# Security Analysis of Advanced Encryption Standard (AES) for Image Encryption

Rıdvan Küçükbacak[1*], Mahmut Bağcı[2]

**Affiliations**

[1] Master's Program in Management Information Systems, Graduate School of Social Science, Yeditepe University, Istanbul, 34755, Turkey

[2] Master's Program in Management Information Systems, Graduate School of Social Science, Yeditepe University, Istanbul, 34755, Turkey

*To whom correspondence should be addressed; E-mail: ridvan.kucukbacak@std.yeditepe.edu.tr

**Abstract**

In recent years, there have been major advancements in multimedia technologies and accordingly, file transfer over the internet has become extremely frequent. However, some security issues can occur in the internet, since it is a very insecure channel. To preserve the privacy and security of multimedia data transmitted over the internet, a number of encryption algorithms have been developed. This research presents a methodology for examining practically used image processing encryption algorithms. To measure the quality of encoded images, a number of factors such as correlation coefficient and information entropypixel change rate are employed instead of visual evaluation. In this study, the image encryption efficiency of the Advanced Encryption Standard (AES) is analyzed and the security level is evaluated. For digital pictures, AES security evaluations have been conducted against brute force, statistical, and other attacks. The results of the tests are provided to see if these algorithms are secure for digital photos. Examination of the image encryption algorithms reveal that images can be encrypted by the AES method robustly. Applied tests are independent from encryption algorithm and thus they are applicable to all image encryption algorithms.

**Keywords**: Image encryption; Security analysis; AES; Cryptography

## INTRODUCTION

Multimedia encryption technology originally appeared in the 1980s, and by the mid-1990s, it had become a hot topic of research. Raw data encryption, compressed data encryption, and partial encryption are the three stages of development (Li et al. 2004).

Only a few multimedia encoding methods were standardized prior to the 1990s. The majority of multimedia data (images, videos) was transferred or stored in its unprocessed state. Multimedia encryption was primarily dependent on pixel permutation or scrambling, in which the video/image was changed in such a way that the resulting data was incomprehensible (Li et al., 2001,p.321). Gap-filling curves, for example, are used to alter image/video data, complicating the link between adjacent images/video pixels. The Eurocrypt standard is used by European television networks to encrypt signals (Saha & Majumdar, 2021). These methods are used because they have low computational complexity and cost. However, such changes in the relationship between neighboring pixels, causing confining not to work. Therefore, these encryption algorithms are only advantageous for an application that does not require compression.

With the advancement of multimedia technology in the early 1990s, JPEG, MPEG, and other picture and audio/video encoding standards such multimedia data was compressed before being saved or transferred, and was not ideal for raw data encryption.

Multimedia applications required greater real-time processing after the advancement of internet technology in the late 1990s. The size of the final encrypted file is reduced and the encryption efficiency is boosted by encrypting only particular parts of the data. Due to the fast proliferation of computer networks, information security needs have become critical to safeguard privacy and confidentiality. Accordingly, encryption and decryption algorithms such as the Advanced Encryption Standard (AES) and Data Encryption Standard (DES) have been introduced, and they have been widely used to encrypt files containing large amounts of data.

In general, security systems are based on two main components that are data hiding and cryptography. A detailed classification of these components are shown in Figure 1. In this thesis, the robustness of information security systems are tested from the perspective of image encryption techniques, and the reliability of the AES method is demonstrated.

