

Performance Analysis of Symmetric and Asymmetric Encryption Algorithms in Digital Images

Mehmet HACIBEYOGLU
Necmettin Erbakan University

Bashir Sheikh Abdullahi JAMA
Necmettin Erbakan University

Introduction

With the progression of innovation and the internet, the main issue about information security and protection has arisen (Furht, Socek, & Eskicioglu, 2004). Many individuals these days are worried about their data being taken while looking for data on the internet. We carefully peruse the internet for data or share significant data with associates, as though somebody was gazing at us out the window. A thought known as information encryption has been introduced as an answer for this issue. Information encryption is the demonstration of diverting information from a plain message or clear, design into a format that the right sender and planned recipient can comprehend. Encoded information ordinarily shows up as a long line of arbitrary letters and numbers. The expected beneficiary of the information has the key or an exceptional means to change over the information from encoded to the decoded structure (Davis, 1978).

Recently days, the attackers is utilized an approach known as a brute force which endeavor arbitrary keys until they obtain the fitting one which is the most basic method of attack on encryption. The length of the key impacts the number of keys that can be utilized and the persuasiveness of this attack. It's memorable's crucial that while encryption strength is straightforwardly connected with key size, the quantity of resources needed to do the computation raises as well (Bhanot & Hans, 2015). Data encryption ensures the security of advanced information as it is put away on computer network frameworks and conveyed across the internet or other network systems (Davis, 1978). Encryption should be appropriately intended to try not to dial back a framework's exhibition. Equipment, such as chips or hard drives, operating frameworks, like MS Windows or Linux, and encryption programs from NIST-ensured providers are the three levels of encryption, recorded from best to most exceedingly terrible execution. As indicated by merchant benchmarks for every one of the three degrees of encryption, frameworks will scarcely lose a small portion of a percent of their speed, and the end client won't see the distinction. To check these statements, more benchmarks might be required. This data might be accessible from staff who give specialized help to different projects at your foundation; if not, the CDC's NPCR can work with NPCR projects to build up a rundown of benchmarks (Furht et al., 2004).

Image encryption has been the subject of broad exploration of research. A picture encryption plot is introduced in which the places of picture pixels are rearranged and the dim upsides of image pixels are changed to befuddle the connection between the encrypted picture and the plain picture (Guan et al., 2005). The Arnold feline guide is utilized to rearrange the places of image pixels in the spatial space in this procedure. From that point onward, Chen's turbulent framework's discrete result signal is preprocessed to make it satisfactory for grayscale picture encryption. An astounding picture encryption algorithm the usage of a plane little bit of a source image changed into delivered as bitplane bit safety key to scramble pics to work on protection picture encryption strategies primarily based on bitplane bit decay (Zhou et al., 2014). To scramble the photographs, Ye et al. (2010) utilized the strategic guide. The stage is done at the piece level in this technique. This technique is impervious to an assortment of security attacks. Zhu et al. (2011) suggested a piece-level change and dissemination algorithm for picture encryption. Change and dissemination activities are performed utilizing the Arnold map and strategic guide in this strategy.

Kanso et al. (2012) used a three-layered Arnold change to create secret keys to encode the pictures. This approach is broken into three stages rearranging, scrambling, and veiling. This method is very touchy to the picture utilized as a piece of information. It secures against known plaintext and picked plaintext assaults all the more viably. Khan and Shah (2014) worked on the mathematical and factual elements of the S-confine by carrying out it in a turbulent way using relative and Lorenz changes. S-confine is for the most part utilized square encryption to make pixels become confounded. It works on the disarray and dispersion of the information picture to shield it from security attacks.

Material and Methods

Encryption methods are arranged by three standards. The first is the number of keys utilized by the encryption process (zero, one, and two keys), the second is the operation type of the encryption algorithm (substitution, displacements, and production), and the third is the plain text handling structure utilized by the encryption calculations (block-based and stream-based). Besides, the encryption methods are extensively ordered into fundamental classes: Symmetric and asymmetric encryption (Sharif et al., 2010).

Symmetric encryption utilizes a solitary, private key for encryption and unscrambling. It is a quicker strategy than unbalanced encryption and is best utilized by people or inside shut frameworks. Involving symmetric strategies with numerous clients in open frameworks, for example, over an organization, requires the transmission of the key and sets out freedom for robbery. The most regularly utilized kind of symmetric encryption is AES (Sharif et al., 2010).

Asymmetric encryption utilizes a couple of numerically connected public and private keys that must be utilized together. Encryption should be possible with one or the other

key, yet unscrambling should be finished with the related key. Since the public key might be uninhibitedly traded without gambling information burglary, awry encryption is used by different clients and over open organizations, like the Internet. ElGamal, RSA, DSA, and PKCS are the most routinely utilized sorts of hilter kilter encryption (Lai et al.,2010).

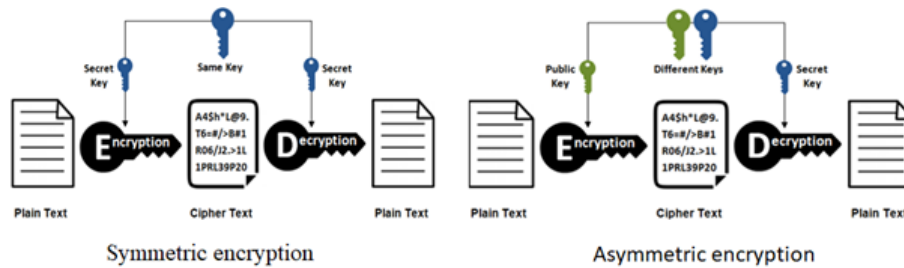


Figure 1. Symmetric encryption and asymmetric encryption processes (“Symmetric vs. Asymmetric Encryption,” 2022)

Data Encryption Standard Algorithm

The Data Encryption Standard is a block-based symmetric-key methodology for the encryption of different forms of information in 64-digit blocks. This suggests that 64 pieces of plain text are taken care of into DES, which produces 64 pieces of ciphertext. Encryption and unscrambling utilize a similar calculation and key, with slight varieties. The DES algorithm has a 56-bit key length. Since the DES approach has been demonstrated to be helpless against amazingly strong assaults, its prevalence has been on disappearing (Kansal & Mittal, 2015).

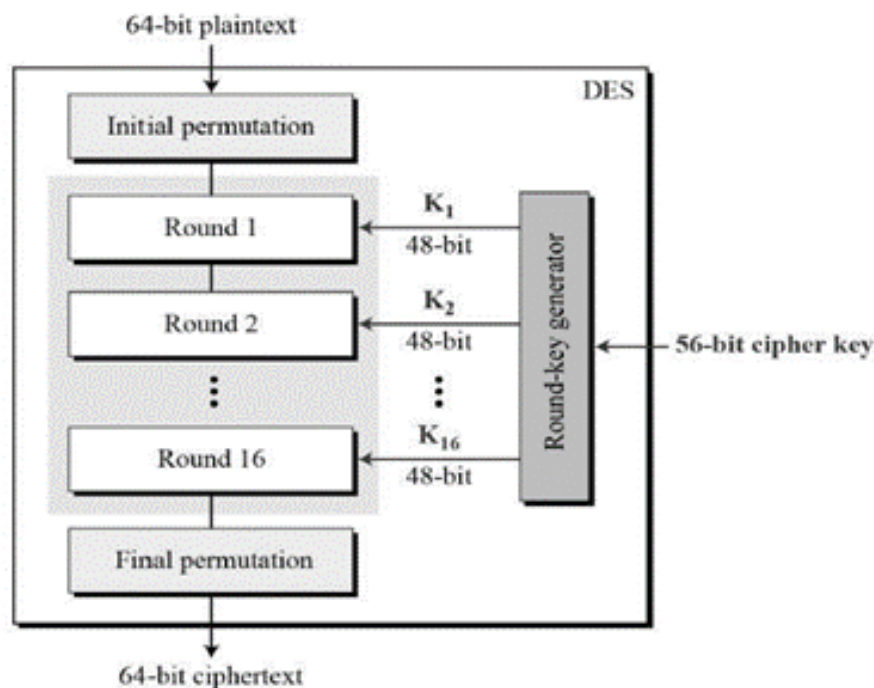


Figure 2. DES algorithm operation procedure (“Data Encryption Standard”, 2022)

DES is a block-based approach depending on the Feistel Cipher, the method should determine three fundamental things needed for the encryption operation, in particular the Round work, the Key table, and the First and last permutation. The first and only changes are straight Permutation boxes (P-boxes) that are inverses of one another. They have no cryptography importance in DES (Kansal & Mittal, 2015). The underlying and last changes are displayed in fig (3).

