.

[82] W. J. Chew, L.-M. Ang, and K. P. Seng, "Automatic model based face feature detection system," in *2008 International Symposium on Information Technology*, 2008, vol. 2: IEEE, pp. 1-6.

[83] H. Andre, F. Girardin, A. Bourdon, J. Antoni, and D. Rémond, "Precision of the IAS monitoring system based on the elapsed time method in the spectral domain," *Mechanical Systems and Signal Processing*, vol. 44, no. 1-2, pp. 14-30, 2014.

[84] B. Kusy, P. Dutta, P. Levis, M. Maroti, A. Ledeczi, and D. Culler, "Elapsed time on arrival: a simple and versatile primitive for canonical time synchronisation services," *International Journal of Ad Hoc and Ubiquitous Computing*, vol. 1, no. 4, pp. 239-251, 2006.

[85] J. J. Paton and D. V. Buonomano, "The neural basis of timing: distributed mechanisms for diverse functions," *Neuron*, vol. 98, no. 4, pp. 687-705, 2018.

[86] A. Bunde, J. F. Eichner, J. W. Kantelhardt, and S. Havlin, "Long-term memory: A natural mechanism for the clustering of extreme events and anomalous residual times in climate records," *Physical Review Letters*, vol. 94, no. 4, p. 048701, 2005.

[87] S.-T. Suo *et al.*, "Histogram analysis of apparent diffusion coefficient at 3.0 T in urinary bladder lesions: correlation with pathologic findings," *Academic radiology*, vol. 21, no. 8, pp. 1027-1034, 2014.

[88] G. Qu, S. Hariri, and M. Yousif, "A new dependency and correlation analysis for features," *IEEE Transactions on Knowledge and Data Engineering,* vol. 17, no. 9, pp. 1199-1207, 2005.

[89] A. Hore and D. Ziou, "Image quality metrics: PSNR vs. SSIM," in *2010 20th international conference on pattern recognition*, 2010: IEEE, pp. 2366-2369.

[90] D. R. I. M. Setiadi, "PSNR vs SSIM: imperceptibility quality assessment for image steganography," *Multimedia Tools and Applications,* vol. 80, no. 6, pp. 8423-8444, 2021.

[91] L. Jost, "Entropy and diversity," *Oikos,* vol. 113, no. 2, pp. 363-375, 2006.

[92] L. Chen, L. Xu, N. Shah, Z. Gao, Y. Lu, and W. Shi, "On security analysis of proof-of-elapsed-time (poet)," in *Stabilization, Safety, and Security of Distributed Systems: 19th International Symposium, SSS 2017, Boston, MA, USA, November 5–8, 2017, Proceedings 19*, 2017: Springer, pp. 282-297.