Figure 1. Classification of information security techniques

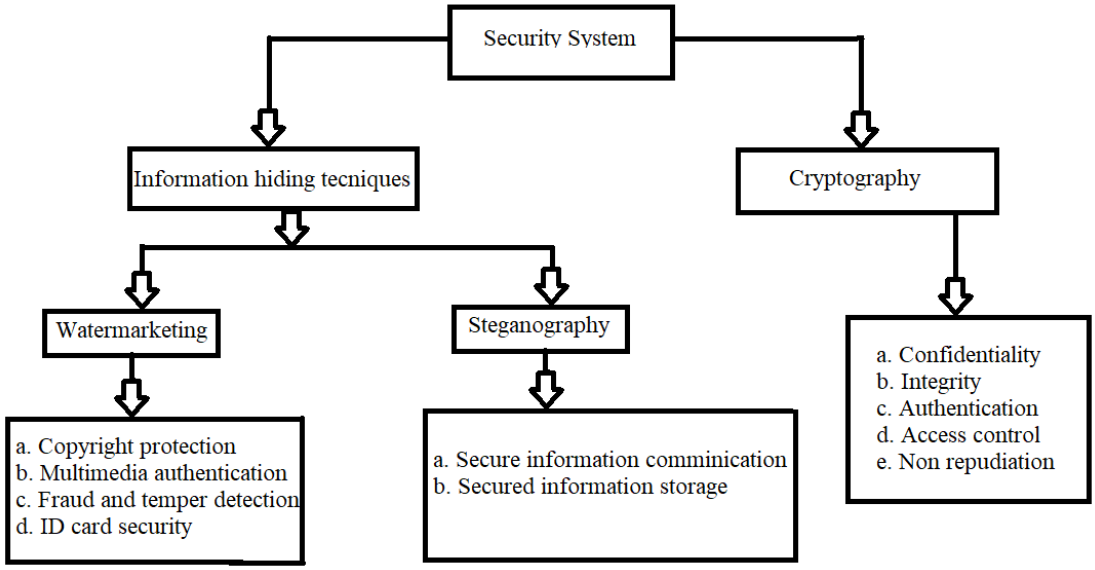



**Image Encryption Using AES**

The Advanced Encryption Standard (AES) has become the most widely used symmetric encryption standard. Despite the term "Standard" in its name pertains largely to US government processes, the AES block cipher is required in numerous industry standards and is used in many commercial systems (Fips, 2001). Commercial standards that utilise AES include the Internet security standard IPsec, TLS, the Wi-Fi encryption standard IEEE 802.11i, the secure shell network protocol SSH (Secure Shell), Internet telephony Skype, and a variety of security solutions throughout the world. The most well-known attack against AES is brute force.

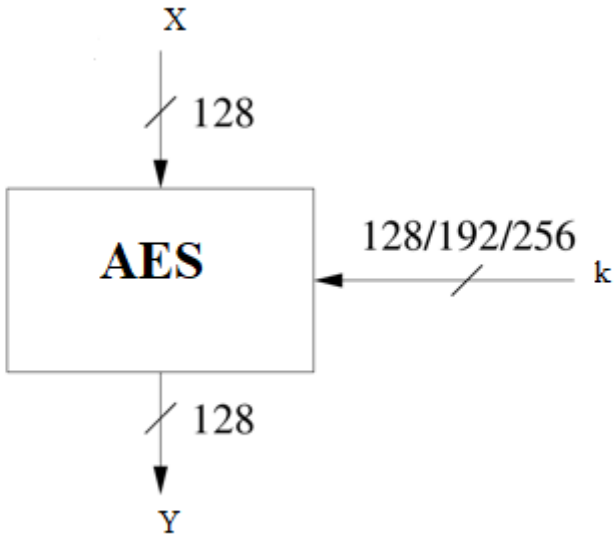
The National Institute of Standards and Technology (NIST) requested proposals for a new Advanced Encryption Standard in 1997 (AES). Unlike DES, the AES algorithm is chosen in an open procedure controlled by NIST. In the three rounds of AES evaluation that followed, NIST and the international scientific community argued the pros and cons of the proposed ciphers, which are pared down by the number of feasible alternatives. In 2001, NIST declared Rijndael to be the replacement for AES, and it is published as the final standard (FIPS PUB 197). Rijndael is established by two adolescent Belgian cryptographers.

It is expected that the AES algorithm will also play an active role in strategic applications. Because it can be implemented in hardware enables the encryption algorithm to take place

in strategic communication equipment as well. It is possible to develop applications that require high speed on hardware by using the AES algorithm. Encryption and decryption are secure with AES encryption used in many highly sensitive applications such as image encryption, ATM networks, Confidential Collaboration Documents, Personal Storage Devices, Smart Cards, Government Documents, Personal Information Protection and other applications. In the AES selection process, NIST's performance criteria are determined as high speed and low RAM requirement. Designed with these criteria in mind, AES works with high performance on many different hardware.

The Rijndael block cipher is roughly comparable to the AES encryption technique. A Rijndael block and key can have a size of 128, 192, or 256 bits. Only a 128-bit block size is required under the AES standard. As a consequence, with a block length of only 128 bits, the AES algorithm is known as Rijndael. Figure 2 depicts the input and output parameters. In this study, we'll look at a version of the traditional Rijndael with a block length of only 128 bits.