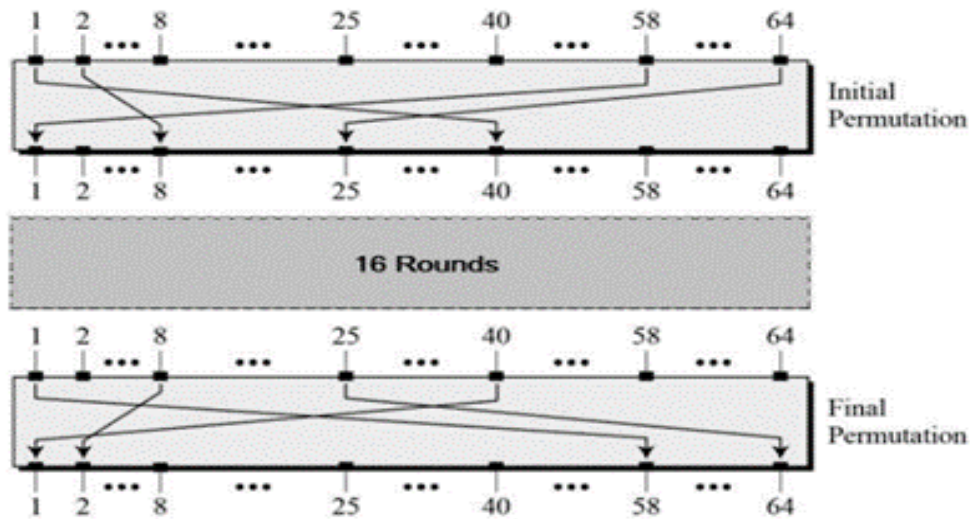


Figure 3. DES algorithm operation procedure (“Data Encryption Standard”, 2022)

After performing the first and last permutation, the round function f was used, which applied a 48-bit key to the rightmost 32 bits to produce a 32-bit output.

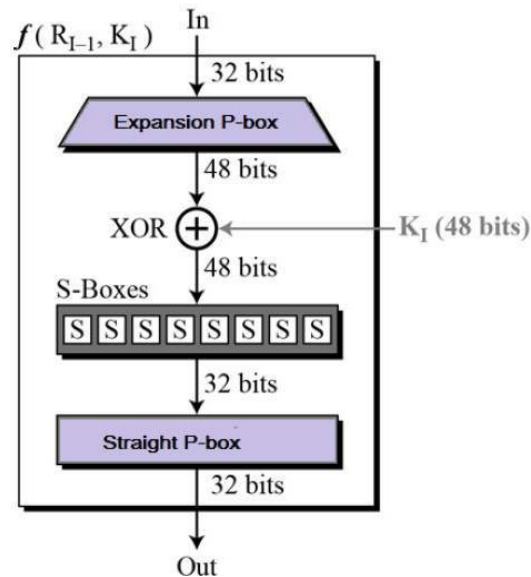


Figure 4. DES algorithm operation procedure (“Data Encryption Standard”, 2022)

Since the round key is 48 parts and the correct facts (data) are 32 bits, it's miles expected to first decorate the suitable contribution to forty eight components in the DES path, that's the execution of the improvement exchange field.(Davis, 1978).

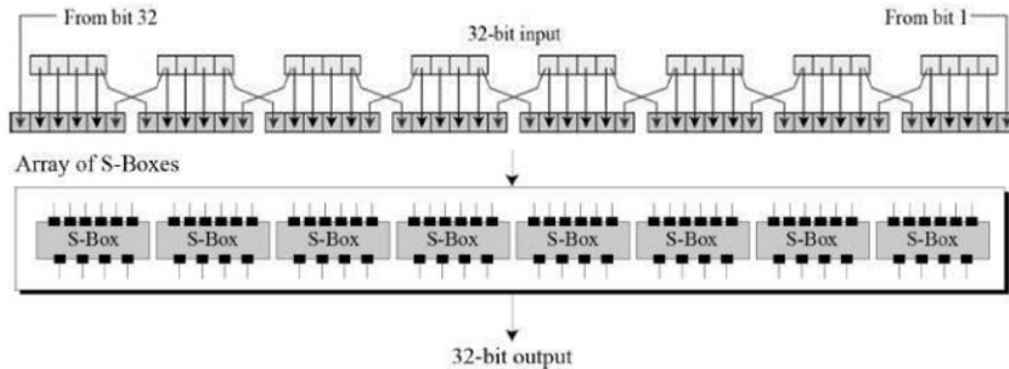


Figure 5. Demonstrates key expansion and XOR of DES algorithm (“Data Encryption Standard”, 2022)

Key creation is the penultimate stage in the DES method’s encryption cycle, which creates sixteen 48-piece keys from a 56-digit figure key. Figure 6 portrays the key creation process.

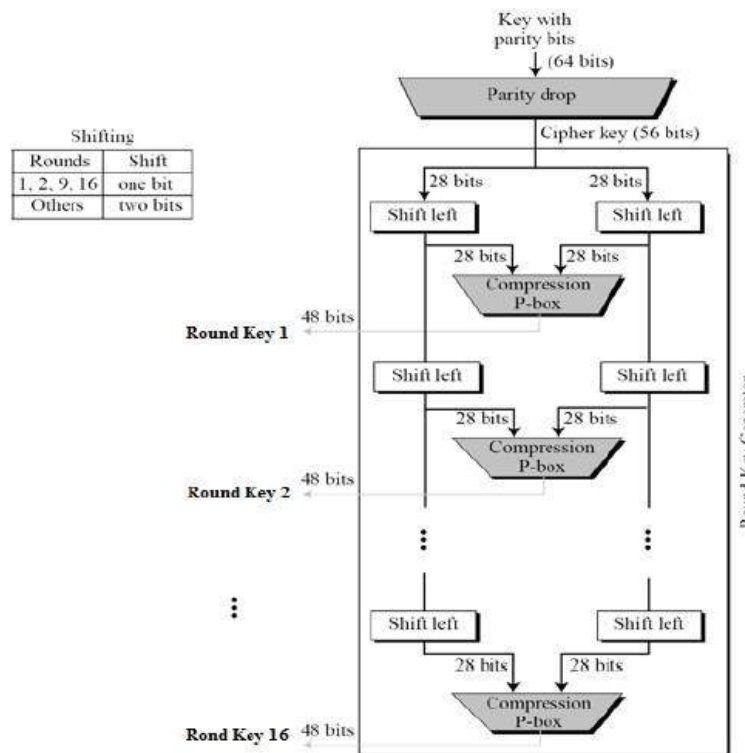


Figure 6. Key generation of DES algorithm

Triple DES

The DES cipher is repeated three times to produce the Triple DES block cipher algorithm. The Triple DES algorithm is called TDES or TDEA (Triple Data Encryption Algorithm). (Barker & Mouha, 2017). TDES was selected as a straightforward option to expand the key space without switching to a novel algorithm after it was discovered that a 56-bit key DES was insufficient to prevent brute force assaults. To keep away from meet-in-the-center attacks, which might be a hit with double DES encryption, 3 strategies are required. 3DES is a frequently utilized encryption technique in the financial industry. It’s to up amazing the preceding block cipher DES. It has some of advantages, which include

ease of implementation in each hardware and software program, and wide approval among cryptographic libraries as well as protocols. 3DES improves the security of DES by using three 56-bit keys DES instead of two keys. (Cardarilli, Di Nunzio, Fazzolari, & Re, 2015). The following is a description of the 3DES encryption method, where K1, K2, and K3 are the three 56-bit keys.

