**IMAGE ENCRYPTION TECHNIQUES**

**Modified AES:**

The Advanced Encryption Standard (AES) is used as a standard by the U.S. government and various organizations. It is highly efficient in its basic 128-bit form and uses 192 and 256-bit keys for some robust encryption. AES is hailed as more effective than its predecessors such as Triple DES as it uses longer and more complex keys. The decryption is fast and finds applications in firewalls, routers or any other application that uses encryption. It is considered impervious to any attack except brute force that can try to decipher all the 128, 192 or 256-bit encryptions. It is thought to become the standard in the private sector soon as well. Modified AES is a modified AES algorithm. It is formed by the AES algorithm and a key stream generator. The latter has two different forms; (i) A5/1 key stream generator and (ii) W7 key stream generator

**Triple DES:**

Triple DES was designed as a successor to the once extensively used Data Encryption Standard (DES) algorithm. This symmetric-key method of data encryption was made obsolete by the hackers who constantly exploited its vulnerabilities. The algorithm uses a 56-bit individual key with the total key length adding up to 168 bits. However, since it is consecutive encryption, there is a middle-level vulnerability that decreases its protection to the level of a 112-bit key.

Because of the complexity in the way it works, the Triple DES encryption is slower, but still, its effectiveness is good enough to keep it as one of the approved data encryption algorithms till 2030. It is also slowly phased out and used for its dependability in financial services and other industries as a hardware encryption solution.

**RSA:**

The Rivest-Shamir-Adleman (RSA) is established as the standard public-key encryption algorithm. It is asymmetric because it has a public and a private key that encrypts data being sent and received. The encryption is starting on the RSA algorithm with the selection of two large prime numbers, along with an auxiliary value, as the public key. The prime numbers are keep in secret. The public key is used to encrypt a message, and private key is used to decrypt a message or information. Its scrambling level takes far too much time for any attackers to break and keeps communication quite secure. The keys for the RSA algorithms are generated by multiplying the large prime number and creating a modulus. Since the numbers involved are large, it makes RSA much safer than DES. While the Triple-DES works with keys equivalent to 112 bits, the RSA keys are 1024 to 2048 bits long. However, the 2048-bit keys are recommended by the government and IT industry.

**Chaotic System:**

The term chaotic comes from “chaos” meaning confusion. It refers to a state that does not have a deterministic behavior and is a complex system that shows sensitivity towards initial conditions. Techniques focused on chaotic systems was studied and analyzed extensively in the recent years and because of its reduced mathematical complexity and better safety, this scheme is becoming influential. The encryption comprises of two components: confusion phase and diffusion phase. In confusion phase, the original or plain RGB image is partitioned into three color channels red, green and blue after that block scrambling is carried over where the image is split into blocks of sixteen. With the resultant, arnold cat map is performed to shuffle the pixels of the color image. Row-Column wise scrambling is conducted after implementing the arnold cat map.

**BlowFish:**

Developed in 1993, the Blowfish encryption algorithm is an alternative for Data Encryption Standard (DES). The developer placed the protocol to the public to make it readily available for any interested user.Compared to DES, it is substantially faster and offers better encryption security.

It is an asymmetric type of encryption protocol: uses a single key for both encryption and decryption. It is a significantly fast operation because it involves a relatively small number of rounds as well as its clarity of functionality.

Nevertheless, its key-scheduling consumes a lot of time, although it has an upper hand when it comes to protecting brute-force threats.

Also, its 64-bit block length (size) is rather small making it endangered by birthday attacks compared to AES whose block size is 128 bits and above.

**Image Encryption using Affine Transform and XOR Operation**

It is a symmetric key encryption technique that first scrambles the locations of pixels

using 4 8-bit sub keys and then encrypt the pixel values by XOR the selected 9-bit key. The scrambling operation is done using Arnold transformation cipher techniques that breaks the correlations of the neighbouring pixels and make image unidentifiable. The XOR operation then changes the pixel values making the image very meaningless.

**TwoFish:**

This form of the encryption algorithm is a [symmetric key block cipher](https://www.sciencedirect.com/topics/computer-science/symmetric-key-cryptography) which is characterized by 128-bit block size and whose keys’ size can run up to 256 bits.

This protocol uses one key for encryption and decryption.

It is a fast and flexible standard for eight-bit and thirty two-bit CPUs, and small smart cards. The protocol works exemplarily in hardware and has numerous functionality commutations between the speed of encryption and the setup time making it distinctive amongst other protocols. The standard shares some features with its predecessor, blowfish Encryption Algorithm and AES. At one time, this encryption algorithm was a real contestant for the best encryption standard, but the present AES beat it out. This algorithm bears several peculiar characteristics that distinguish it from other standards.