Figure 2. AES input and output parameters



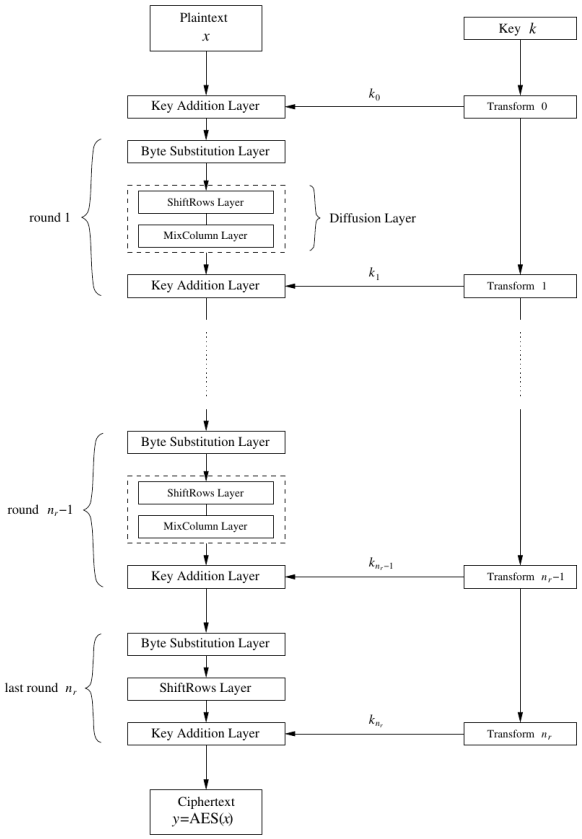

As previously stated, Rijndael is required by NIST to support all three key lengths. The cipher's internal cycles are a function of the key length as specified in Table 1.

Table 1. Cycle counts and key sizes for AES

| Key Lengths | # Rounds = $n_r$ |
|---|---|
| 128 bit | 10 |
| 192 bit | 12 |
| 256 bit | 14 |

Layers make up AES encryption. The bus's 128 bits are processed by each tier. The algorithm's state is also known as the bus. There are three different types of layers. Every round, except the first, has three layers: plaintext x, ciphertext y, and round number nr, as illustrated in Figure 3. Furthermore, the last round number does not employ the MixColumn transform, resulting in a symmetrical encryption and decryption technique.

Figure 3. Block diagram of AES algorithm



Note. (Bhat et al., 2015)

Brief description for layers:

In key timing, a 128-bit loop key or subkey obtained from the master key is XORed on a case-by-case basis in the Key Addition Layer.

Each element of the state in the loop is converted non-linearly using lookup tables with particular mathematical features in the Byte Substitution layer (S-Box). This causes data to get jumbled, resulting in changes in each state bit propagating fast throughout the bus. Nonlinearity is provided by this layer.

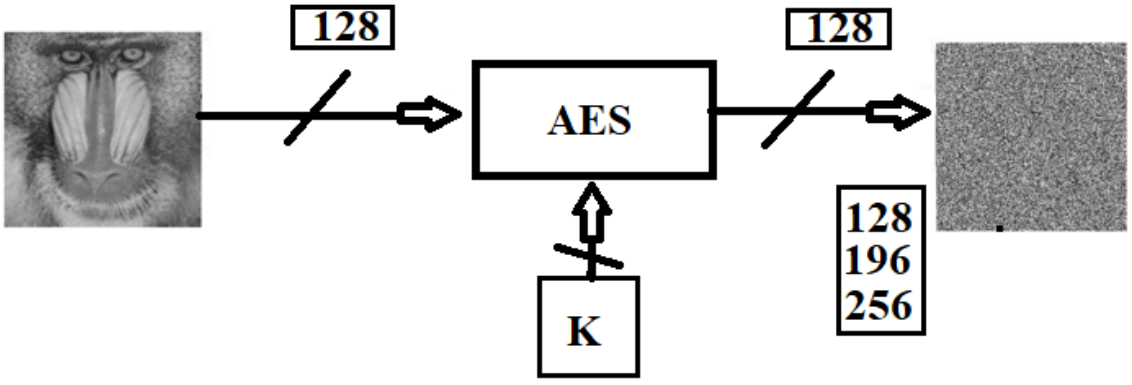
Diffusion layer allows diffusion to occur across all state bits. It is made up of two sublayers, each of which performs linear operations:

- ShiftRows Layer: Data is mixed at the byte level.
- MixColumn Layer: It's a matrix operation that combines (mixes) 4-byte chunks.