3DES Encryption Algorithm:

- Begin the encryption process of plaintext with the use of the K1 and the DES method.
- In the second step, decryption is executed on the encrypted output by using the DES algorithm and K2.
- The decrypted output should be encrypted another time using the DES algorithm and K3.

This kind of encryption technique produces the output of the 3DES cipher text.

3DES Decryption Algorithm:

- The cipher picture can be decrypted using the DES and K3.
- The decrypted output should be encrypted using the DES and K2.
- To covert the encrypted data that has been decrypted, use the DES and K1.

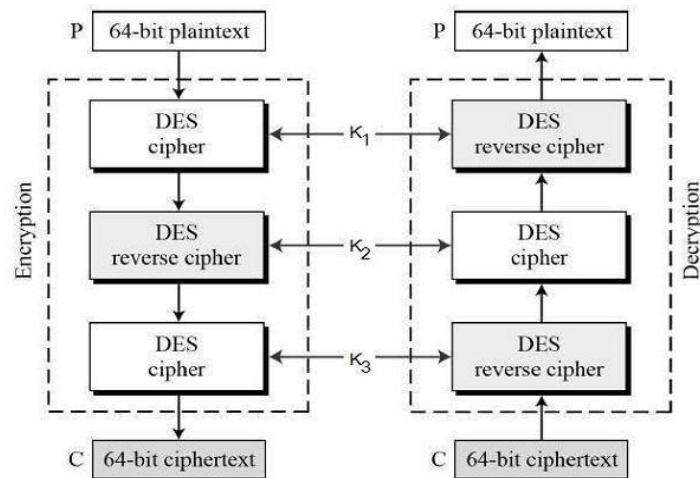


Figure 7. 3DES steps

Advanced Encryption Standard Algorithm

The most well-known and often preferred symmetric encryption (SE) method is the Advanced Encryption Standard (AES). It is regarded as being considerably faster than triple DES. The excessively small key size of DES necessitated a trade. With growing registering power, it was perceived as being defenseless versus all-out key inquiry attacks. Triple DES was designed to overcome this drawback, but it was thought to be slow. The element of AES is a Symmetric-key square code algorithm that utilizes 128-digit information with 128/192/256-bit keys. It provides complete determination and setup details and is faster and more stable than Triple-DES (Kaur & Kumar, 2020).

AES is an iterative rather than stream cipher. It is carried out by using the concept of replacement permutation technique which determines it. It includes a series of linked processes, some of which replace inputs with clear results (replacements), while others involve moving parts about (changes). It's odd that AES does all of its calculation on bytes rather than bits. From this point forward, AES interprets a plaintext block's 128 pieces as 16 bytes. For handling as a lattice, these 16 bytes are divided into four pieces and four lines. In contrast to DES, the number of rounds in AES varies and depends on the size of the key. AES uses 10 rounds for keys with 128 digits, 12 rounds for keys with 192 pieces, and 14 rounds for keys with 256 cycles. These rounds each use a different 128-cycle round key that is derived from the initial AES key (Xiang et al., 2006).

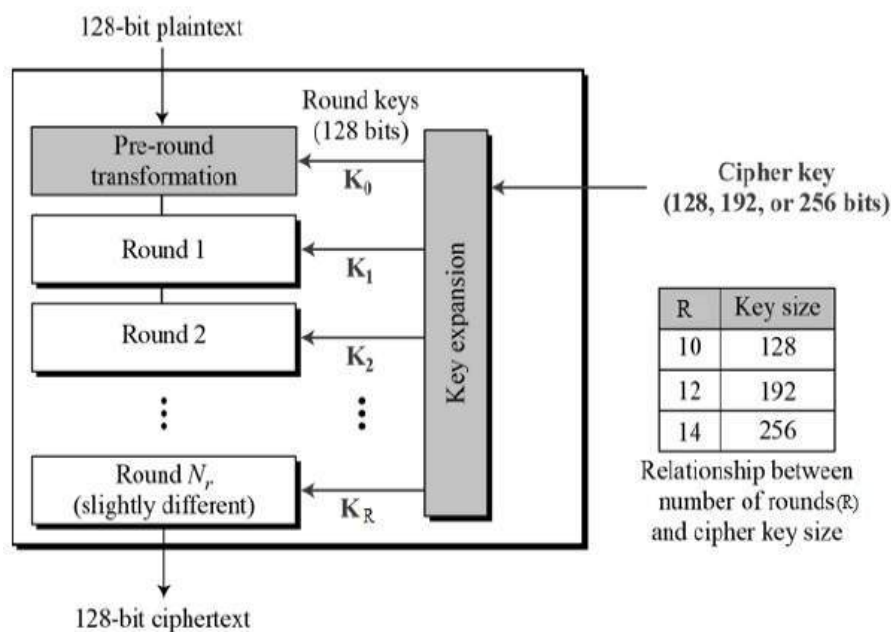


Figure 8. Demonstrates structure of AES algorithm

The main information to be scrambled is separated into a progression of the block. each block (16 input bytes) is supplanted by alluding to a proper table (S-box) given in the plan, and every one of the four columns of the matrix is moved. On the left, every four-byte segment is presently changed over utilizing an exceptional numerical capacity. This capacity takes four bytes of a segment as info and results from four new bytes that supplant the first segment, and 16 bytes of the network are presently viewed as 128 pieces and XORed to 128 pieces of the round key(Nadeem, & Javed, 2005,).

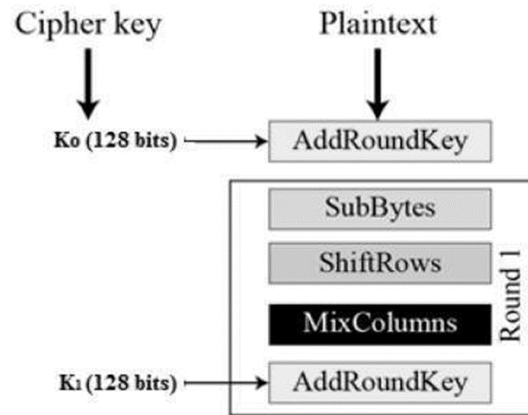


Figure 9. Demonstrates steps of the AES encryption process

RSA Encryption Algorithm

The RSA encryption is a largely utilized asymmetric encryption (SE) method in a range of products and services. Hence to carry out encryption and decryption in a specific data, the SE makes use of a couple of keys which are mathematically consolidated. The set of key pairs are formed by using a private and a public key, in which the general public key is to be had to anyone, and the personal secret is a secret known only to the creator of the important thing pair. With RSA, facts may be encrypted with either the private or public key, at the same time as the alternative key decrypts it. This is one of the motives why RSA is the maximum widely used asymmetric encryption approach (Dhakar, Ravi Shankar, Amit Kumar Gupta, 2012).

