Abstract__ Now a day multimedia data protection has become a very important process that can be achieved by encryption. Encryption is an essential, effective, and effective component of ensuring secure communication between the sender and receiver by transmitting the information in an unintelligible form and only the authorized recipient can access information. In this paper, we examine the different methods of encryption such as Symmetric, Asymmetric and Chaotic techniques.

**Keywords**: Chaotic, Cryptography, encryption algorithms, Data Encryption Standard (DES), Triple Data Encryption Standard (3DES), Blowfish, Advanced Encryption Standard (AES).

1. INTRODUCTION

In recent years, with the rapid development of computer technology, digital image processing technology has also rapidly developed and penetrated into all aspects of life, such as remote sensing, wireless communication, multimedia systems, medical imaging, telemedicine, and military communication, etc. So the need to secure and reliable means of communication containing images and videos have become extremely necessary to protect private image data from those who illegally try to have access. Image encryption is a significant process to deny any unauthorized user access. Sometime encryption used to increase the ambiguity of the data inside the image when it used with steganography at the same time and watermarking as well. In the keyless cryptosystem, the relationship between the plaintext and cipher text having a different version of the message is exclusively depend on the encryption algorithm. The keyless
cryptosystem is generally less secure than key-based systems because anyone can gain access to the algorithm will be able to decrypt every message that was encoded using keyless cryptosystem such as Caesar cipher. The key-based cryptosystem can be further categories into symmetric key (secret key) encryption and asymmetric key (public key) encryption based on the type of security keys utilized for the encryption or decryption process. The detail of the cryptosystems is explained as follows:

2. **Symmetric encryption**

Symmetric encryption is a type of encryption where only one key is used to both encrypt and decrypt electronic information. The peoples communicating via Symmetric encryption must exchange the key so that it can be used in the decryption process. This encryption method differs from asymmetric encryption where a pair of keys, one public and one private, is used to encrypt and decrypt messages. By using symmetric encryption algorithms, data is converted to a form that cannot be understood by anyone who does not possess the secret key to decrypt it once the intended recipient who possesses the key has the message, the algorithm reverses its action so that the message is returned to its original.

There are two types of symmetric encryption algorithms:

**A. Block algorithm**

Set lengths of bits are encrypted in blocks of electronic data with the use of a specific secret key. As the data is being encrypted, the system holds the data in its memory as it waits for complete blocks. For example, a common block cipher, AES, encrypts 128 bit blocks with a key of predetermined...
length: 128, 192, or 256 bits. Block ciphers are pseudorandom permutation (PRP) families that operate on the fixed size of bits block.

Block encryption algorithms include:

(I) **AES**

The AES encryption algorithm defines a number of transformations that are to be performed on data stored in an array. The first step of the cipher is to put the data into an array; after which, the cipher transformations are repeated over a number of encryption rounds. The number of rounds is determined by the key length, with 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys.

(II) **Blowfish**

Blowfish is a symmetric encryption algorithm, meaning that it uses the same secret key to both encrypt and decrypt messages. Blowfish is also a
block cipher, meaning that it divides a message up into fixed length blocks during encryption and decryption.

(III) DES

Des is a block cipher, and encrypts data in blocks of size of 64 bit each, means 64 bits of plain text goes as the input to DES, which produces 64 bits of cipher text. The same algorithm and key are used for encryption and decryption, with minor differences. The key length is 56 bits.

B. Stream algorithms

Stream algorithms are not retained in the encryption system’s memory, but arrive in data stream algorithms. This type of procedure is considered somewhat safer, since a disk or system is not retaining the data without encryption in the Memory components.

Stream encryption algorithms include:

(I) **RC4** is a stream cipher and variable length key algorithm. This algorithm encrypts one byte at a time or larger units on a time. A key input is pseudorandom bit generator that produces a stream 8-bit number that is unpredictable without knowledge of input key, The output of the generator is called key-stream, is combined one byte at a time with the plaintext stream cipher using X-OR operation

(II) **Seal** (Software-Optimized Encryption Algorithm) is a stream cipher optimized for machines with a 32-bit word size and plenty of RAM with
a reported performance of around 4 cycles per byte.

(III) **Quad** is a modern stream cipher, i.e. it uses a key and an initialization value (IV) to produce a key stream sequence. A Key and IV setup is also defined which also rely on multivariate quadratic system.

**Advantage of symmetric encryption:**

1. The main advantage of symmetric encryption over asymmetric encryption is that it is fast and efficient for large amounts of data; the disadvantage is the need to keep the key secure.

2. One of the drawbacks to public key encryption systems is that they need relatively complicated mathematics to work, making them very computationally intensive. Encrypting and decrypting symmetric key data is relatively easy to do, giving you very good reading and writing performance. In fact, many solid state drives, which are typically extremely fast.

**Disadvantage of symmetric encryption:**

1. When someone gets their hands on a symmetric key, they can decrypt everything encrypted with that key. When you're using symmetric encryption for two-way communications, this means that both sides of the conversation get compromised. With asymmetrical public-key encryption, someone that gets your private key can decrypt messages sent to you, but can't decrypt what you send to the other party, since that is encrypted with a different key pair.

2. Disadvantage is the need to keep the key secret. This can be especially challenging where encryption and decryption take place in different locations, requiring the key to be moved.