Key setup calculates subkeys from the original AES key.

In this study, gray level image pixels are extracted from the image file and directly encrypted with the AES algorithm using a 256-bit key as in Figure 4. The image is first within pixel values and then given to the AES algorithm as input. The output is divided into 256-bit pixels and then represented as pixel values of a bitmap image. Each block is encrypted using CBC mode. Security analyzes are made on the encrypted image obtained as a result of encryption.

Figure 4. AES algorithm Image input and output



## RESULTS

### Histogram Analysis

A histogram is a graphical depiction of the number of different color values in a numerical image. It is possible to obtain brightness or tone information about pictures by the histograms. In Figure 20, the histogram graphics of the images obtained by encoding 256x256 flat Mandrill (a) and AES (b) are compared, while encrypted image histogram have the following properties:

1. The histogram of the original image is completely different.
2. Uniform distribution, i.e., any gray level pixel value has the same probability of occurring.

*Figure 5. Histogram comparison (a) Histogram plot of plain mandrill image (b) Histogram of AES encoded image*

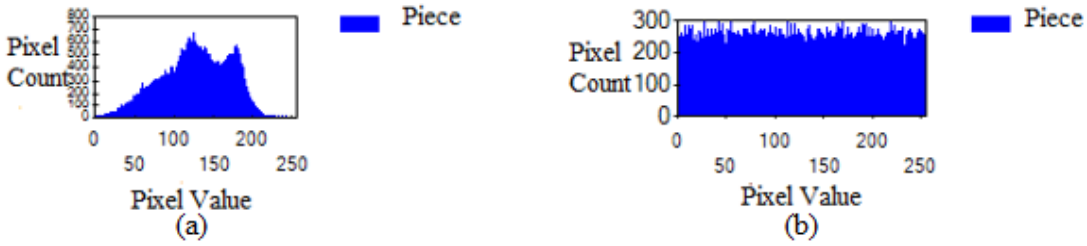



*Figure 5. Histogram comparison (a) Histogram plot of plain mandrill image (b) Histogram of AES encoded image*

As can be seen from the Figure 5 (b), the histogram graph of the encrypted picture created as a consequence of encryption using AES is close to linear character and regularity. This can be explained by the change of pixel values.

### Information Entropy

Entropy is a concept that is defined by Shannon in 1948 and comes from information theory (Shannon, 1949, p. 687). When analyzing an encryption system, the idea of entropy is extremely significant. The main feature of uncertainty is information entropy. Entropy measures the degree of uncertainty that exists in the system. The more predictable a sequence is, the more information it contains. So the way to hide information is to remove predictability. Information theory is now used extensively in cryptography, network

security, communication systems, data compression, error correlation, and other fields (Enayatifar , 2011, p. 221).

$$H(m) = \sum_{i=0}^{L-1} p(m_i) \log \frac{1}{p(m_i)} \quad (1)$$

In image coding, L stands for the total number of symbols and the total amount of pixels. The logarithm is taken in terms of base 2. The probability that a pixel is mi is denoted by p(m_i). If the entropy of the encoded picture comes close enough to the logarithm L, the histogram of the picture can be said to be smooth enough. For example, assuming that a message contains the symbol 2^8 (s={ s_1,s_2,…,s_(2^8 ) }) with the same probability, equation (1) generates a true random value such that H(s) = 8. This value is the ideal value. But in reality, the content of an encrypted message seldom contains genuine random symbols. As a result, the encrypted message's entropy is lower than its optimal value.

Table 4 shows the H(m) entropy values of the AES encrypted picture after calculating the likelihood of discovering all gray level values in the encrypted image. These values are extremely close to the optimal gray image value of 8. Therefore, it can be said that the encryption system is safe according to entropy attacks.

Table 2. Entropy values of mandrill image encrypted with AES

| | **Entropy** | |
|---|---|---|
| | **Plain Image** | **Encrypted Image** |
| **Entropy Value** | 7,1869 | 7,9993 |

**Correlation Coefficient**

Correlation is a term used in probability theory and statistics to describe the direction and strength of a linear relationship between two random variables. In a statistical context, correlation reflects how far off two variables are from being independent. The direction and amount of the link between the independent variables are indicated by the correlation coefficient. This coefficient can have a value of (-1) or (+1). Positive numbers represent a direct linear relationship, whereas negative values represent an inverse linear relationship. There is no linear relationship between the variables if the correlation coefficient is 0. As

a result of the various conditions, many correlation coefficients have been produced. The Pearson product-moment correlation coefficient is one of the most well-known of these (Newton, 1997).