The functionality to scramble with either the non-public or public key continues a massive range of services to RSA users. When the public one used for encryption, the data have to be decrypted with a personal or private key. This is ideal for transferring sensitive information over a connection or the Internet, wherein the information receiver affords its public key to the sender. After the use of the receiver's public key to encrypt the sensitive facts, the sender of the data transmits it to the recipient. Because the public key has encrypted the touchy facts, most effective the proprietor of the non-public key can decrypt it. Only the intended recipient of the records may decrypt it, even though the records is intercepted within the transmission (Liu & Yang, 2018). Using a personal key to encrypt a message is another approach to making use of RSA for asymmetric encryption. In this illustration, the sender of the records uses its private key to encrypt the facts before sending both the encrypted facts and its public key to the recipient of the information. Using the sender's public key to decode the data, the receiver can then affirm that the sender is who they claim to be. Although this approach enables statistics to be stolen and tested in transit, its true aim is to establish the sender's identification. The recipient will be aware that the records was altered if the information had been stolen and modified within the direction because the general public key cannot decrypt this message. The recipient may be aware that the information became altered at the same

time as in transit if the statistics are stolen and updated in transit when you consider that the general public secret is not able to decipher these messages (Aufa et al., 2018). The RSA algorithm makes sure the keys are as safe as possible. The following steps will show you how it works:

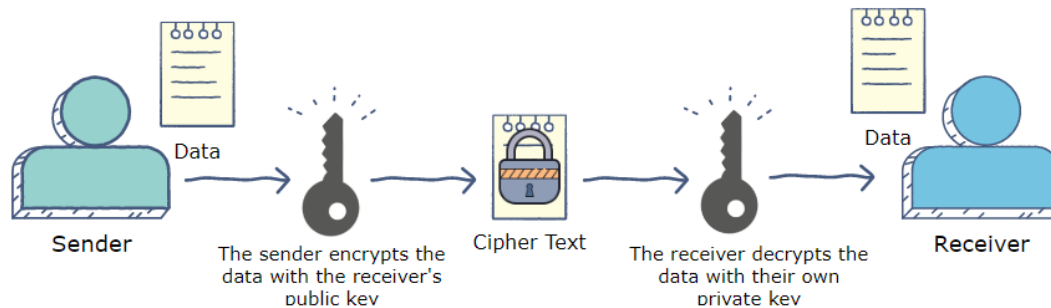


Figure 10. RSA

The RSA algorithm makes sure the keys are as safe as possible. The following steps will show you how it works:

Generating the keys

- Choose any two big prime numbers, x and y . The prime numbers need to be big so that they shall be hard for anyone to guess it.
- Compute $n=x \times y$
- Compute the totient function same as $\phi(n)=(x-1)(y-1)$.
- Choose an integer e , in such way that e is co-prime to $\phi(n)$ and $1 < e < \phi(n)$. The pair of numbers (n, e) sum up the public key.
- Compute d such that $e \cdot d = 1 \text{ mode } \phi(n)$. In this case d can be calculated using the extended Euclidean algorithm. The pair (n, d) sum up the private key.

2. Encryption

- Let plaintext, represented as a number, the ciphertext is calculated as: .

3. Decryption

- While using the private key, the plaintext can be computed using: .

Elliptic Curve Cryptography (ECC)

Another efficient method for data encoding and encoding is elliptic curve cryptography (ECC) which is encryption generation based on keys. The ECC specializes in pairs of public and private keys for decrypting and encrypting website visitors. A better generation of advanced cryptography than RSA is ECC algorithm. To generate safety among key pairs for public key encryption, it uses elliptic curve arithmetic (Zhang & Wang, 2018).

ECC has lately gained popularity because of its smaller key size and capability to keep security, while RSA calls for excessive top numbers as opposed to ECC to reach similar final results. The desire for devices to stay relaxed grows as keys get longer, placing pressure on the limited cell resources, therefore it is very likely that this trend will continue. For this reason, understanding elliptic curve cryptography is essential (Dawahdeh et al., 2018; Bhanot & Hans, 2015).

ECC's public key encryption techniques, in contrast to RSA's, are based on the algebraic

structure of elliptic curves over finite fields. As a result, ECC generates keys that are more difficult to decode mathematically. ECC is therefore regarded as the next generation of public key cryptography and is much more secure than RSA. Applying ECC also makes sense to maintain high levels of safety and overall performance. This is owing to the fact that ECC is being employed more frequently by websites as a means of advancing online data protection while also increasing mobile optimization. The call for a concise guide to ECC grows as greater internet websites use ECC to encrypt information (Bhanot&Hans, 2015). The latest ECC utilizes EC which is a plane curve over a finite field composed of points that satisfy the equation: $y^2 = x^3 + ax + b$.

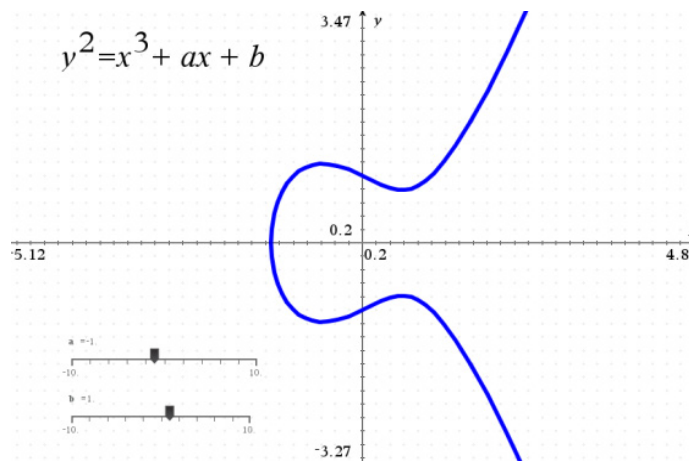


Figure 11. ECC

In this elliptic curve cryptography example, any point on the curve may be reflected over the x-axis and the curve will not alter. Any non-vertical line that crosses the curve fewer than 3 instances can be appeared as such. Elliptic curve encryption is far smaller than different kinds of encryption, which offers smaller, cellular devices greater energy. For two keys of the equal size, RSA's factoring encryption is extra susceptible considering factoring is less difficult and requires less effort than calculating for an elliptic curve discrete logarithm. With ECC, you could use smaller keys to acquire the equal stage of protection. When compared to RSA, ECC offers advanced security with quicker, shorter keys considering cell devices will need to do increasingly more cryptography with reducing computational power inside the destiny (Zhang & Wang, 2018). One of the most famous strategies for imposing digital signatures in cryptocurrencies is ECC. Both Bitcoin and Ethereum use the Elliptic Curve Digital Signature Algorithm to signal transactions (ECDSA). ECC, however, is used outdoors of cryptocurrency as properly. The majority of online apps will finally put into effect this encryption fashionable because of its shorter key period and effectiveness (Wang et al., 2020).

Performance Metrics

Differential Analysis

Many performance matrices are used to study differential attack, but the most common

are: the Number of Pixel Change Rate (NPCR) and Unified Average Changing Intensity (UACI) parameters. The differential attack is used to test the encryption algorithm's sensitivity to even smallest changes in the plain picture. Attackers frequently make slight improvements to the plain image. Then, using the same mystery key, encrypt both the plain and modified images. After that, it tries to find a link between encrypted plain and modified image (Kaur & Kumar, 2020).