**3. Asymmetric encryption**

A technique used for keeping sensitive information safe, asymmetric encryption is a popular one. Read our article and learn more about what asymmetric encryption is and how it can be useful for your organization. Each and every day, we send massive amounts of personal or sensitive data over the internet. For business purposes, entertainment, shopping, health services and more, we exchange tons of important information. Even for
logging on to social media platforms, we type and send our password and username. That is why, keeping such data safe has gained utmost importance. As a result, various cyber security techniques including encryption are being used. Being one of the two main kinds of encryption, asymmetrical encryption is often preferred. In this article, we will take a closer look at what asymmetrical encryption is and how it can be helpful for your organization. Asymmetrical encryption (is defined a public key cryptography) is an encryption system that uses a pair of different keys. In comparison to the symmetrical encryption method, asymmetrical encryption is a newer system. As the name implies, the keys used in this method are not identical to one another. One of the keys are often shared with many people and called the public key. Other one is not shared and aptly, it is called the private key. Together the two are called Private and Public Key Pair. Asymmetrical encryption work by Even though the two keys used in asymmetrical encryption are different from one another, they complement each other. Often, the public key is used for the encryption purposes. The sender encrypts their message with the public key, so that nobody but the intended recipient can access the content. On the other hand, the intended receiver possesses the private key. When they receive the encrypted message by the sender, they decrypt it with the help of their private key. This way, an unauthenticated party cannot decrypt the message even though they somehow manage to get the message itself. In order to put things in perspective, let’s illustrate the whole key and lock ordeal with an analogy.

**critical information** Let’s say that you are in charge of an agency that coordinates spies. Naturally, your agents need to communicate with you in a safe and secret way. You give the public key to your agents and keep the private key yourself. Your agents encrypt their message with their keys, so if their messages are captured by the third parties none of the sensitive information will be spilled. At the headquarters, you, the only holder of the private key can decrypt the messages from your agents and access the critical information.

**The applications of asymmetrical encryptions:**
Asymmetrical encryption can be used for many different purposes, but the most apparent one is, as our analogy above suggests, ensuring the confidentiality. In other words, you can use asymmetrical encryption in
order to make sure that your message is not read by any other parties than your intended, authorized recipient.

Moreover, asymmetrical encryption techniques can be used for providing sender authentication. In order to do so, asymmetrical encryption is implemented into the digital signature.

This type of encryption can also be used in non-repudiation protocols, password-authenticated key agreement, digital cash and many more applications.

It might be beneficial for you to check SIEM and SOAR solutions of Log sign in order to protect your business from cyber threats

**Advantages**

The private key does not need to be transmitted via a secure channel (as opposed to the symmetric encryption) in order for the encryption to be successful.

There is the possibility of an electronic signature (digital signature)

**Disadvantages**

The high cost to encrypt and decrypt messages much slower compared to symmetric encryption.

**CHAOTIC TECHNIQUES**

Chaotic cryptography is the application of the mathematical chaos theory to the practice of the cryptography. The advantages of using this method over traditional encryption algorithms is to provide encryption with high security, speed, reasonable computational overheads, sensitive dependence on initial conditions, no periodicity, nonconference, and computational power requirements. Chaos theory was invited by Edward N Lorenz in 1963. Chaos theory has been established since 1970s by many different research areas, such as mathematics, physics, engineering, biology, economics, and philosophy, etc. In common usage, chaos means a state of disorganization. Since there is no universally accepted mathematical definition of chaos, a commonly used definition is that, for a dynamical system to be said as chaotic, it must have the following
Features: 1) It must be sensitive to initial conditions, 2) Its periodic orbit must be dense, and 3) It must be topologically mixing. Two examples must be considered: Chaotic map and Hyper-chaotic map. **Chaotic map**

The logistic map is the simplest chaotic map and the most transparent system in which the transition to chaos is obvious. The encryption scheme for chaotic map is consisting of two steps: permutation and diffusion process as shown as in Fig.

![Image](image.png)

The image encryption process includes permutation and diffusion process. The chaotic logistic maps are used to generate random sequence to scramble and diffuse the original image pixels. In permutation process, pixels of the original image will be scrambled in spatial domain. While in diffusion process, the randomly generated binary sequence will be masked with bits of pixel in the original image.

**Hyper-chaotic map**

Hyper-chaotic map is a high-dimensional chaotic system and is safer than low-dimensional chaotic maps when used in cryptographic algorithms because high-dimensional chaotic systems are better sensitive, larger key space, more randomness and complex dynamic characteristics such as 5D multi-wing hyper-chaotic system.

**conclusion**
in this paper, we delivered image encryption algorithms together with the Advanced Encryption Standard (AES), and also the encoding Standard (DES) are no longer reliable in digital photo encryption given the huge Statistics capacity. Symmetric encoding algorithms is classed into stream ciphers and block ciphers wherever the image-pixels are encrypted one-by-one in stream ciphers and victimization blocks of bits in block ciphers. The parallel secret writing is utilized for bulk knowledge transmission. Symmetric secret writing is quick in execution. Parallel secret writing uses one key for every encryption and cryptography. Algorithms DES, AES, and RC4 and chaos may be a regular thing of engineering dynamics going down during a huge quite troubles. Within the presence of dissipation a non-stop enter of power is required for chronic chaos producing chaotic attractors. The need of regularity within the forcing limits the big variety of really (mathematical) chaotic structures. And Asymmetric encryption is additionally called Public Key Cryptography, since users usually create the same key pair, while keeping the opposite secret. Through encrypting a message with the recipient's public key, users may submit hidden messages. During this scenario, the message are often decrypted only by the intended recipient as only that person will have access to the right secret key.