It's calculated by multiplying the product of two variables standard deviations by their covariance. Pearson correlation coefficients are utilized to determine the degree of reliance between the two pictures in this investigation.

In a meaningful picture, the correlation between two neighboring horizontal, vertical, and diagonal pixels is generally strong. Because the pixel values of a meaningful picture are quite near to each other. The correlation between two nearby pixels is tested using correlation analysis. First, from the encrypted image, p pairs of neighboring horizontal, vertical, and diagonal pixels are randomly picked. Each pair's correlation coefficients are determined as in $r_{uv}$ (8).

$$E(u) = \frac{1}{p}\sum_{i=1}^{p} u_i \tag{2}$$

$$D(u) = \frac{1}{p}\sum_{i=1}^{p} (u_i - E(u))^2 \tag{3}$$

$$cov(u, v) = E\{(u - E(u))(v - E(v))\} \tag{4}$$

$$r_{uv} = \frac{cov(u, v)}{\sqrt{D(u)D(v)}} \tag{5}$$

$$r_{uv} = \frac{cov(u, v)}{\sqrt{D(u)D(v)}} \tag{6}$$

Here, $\sqrt{D(u)}$ is standard deviation and E(u) is mean. cov(u, v) is covariance of pixels, u and v are the values of two adjacent pixels in the image and p is the number of the selected

pixel pair. The same calculation is calculated in the vertical and diagonal directions. Correlation coefficients between neighboring pixels of the flat image are usually large and approach 1. In encrypted images, it is usually small and close to 0. A good cryptosystem should remove the associations of adjacent pixels in the plain picture as much as possible in the encrypted picture. The graphical representation of the correlation coefficient analysis with 1000 pairs of neighboring pixels is shown in Figure 6. By looking at Figure 7, we can easily understand that the linear pixel relationship in the plain picture is not existed in the encrypted picture. It is calculated according to the horizontal, vertical and diagonal neighborhoods of the image encrypted with the AES encryption standard. The correlation coefficients calculated in the picture below are compared and shown in Table 3.

Figure 6. Correlation graphs (a), (b), (c) relations of adjacent horizontal, vertical and diagonal pixels in flat mandrill picture, (d), (e), (f) horizontal, vertical and diagonal neighboring pixels, respectively, in AES relations in the mandrill image encrypted