The Number of Pixel Change Rate is characterized as an action used to compute the proportion of various pixel numbers between two encoded pictures whose ordinary images vary by a solitary pixel. A set of policies is extra resistant to differential assaults if it has an excessive NPCR score (Kaur & Kumar, 2020). The following formula can be used to calculate NPCR (Kaur & Kumar, 2020).

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W * H} * 100 \quad (1)$$

$$D(i,j) = 0 \text{ if } E(i,j) = E'(i,j) \text{ 1if } E(i,j) \neq E'(i,j) \quad (2)$$

W and H stand for the image's width and height, respectively. The variation in comparable pixels between the simple image and the scrambled image shown as $E'(i,j)$ and the scrambled image of the modified image $E(i,j)$ is shown as $D(i,j)$. The range of NPCR $\in [0, 100]$. Also the NPCR value of a scrambled image should be close to 100 (Kaur & Kumar, 2020).

The UACI (Unified Average Changing Intensity) is a matrix for calculating the average intensity of differences between the plain and encrypted image (Dawahdeh et al., 2018). It can be defined in the following way (Kaur & Kumar, 2020).

$$UACI = \frac{(\sum_{i,j} E(i,j) - E'(i,j))}{(255 * W * H)} * 100 \quad (3)$$

Here $E(i,j)$ and $E'(I,j)$ are the encrypted picture of plain and changed images, respectively. The values of NPCR and UACI supposed to be maximized.

Statistical Analysis

Statistical analysis of a scrambled image can also be used to crack encryption systems. The HA (Histogram analysis) as well as CC (correlation coefficient) are image evaluation metrics used to analyze histograms and the correlation between neighboring pixels of an encoded, or original one to confirm the resistance of an coding system to statistical attacks (Kaur & Kumar, 2020).

Histogram Analysis (HA) displays the pixel value distribution of the image. An original image's histogram ought to look entirely different from a scrambled image. Normal photos' histograms are by nature not uniform. The histograms of photos that have been

scrambled, however, should be uniform (Kaur & Kumar, 2020). This indicates that the spatial distribution of all pixels is uniform.

Correlation Coefficient (CC) is used to compare identical pixels between an image that is encrypted and one that is not. In the original image, the horizontal, diagonal, and vertical values of adjacent pixels are closely connected. The most effective picture encryption method reduces this relationship in the ciphered picture (Somaraj, 2015). Correlation coefficient can be computed as follows (Bhanot & Hans, 2015):

$$r_{x,y} = \frac{C(x,y)}{\sqrt{D(x)} * \sqrt{D(y)}} \quad (4)$$

$$C(x,y) = \frac{(\sum_{(i=1)}^K (x_i - E(x)) * (y_i - E(y)))}{K} \quad (5)$$

$$D(x) = \frac{1}{K} \sum_{(i=1)}^K (x_i - E(x))^2 \quad (6)$$

$$D(y) = \frac{1}{K} \sum_{(i=1)}^K (y_i - E(y))^2 \quad (7)$$

Here, $C(x,y)$ represents the co-variance between the x and y patterns. Furthermore, x and y are the 2 coordinates of an image. K is the number of pixel couples (x_i, y_i) . $D(x)$ and $D(y)$ are the deviation of x and y , simultaneously. $E(x)$ is the mean of x_i -pixel values. The range of CC should be a value between $[-1, 1]$. The CC value of an encoded image must be close to zero.

Information Entropy (IE)

It determines the typical amount of data included in each picture bit. It offers all the details that are contained in an image. Every pixel has a different value. So each pixel in an encrypted image has a uniform probability distribution, according to the entropy of the picture (Bhanot & Hans, 2015). It can be calculated as follows (Belazi, Abd El-Latif, & Belghith, 2016):

$$H(s) = -\sum_s (P(s_i) * \log_2 P(s_i)) \quad (8)$$

Here $H(S)$ represents the entropy of message source (S). $P(s_i)$ demonstrates the likelihood of occurrence of s_i . The value of IE $[0; 8]$. It must be close to 8 for 8-bit picture. Bit Correct Ratio (BCR) is used to determine how an encrypted image differs from its original. It checks to make sure the decrypted picture is accurate. (Belazi et al., 2016). It may be solved using the formula (Belazi et al., 2016):

$$BCR = (1 - \frac{(\sum_{(x,y)}^{(M*N)} O(x,y) \oplus R(x,y))}{M * N}) \quad (9)$$

Here, x and y represent the M x N pixel pictures' pixel coordinates. O is a plain image and R is the decrypted image. represents the XOR operation. The range of BCR [0, 1].

Mean Squared Error (MSE)

The MSE is a technique for comparing an original image's "true" pixel values to a decoded image. The discrepancy between an image's original values and its decrypted values is the mistake.(Kaur & Kumar, 2020). Below is a definition of MSE:

$$MSE = \frac{1}{MN} \sum_{(x=1)}^M \sum_{(y=1)}^N [O(x,y) - R(x,y)]^2 \quad (10)$$

Here, x and y represent the MxN-pixel pictures' pixel coordinates. The encoded and plain pictures are O and R, respectively. The value of MSE [0, ∞]. The value of MSE between plain and decoded must be minimum.

Peak Signal to Noise Ratio (PSNR)

PSNR is used to measure the quality between the plain and decoded images (Kaur & Kumar, 2020). PSNR can be calculated mathematically as follows:

$$PSNR = 10 \log_{10} \frac{(2^n - 1)^2}{MSE} \quad (11)$$

Here n is the number of bits per pixel. PSNR is measured in decibel (dB). The value of PSNR [0, 1]. The value of PSNR must be maximum between plain and decoded images.

Structural Similarity Index (SSIM)

The SSIM shows how comparable the plain and decrypted images are. It is a parameter for evaluating the quality of decrypted images. It is calculated between many windows of images of the same size (Kaur & Kumar, 2020). Below you will find a definition:

$$SSIM = \frac{(2\mu_i\mu_d + C_1)*(2\sigma_{id} + C_1)}{(\mu_i^2 + \mu_d^2 + C_1)*(\sigma_i^2 + \sigma_d^2 + C_2)} \quad (12)$$

Here μ_i and μ_d are the average of an input (I) and decoded (D) image, respectively. σ_i^2 and σ_d^2 denote the variance of I and D, respectively. σ_{id} is the covariance of I and D. C_1 and C_2 are the regularization parameters with values $(0.01P)^2$ and $(0.03P)^2$, respectively, where P is the specified value for the dynamic range. The range of SSIM $\in [-1, 1]$.

Root Mean Squared Error (RMSE)

The RMSE evaluates the root of the MSE and delivers more exact and accurate statistics. (Cao, Wei, Guo, & Wang, 2017). It can be calculated analytically as:

$$RMSE = \sqrt{\frac{\sum_{x=1}^M \sum_{y=1}^N [O(x,y) - D(X,Y)]^2}{M * N}} \quad (13)$$

Where the coordinates for each pixel in an image with a size of $M \times N$ are x and y . O and D stands for the original and decrypted images, respectively. The range of RMSE $\in [0, \infty]$.

Mean Absolute Error (MAE)

The MAE calculates the variation between plain and encrypted pictures (Kaur & Kumar, 2020). It can be calculated as:

$$MAE = \frac{1}{MN} / \sum_{x=1}^M \sum_{y=1}^N |O(x, y) - E(x, y)| \quad (14)$$

Here $O(x, y)$ and $E(x, y)$ mean plain and scrambled images, respectively. x and y demonstrate the pixel coordinates of picture with size of $M \times N$. The range of MAE Execution Time (ET) $[0, 2^n - 1]$, where n represents the number of bits per pixel. The MAE between the original and encrypted photos should be at maximum.

Execution Time (ET)

The execution time (ET) of a specific picture encryption algorithm is calculated. It is the sum of the compile and run times. ET should be kept to a minimum to make image encryption practical. Seconds, milliseconds, and minutes are the most common units of measurement (Kaur & Kumar, 2020).

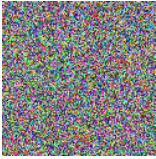
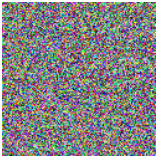
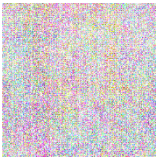
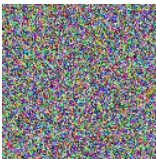
Dataset

The BSD dataset is abbreviated as the Berkeley Segmentation Dataset, which is a dataset designed to conduct different scientific research in the fields of image and computer vision (Arbeláez, Maire, Fowlkes, & Malik, 2011). This database is frequently used for image noise removal, segmentation, enhancement, and many other image processing operations. In this article, some sample color images are taken from BSD to implement the encryption algorithms used in the study. The goal is to test how AES, DES, 3DES, RSA and ECC algorithms can encrypt and decrypt images to protect sensitive digital pictures from attackers and unauthorized users.

Experimental Results

The performance of the different encryption algorithm are examined in this study was using some color images taken from the BSDS500 database. The applications within the scope of the study were developed using MATLAB which effective software environment tool that enables image analysts to perform some image-related activities such as analysis, demonstration, and enhancement, and a comprehensive set of image processing applications and standard algorithms for image processing. The visual image result of the study were given in below:

Table 1. Visual result

Algorithm	Input image	Encrypted image	Decrypted image
AES			
DES			
TDES			
RSA			
ECC			

In the figure above, the encryption and decryption results of the five algorithms in the study. As can be seen, the results of these algorithms are not visually separated but can be distinguished using image evaluation and performance matrices.

In the study, NPCR and UACI analysis was performed, and Table 1 shows all the average values of the different algorithms in the study for the images in the experiment. According to the results of the experiments in Table 1, the NPCR and UACI values for all eight test images are more than 99 and 33%, respectively. These average values are very high, which is due to the diffusion stage (DS) included in these algorithms. The DS causes a large change in the encrypted image when a particular pixel in the plain image is altered, i.e., the DI make the process very susceptible to beginning pixel setting.

Table 2. NPCR and UACI values for one-bit change in key value

	Lena (1)		28083		78019		113044	
Algorithms	NPCR	UACI	NPCR	UACI	NPCR	UACI	NPCR	UACI
AES	99.6414	33.4250	99.7256	33.8467	99.6938	33.2103	99.7846	33.2481
DES	94.0019	32.7270	99.0042	33.0121	98.6037	33.0541	98.8054	33.4627
3DES	98.0932	33.0110	99.8702	33.7601	99.0454	33.1471	99.4048	32.8031

RSA	99.0782	33.0456	99.0166	34.4017	99.9238	33.9975	99.89228	33.7459
ECC	99.0836	33.9701	98.0723	33.6403	99.0521	33.4343	99.0461	33.2043
	135069		157055		179084		124084	
Algorithms	NPCR	UACI	NPCR	UACI	NPCR	UACI	NPCR	UACI
AES	99.8743	33.2947	99.8941	33.3145	99.7985	33.0071	99.5419	33.9807
DES	97.2654	32.9514	98.7519	33.2974	98.1564	33.0175	96.2126	32.7942
3DES	99.8785	33.7534	99.3497	33.7614	99.7161	33.4201	98.1317	33.5475
RSA	99.8502	33.9997	99.9734	34.0014	99.1469	33.9976	99.4149	33.9992
ECC	98.9985	33.2891	97.3157	33.1764	96.4782	32.1403	99.4712	33.1037

An examination on the correlation analysis (CC) and information entropy (IE) of the mixed and unadulterated pictures. Every one of the pixel sets contains a haphazardly chosen pixel and a neighboring pixel. It tends to be seen that the RSA gave extremely low correlation coefficient values for every one of the eight test pictures, mirroring the high opposition of the technique to statistical attacks. There is a correlation in the flat image, and the pixel values are only occasionally irregular, so the entropy value is largely more modest than the best value of 8. The entropy can be the extreme ideal value of 8 when all pixel values are indiscriminately entangled. Table 2 displays the entropy values of the encoded images. From the results obtained, it can be seen that the entropy of the encrypted images is extremely close to the best value of 8. The data leakage in the cryptographic algorithms is insignificant and is safe from entropy-based attacks.

This demonstrates their decreased resistance to the statistical attacks. However, these qualities are still relatively lesser than the first CC, henceforth guaranteeing protection from statistical attacks dependent upon some degree. An overall pattern of lower connection can likewise be viewed as the picture size increments which support the histogram perception of expansion in thus can't be viewed as effective on visual evaluation grounds. At long last, every one of the plans give the unscrambled pictures like the first pictures which guarantee the unwavering quality of decoded picture on the off chance that security is guaranteed. The CC value is between - 1 and +1, where the limits shows an ideal negative or positive straight correlation respectively. The zero value of CC indicates that there is no linear relationship between consecutive pixel values.

Table 3. CC and IE values for one-bit change in key value

	Lena (1)		28083		78019		113044	
Algorithms	CC	IE	CC	IE	CC	IE	CC	IE
AES	0.0692	7.8015	0.07193	7.6705	0.0532	7.6126	0.057936	7.9294
DES	0.08345	7.9086	0.06789	7.8785	0.05641	7.6818	0.07414	7.7891
3DES	0.07693	7.8578	0.08657	7.0621	0.06934	7.6718	0.07571	7.4106
RSA	-0.00685	7.6442	0.02311	7.8273	0.24604	7.6079	-0.02828	7.9134

ECC	0.06979	7.7949		0.08291	7.8201		0.02359	7.6418		0.056202	7.4772
	135069			157055			179084			124084	
Algorithms	CC	IE		CC	IE		CC	IE		CC	IE
AES	0.061627	7.5876		0.08146	7.9604		0.07508	7.6544		0.06709	7.8578
DES	0.095478	7.9898		0.09969	7.5438		0.09351	7.3492		0.08601	7.4141
3DES	0.07810	7.7882		0.09678	7.7141		0.08746	7.7565		0.079605	7.6795
RSA	-0.04217	7.4939		0.05997	7.7459		0.02464	7.8352		0.023765	7.8581
ECC	0.092505	7.6379		0.08934	7.5457		0.07846	7.5102		0.087168	7.7545

In the analysis, BCR measurement was also tested to determine the difference between the plain image and the decoded image. The metric usually checks the correctness of the encoded image. The value of this metric should be a number in the range of zero to one. The MSE was also used to compare the original image's true pixel values to the decrypted image. The error is the difference between the values of an original picture and the values of the decrypted image. The MSE of the encrypted image should be maximized to ensure that attackers cannot find the correct pixels of the original image. The result of both BCR and MSE is shown in the table below.