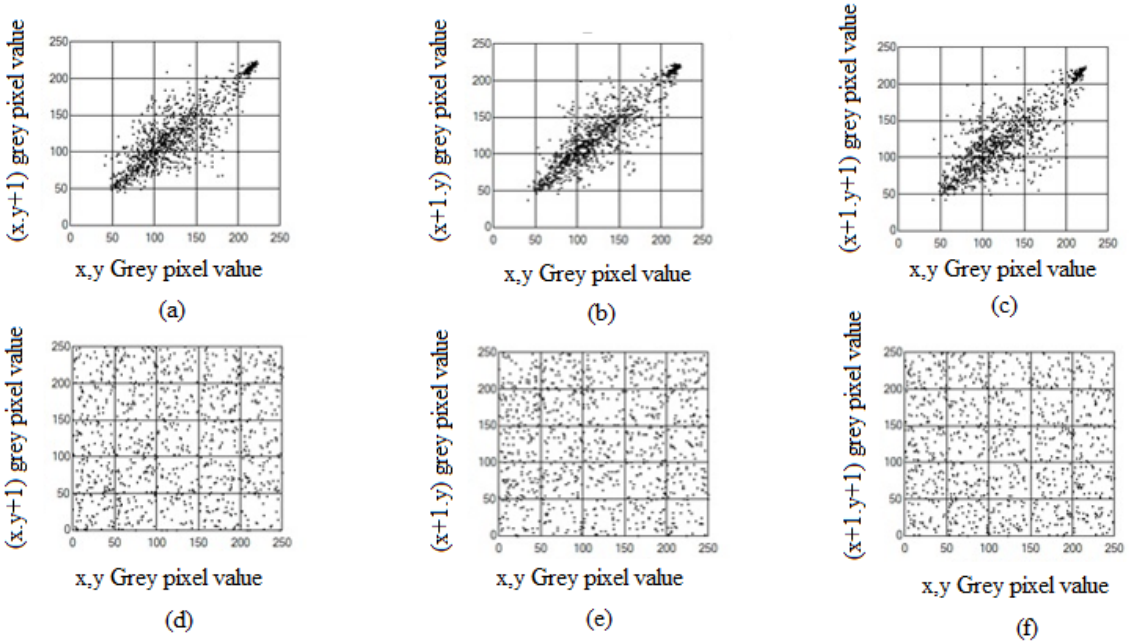



Table 3. Entropy values of mandrill image encrypted with AES

| | **Plain Mandril Image** | **Image encrypted with AES 256-bit key** |
|---|---|---|
| **Horizontal** | 0.96290 | 0.01048 |

| | | |
|---|---|---|
| **Vertical** | 0.93512 | -0.02881 |
| **Diyagonal** | 0.94884 | -0.01724 |

Correlation coefficients according to horizontal, vertical and diagonal pixels in flat picture are 0.96290, 0.93512, 0.94884, respectively. This means the pixels in the flat picture have a strong relationship with their neighbors. The horizontal, vertical, and diagonal correlation coefficients for the picture encrypted with AES using a 256-bit key are 0.01048, -0.02881, and -0.01724, respectively. This means that the encrypted image's pixels have a poor correlation with their neighbors. The correlation coefficients are really close to the ideal value of 0.

**Differential Attack**

Biham and Shamir are the first to introduce differential cryptanalysis (Alvarez et al., 2000, p. 194). The purpose of the differential attack is to discover the secret key. Differential attack examines how small changes in the plain text make changes to the encrypted image. These changes can be used to identify possible keys. Diffusion should be a strong feature of a solid encryption scheme. When a single bit of plaintext is changed, the ciphertext must likewise change unexpectedly. The propagation nature of an image encoding technique can be defined by whether the output pixels of the ciphertext image and the input pixels of the plain image are extremely closely related. The more complex these features of the encryption method are, the more secure it is against differential attacks.

The general strategy for a differential attack is to compare the randomly selected original image with the encrypted images obtained by encrypting a randomly modified pixel with the same key. A small change in the flat image creates a large and unexpected change in the encoded image, neutralizing different attacks. The number of pixel change rate (NPCR - Number of Pixel Change Rate) and the combined average changing intensity (UACI - Unified Average Changing Intensity) techniques are employed in this study to examine the reliability of the picture encryption method using AES against differential assaults.

NPCR is the ratio of pixel differences in encrypted images obtained by encrypting two plain images with the equal key, and it is calculated as in (7). The average density

difference between two encrypted pictures is obtained using the formula in UACI (8). The encrypted pictures c1 and c2 are the plain image and its one-pixel changed variant, respectively, encrypted with the same key.

$$D(i,j) = \begin{cases} 1, & c_{1(i,j)} \neq c_{2(i,j)} \\ 0, & \text{otherwise} \end{cases} \quad (6)$$

$$NPCR = \frac{\sum_{i,j} D(i,j)}{M \times N} \times 100\% \quad (7)$$

$$UACI = \frac{1}{MxN}\left[\sum_{i,j} \frac{|c_{1(i,j)} - c_{2(i,j)}|}{255}\right] \times 100\% \quad (8)$$

Table 4 shows the NPCR and UACI values obtained in encryption with various keys. Because the NPCR and UACI values in this study are close to ideal levels, they can withstand differential type assaults. The ideal value of NPCR and UACI are 99.61 % and 33.46% , respectively(Bensikaddour et al., 2020).

Table 4. NPCR and UACI comparisons of chaotic image coding in the study

| **Key** | **NPCR** | **UACI** |
|---|---|---|
| | **With bit-based scrambling** | **With bit-based scrambling** |
| 1 | 99,62697 | 33,48819 |
| 2 | 99,64311 | 33,56764 |
| 3 | 99,60474 | 33,60573 |
| 4 | 99,60046 | 33,49480 |
| 5 | 99, 64811 | 33,58362 |

## Key Space Study

An effective encryption system must have sufficient key length to with stand assaults using brute force. Theoretically, there is no encryption system that cannot be cracked with brute force attacks. With the advancement of technology, the success times of brute force attacks can be extended with sufficient key sizes. Therefore, encryption systems such as AES are standardized with multiple different key sizes. The AES encryption standard can be used with keys of 128, 192 and 256 bits. To make encryption systems resistant to brute force assaults, Alvarez and Li proposed that key sizes be at least 2100 characters long (Alvarez & Li, 2006, p. 2135). In this study, the AES standard using a 256-bit key is used. This key size is considered secure.