Table 4. BCR and MSE values for one-bit change in key value

	Lena (1)		28083		78019		113044	
Algo-rithms	BCR	MSE	BCR	MSE	BCR	MSE	BCR	MSE
AES	0.05484	0.60024	0.07468	0.71062	0.01351	0.54721	0.062402	0.31233
DES	0.068878	0.49174	0.08678	0.33645	0.06878	0.38704	0.069878	0.09331
3DES	0.05946	1.7196	0.06964	0.42857	0.43874	0.51065	0.079464	0.27469
RSA	0.041107	0.3617	0.04585	0.62874	0.02107	0.76454	0.061107	0.84787
ECC	0.052402	2.09834	0.06738	0.62242	0.05914	0.55626	0.058465	0.70116
	135069		157055		179084		124084	
Algo-rithms	BCR	MSE	BCR	MSE	BCR	MSE	BCR	MSE
AES	0.055439	0.40979	0.06402	0.63092	0.08242	0.65434	0.072402	0.47971
DES	0.068878	0.64464	0.0887	0.54234	0.07978	0.6986	0.08878	0.7219
3DES	0.089464	0.63371	0.07946	0.37046	0.08064	0.82154	0.079464	0.4959
RSA	0.043107	0.09751	0.04117	0.95421	0.03107	0.08741	0.051107	0.7883
ECC	0.050914	0.60256	0.05914	0.46545	0.04814	0.84029	0.060914	0.4857

The PSNR metric of the encoded image was tested in the analysis. The PSNR value range should start at zero and go to infinity. Normally PSNR should be maximized as much as possible. The Structural Similarity Index (SSIM) has also been tested, and the encrypted SSIM value should be minimized so that attackers cannot fully locate the original image. The PSNR and SSIM results are shown in the table below.

Table 5. Peak Signal to Noise Ratio (PSNR) and Structural Similarity Index (SSIM)

	Lena (1)		28083		78019		113044	
Algorithms	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM
AES	39.5111	0.00841	38.5956	0.02680	36.9558	0.00602	35.5718	0.00475
DES	39.0102	0.00852	40.4546	0.00529	38.3998	0.00598	37.4035	0.00483
3DES	40.4991	0.00653	41.1322	0.00498	37.6827	0.00560	37.5261	0.00491
RSA	41.0848	0.00504	18.5969	0.01003	9.02328	0.00116	13.2627	0.01008
ECC	36.5244	0.00527	37.3107	0.00937	39.5754	0.00676	37.7165	0.00633
	135069		157055		179084		124084	
Algorithms	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM
AES	36.3375	0.00627	36.0703	0.00674	33.6552	0.00706	37.041	0.00836
DES	40.8517	0.00454	37.333	0.00730	39.7253	0.00752	41.1306	0.00906
3DES	40.7503	0.00414	37.4737	0.00698	38.9231	0.00629	41.0213	0.00832
RSA	9.7663	0.00324	10.0839	0.00177	7.71929	0.00535	6.61093	0.00804
ECC	39.3381	0.00435	38.1078	0.00439	36.8471	0.00632	39.2697	0.00842

The RMSE metric of the encoded image was tested in the analysis. The RMSE range of values should start at zero and go to infinity. Normally PSNR should be minimized as much as possible. The RMSE results are shown in the table below.

Table 6. Root Mean Squared Error (RMSE)

	Lena (1)	28083	78019	113044
Algorithms	RMSE	RMSE	RMSE	RMSE
AES	0.90103	0.89722	0.9246	0.88303
DES	0.89493	0.87993	0.8719	0.87493
3DES	0.91068	0.91068	0.9168	0.92166
RSA	0.95906	0.97176	0.8916	0.85906
ECC	0.88703	0.89418	0.8835	0.88292
	135069	157055	179084	124084
Algorithms	RMSE	RMSE	RMSE	RMSE
AES	0.91183	0.88702	0.8873	0.8832
DES	0.87493	0.87493	0.8749	0.8794
3DES	0.91268	0.93168	0.9168	0.9166
RSA	0.89906	0.89596	0.8996	0.8956
ECC	0.88535	0.88135	0.8535	0.8813

In the analysis, the Mean Absolute Error (MAE) and Execution Time (ET) matrices of the encoded image were tested. The MAE value range should start at zero and go to infinity. Normally MAE should be maximized as much as possible to prevent attacks from decrypting the encrypted image. On the other hand, ET was tested to measure the time required to execute a given image encryption algorithm. The ET should be kept to minimum to show the performance of the encryption algorithm. The ET and MAE results are shown in the table below.

Table 7. Mean Absolute Error (MAE)and Execution Time (ET)

	Lena (1)		28083		78019		113044	
Algorithms	MAE	ET	MAE	ET(sec)	MAE	ET	MAE	ET
AES	86.4335	1.29688	82.1031	1.73438	80.3625	1.2338	87.03155	1.4844
DES	84.773	2.3594	77.0587	2.60938	79.1609	2.9838	83.05234	2.48438
3DES	85.0148	5.4375	81.0904	4.85938	81.1789	3.4065	84.73543	5.4375
RSA	87.0656	5.23438	86.2739	5.95313	86.456	4.935	87.3679	5.6875
ECC	88.0638	1.95313	84.2384	2.04587	85.1615	1.52	87.03624	2.04688
	135069		157055		179084		124084	
Algorithms	MAE	ET	MAE	ET	MAE	ET	MAE	ET
AES	87.07656	1.65625	88.1904	1.4375	85.0267	1.625	89.47442	1.77656
DES	85.14562	1.9375	84.4277	2.10938	83.4852	2.4025	85.8698	2.71875
3DES	86.34568	3.28125	85.7598	4.29688	86.0183	4.4375	87.07948	5.92188
RSA	88.4913	5.625	89.4882	5.48438	86.8384	5.4013	91.8328	5.78125
ECC	87.76373	2.125	82.0598	1.9375	83.6637	1.7663	86.17841	1.82813

Conclusion

Digital images are assuming an inexorably significant part in our lives, because of the huge advances in imaging gadgets and the innovations of these technologies. This makes image security one of the most interesting research fields in image processing and computer vision. Attackers always take advantage of weak or unprotected data transmitted and stored over the internet. They try to sit in the middle of the network to control the data transfer over the network. Therefore, they focus on critical data shared between the ten senders and receivers. In this study, we conducted a comparative study of five encryption algorithms using color images obtained in the BSD300 database. The main purpose is to compare the performances of these algorithms using different methods of image quality evaluation. The algorithms in the scope of the study include AES, DES, TDES, RSA and ECC. The first three algorithms are considered symmetric methods, while other algorithms are considered asymmetric encryption methods. In the experiment, some color images from BSD were used to test the performance of the algorithms. The efficiency of encoding was measured using some image evaluation methods and the results were presented in the study.

In the future, more encryption algorithms such as Blowfish, RC4, RC5, RC6, and Chaotic Map can be added to the work. In addition, performance evaluation criteria can be expanded by adding a feature similarity measurement index (FSIM), key spacing, pixel-based analysis, and many other image evaluation criteria.