**Key Sensitivity**

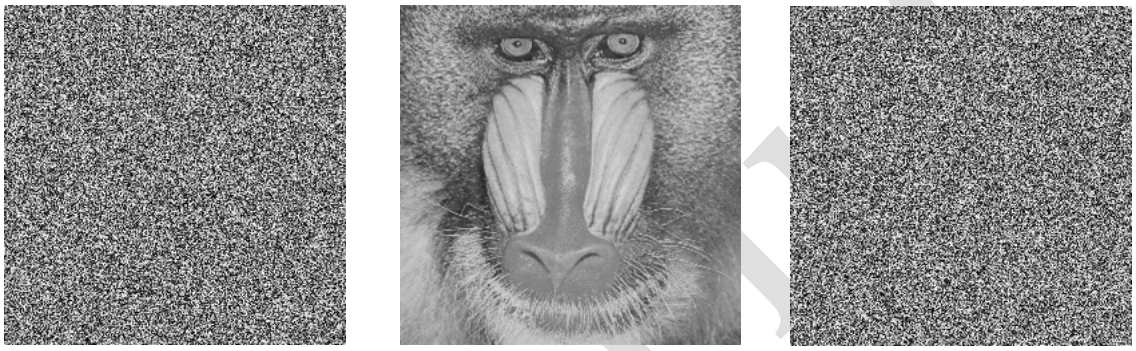
Minor changes in encryption and decryption keys must be detected by a powerful cryptosystem. During the encryption phase, the encrypted picture produced by a little change in the encryption key should be considerably different from the real encrypted image. Similarly, there should be no statistical similarities between the new plain picture acquired and the real flat picture when decryption is conducted with the new key obtained with a little modification in the key used in the decryption step.

The system is sensitive to the smallest change in secret keys, according to encryption and decryption experiments with keys that are very close to each other.The pixel differences between the encrypted picture and the actual encrypted picture produced when we encrypt the same plain picture with a small change in the actual secret key are shown in Table 5. The flat pictures obtained when we decrypt the picture encrypted with the real key and the slightly modified key are shown in Figure 7. As can be seen from Table 5 and Figure 7, the encryption system in this study is sensitive to very small changes in the keys during the encryption and decryption stages.

Table 5. The pixel differences of the picture encrypted with the keys that are very slightly different between them

| | **NPCR** | |
|---|---|---|
| **Image** | **Image size 256x256** | **Image size 512x512** |
| Mandrill | 99.60352 | 99.60645 |

*Figure 7. Key sensitivity in decryption (a) encrypted mandrill picture (b) plain mandrill picture decrypted with real key (c) meaningless picture resulting from decryption by 1-bit change in key*



(a) (b) (c)

**Encryption Quality**

Image encryption quality measurement is a criterion used in the evaluation of image encryption systems. The quality of the encryption is measured by comparing the pixel values of an image that are changed by the encryption process with their original values before encryption. The pixel values of an image change drastically with the encoding process. This change is irregular. The larger the variation in pixel values, the worse the encryption method's quality. The encryption quality of an image algorithm is defined as the difference between the plain image and the encrypted picture (Kalash et al.,2006, p. 279).

P and C represent the flat picture and the encrypted picture of this flat picture with dimensions M x N and L gray level, respectively. P(x, y), C(x, y) $\in$ { 0,1,2...L-1 } will be 0<x<M-1 and 0<y<N-1 will be P plain image and C encrypted image, are the gray level values at (x,y) position in the figure, respectively. If HL(P) is defined as the amount of occurrence of each L gray level pixel value in the encrypted picture and HL(C) as the

amount of occurrence of each L amount of gray pixel value in the plain picture, the level of encryption is the average change of each L gray level that is calculated as

$$\text{Encryption Quality} = \frac{\sum_{L=0}^{255} |H_L(C) - H_L(P)|}{256} \quad (9)$$

Table 6 shows the estimated encryption quality when the picture is encrypted by the AES method with varied key and image sizes.