References

Arbeláez, P., Maire, M., Fowlkes, C., & Malik, J. (2011). Contour detection and

- hierarchical image segmentation. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 33(5), 898–916. <https://doi.org/10.1109/TPAMI.2010.161>.
- Aufa, F. J., Endroyono, & Affandi, A. (2018). Security System Analysis in Combination Method: RSA Encryption and Digital Signature Algorithm. *Proceedings - 2018 4th International Conference on Science and Technology, ICST 2018*. <https://doi.org/10.1109/ICSTC.2018.8528584>.
- Barker, E., & Mouha, N. (2017). Recommendation for the triple data encryption algorithm (TDEA) block cipher.
- Belazi, A., Abd El-Latif, A. A., & Belghith, S. (2016). A novel image encryption scheme based on substitution-permutation network and chaos. *Signal Processing*, 128, 155–170. <https://doi.org/10.1016/J.SIGPRO.2016.03.021>.
- Bhanot, R., & Hans, R. (2015). A Review and Comparative Analysis of Various Encryption Algorithms. *International Journal of Security and Its Applications*, 9(4), 289–306.
- Cao, X., Wei, X., Guo, R., & Wang, C. (2017). No embedding: A novel image cryptosystem for meaningful encryption. *Journal of Visual Communication and Image Representation*, 44, 236–249. <https://doi.org/10.1016/J.JVCIR.2016.08.003>.
- Cardarilli, G. C., Di Nunzio, L., Fazzolari, R., & Re, M. (2015). TDES cryptography algorithm acceleration using a reconfigurable functional unit. *2014 21st IEEE International Conference on Electronics, Circuits and Systems, ICECS 2014*, 419–422. <https://doi.org/10.1109/ICECS.2014.7050011>.
- Data Encryption Standard. (2022). Retrieved July 22, 2022, from https://www.tutorialspoint.com/cryptography/data_encryption_standard.htm.
- Davis, R. M. (1978). The Data Encryption Standard in Perspective. *IEEE Communications Society Magazine*, 16(6), 5–9. <https://doi.org/10.1109/MCOM.1978.1089771>.
- Dawahdeh, Z. E., Yaakob, S. N., & Razif bin Othman, R. (2018). A new image encryption technique combining Elliptic Curve Cryptosystem with Hill Cipher. *Journal of King Saud University - Computer and Information Sciences*, 30(3), 349–355. <https://doi.org/10.1016/J.JKSUCI.2017.06.004>.
- Dhakar, Ravi Shankar, Amit Kumar Gupta and P. S. (2012). Modified RSA encryption algorithm (MREA). *Second International Conference on Advanced Computing & Communication Technologies*, 426–429.
- Furht, B., Socek, D., & Eskicioglu, A. M. (2004). Fundamentals of Multimedia Encryption Techniques. *Multimedia Security Handbook*, 95–132. <https://doi.org/10.1201/9781420038262-3>.
- Guan, Z. H., Huang, F., & Guan, W. (2005). Chaos-based image encryption algorithm. *Physics Letters A*, 346(1–3), 153–157. <https://doi.org/10.1016/J.PHYSLETA.2005.08.006>.
- Kansal, S., & Mittal, M. (2015). Performance evaluation of various symmetric encryption algorithms. *Proceedings of 2014 3rd International Conference on Parallel, Distributed and Grid Computing, PDGC 2014*, 105–109. <https://doi.org/10.1109/PDGC.2014.7030724>.
- Kanso, A., & Ghebleh, M. (2012). A novel image encryption algorithm based on a 3D chaotic map. *Communications in Nonlinear Science and Numerical Simulation*,

- 17(7), 2943–2959. <https://doi.org/10.1016/J.CNSNS.2011.11.030>.
- Kaur, M., & Kumar, V. (2020). A Comprehensive Review on Image Encryption Techniques. *Archives of Computational Methods in Engineering*, 27(1), 15–43. <https://doi.org/10.1007/S11831-018-9298-8>.
- Khan, M., & Shah, T. (2014). A Novel Statistical Analysis of Chaotic S-box in Image Encryption. *3DResearch 2014* 5:3, 5(3), 1–8. <https://doi.org/10.1007/S13319-014-0016-5>.
- Lai, X. J., Lu, M. X., Qin, L., Han, J. S., & Fang, X. W. (2010). Asymmetric encryption and signature method with DNA technology. *Science China Information Sciences* 2010 53:3, 53(3), 506–514. <https://doi.org/10.1007/S11432-010-0063-3>.
- Liu, Yang, et al. (2018). Secure and robust digital image watermarking scheme using logistic and RSA encryption. Elsevier, 95–105.
- Nadeem, A., & Javed, M. Y. (2005, August). A performance comparison of data encryption algorithms. In 2005 international Conference on information and communication technologies (pp. 84-89). IEEE. <https://doi.org/10.1109/ICICT.2005.1598556>.
- Sharif, S. O., Kuncheva, L. I., & Mansoor, S. P. (2010). Classifying encryption algorithms using pattern recognition techniques. *Proceedings 2010 IEEE International Conference on Information Theory and Information Security, ICITIS 2010*, 1168–1172. <https://doi.org/10.1109/ICITIS.2010.5689769>.
- Somaraj, S., and, M. H.-I. J. of S., & 2015, undefined. (2015). Performance and security analysis for image encryption using key image. *Researchgate.Net*. <https://doi.org/10.17485/ijst/2015/v8i35/73141>.
- Symmetric vs. Asymmetric Encryption. (2022). Retrieved July 22, 2022, from <https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences>.
- Wang, H., He, D., & Ji, Y. (2020). Designated-verifier proof of assets for bitcoin exchange using elliptic curve cryptography. *Future Generation Computer Systems*, 107, 854–862. <https://doi.org/10.1016/J.FUTURE.2017.06.028>.
- Xiang, T., Liao, X., Tang, G., Chen, Y., & Wong, K. W. (2006). A novel block cryptosystem based on iterating a chaotic map. *Physics Letters, Section A: General, Atomic and Solid State Physics*, 349(1–4), 109–115. <https://doi.org/10.1016/J.PHYSLETA.2005.02.083>.
- Ye, G. (2010). Image scrambling encryption algorithm of pixel bit based on chaos map. *Pattern Recognition Letters*, 31(5), 347–354. <https://doi.org/10.1016/J.PATREC.2009.11.008>.
- Zhang, X., & Wang, X. (2018). Digital Image Encryption Algorithm Based on Elliptic Curve Public Cryptosystem. *IEEE Access*, 6, 70025–70034. <https://doi.org/10.1109/ACCESS.2018.2879844>.
- Zhou, Y., Cao, W., & Philip Chen, C. L. (2014). Image encryption using binary bitplane. *Signal Processing*, 100, 197–207. <https://doi.org/10.1016/J.SIGPRO.2014.01.020>.
- Zhu, Z. L., Zhang, W., Wong, K. W., & Yu, H. (2011). A chaos-based symmetric image encryption scheme using a bit-level permutation. *Information Sciences*, 181(6), 1171–1186. <https://doi.org/10.1016/J.INS.2010.11.009>.

About the Authors

Mehmet HACIBEYOGLU, PhD, is an Associate Professor of Computer Engineering at Necmettin Erbakan University in Konya, Türkiye. He holds a PhD in Computer Engineering from Selcuk University. His main areas of interest are artificial intelligence, data mining and cyber security applications.

E-mail: hacibeyoglu@erbakan.edu.tr, **ORCID:** 0000-0003-1830-8516.

Bashir Sheikh Abdullahi JAMA, is a computer engineer and junior researcher in the field of computer science and engineering, He is interested in conducting research that improves human life and helps to adapt to the modern technological world. His research interests include artificial intelligence, machine learning, computer vision digital image processing. Currently, he is a PhD student in the Department of Computer Engineering at Necmettin Erbakan University.

E-mail: bashiir204@gmail.com, **ORCID:** 0000-0002-2417-9223

Similarity Index

The similarity index obtained from the plagiarism software for this book chapter is 20%.

To Cite This Chapter:

Hacibeyoglu, M., & Jama, B.S.A (2022). Performance Analysis of Symmetric and Asymmetric Encryption Algorithms in Digital Images, In S. Kocer, O. Dundar (Eds.), *Current Studies in Basic Sciences Engineering and Technology*, (pp. 92–113). ISRES Publishing.