Table 6. Encryption quality for image encryption with AES

| | **Image size 256x256** | **Image size 512x512** |
|---|---|---|
| **AES 128 bit** | 193.27 | 793,76 |
| **AES 256 bit** | 193.45 | 794,37 |

## Performance Analysis

The encryption algorithm's execution speed is crucial in real-time apps on the internet Table 7 shows the performance of the AES encryption technique for various key sizes.

Table 7. Performance comparisons in encryptions with different key sizes of images of different sizes

| | **Encryption time (ms)** | |
|---|---|---|
| **Algorithm** | **Image size 256x256** | **Image size 512x512** |
| AES 128 bit | 0.132 | 0.467 |
| AES 192 bit | 0.136 | 0.472 |
| AES 256 bit | 0.146 | 0.481 |

As shown in Table 7, the encryption speed decreases as the key size increases. The most appropriate key size should be chosen according to the application needs and the performance-security trade-off. Large key sizes should not be suitable for real-time applications

## DISCUSSION

The capacity to execute encryption and decryption with suitable performance, as well as the unauthorized end system's inability to access information about plain text, are directly proportional to the quality of an encryption system. An excellent encryption system must be safe against all known attacks.

Confidentiality (the message cannot be read by unauthorized people), integrity (the message cannot be changed or corrupted by unauthorized persons, no change can be made on the information), and usability (the message must be fully accessible by the person to whom it is intended) used in the field of information security to accept that the images are securely encrypted. Apart from the conditions, some basic conditions given below must be met.

The encryption system must be computationally very secure. Cracking the password should require huge computation time.

1. Encryption and decryption algorithms should be rapid enough to not affect system performance and simple enough to be implemented by people using home computers.
2. The security method should be adaptable and have a wide range of applications.
3. Encrypted image data should not increase in size too much.

## CONCLUSION

Multimedia files contain larger size data than plain text, so studies have been done with more specific encryption algorithms for their encryption. At the same time, there are specific security analysis methods in addition to the security analysis of plain text encryption methods. Multimedia applications must pass all known security analyzes, thus it can be understood whether it is safe.

As a result of the examinations, it has been observed that in today's world where confidentiality is extremely important and information theft is at its peak, data encryption will further develop and the number of cryptology techniques will become stronger due to the point that technology has reached.

In this study, an evaluation framework has been presented to test the reliability of image encryption methods used in information systems.

The entropy value of the encrypted image is close to the ideal value. Histogram graphs show that the pixel values in the encrypted image are randomly and close to each other. As a result of differential attack analysis, it is observed that NPCR and UACI values are very high for AES. Key sizes of AES are long enough to resist brute force attacks. In the key susceptibility test, NPCR and UACI values are quite high and were close to ideal values. As a result of a series of known security analyzes for image encryption methods, it has been observed that the AES encryption method is a secure method in image encryption. This security framework has been implemented as follows:

i. Visual check is the first stage of the test and, if the plain image's characteristics are not entirely masked, the considered cryptosystem is not secure.

ii. Histogram uniformity is essential to evaluate encryption quality.

iii. The correlation coefficients test examines similarity of pixels with their neighbors to determine whether information is destroyed or not.

iv. The key sensitivity test is a useful tool for assessing the encryption algorithm's diffusion qualities.

v. The entropy analysis tests whether the information has been removed on the encrypted image.

vi. The encryption method's key length should be long enough to withstand brute force assaults.

vii. The most suitable key length should be selected considering the performance-security for the requirements of the application.

An image encryption method has been cosidered as a secure algorithm if it passes all the security mesasurements given above. As a special case, security analyzes were performed on the images encrypted with the AES symmetric encryption method in CBC mode using a 256-bit key, and it has been demonstrated that the AES method is a secure method in image encryption.It is important to note that this security framework can be utilized to examine the security of all image encryption methods, since it just needs the data of files stored in standard image formats such as PNG, JPEG or TIFF.

## REFERENCES AND NOTES

Ahmed, H. H., Kalash, H. M.& Farag Allah, O. S. (2006). Encryption quality analysis of rc5 block cipher algorithm for digital images*, Journal of Optical Engineering, 45, 10 (2006)* 277-284.

Alvarez, G. & Li, S.J. (2006). Some basic cryptographic requirements for chaos-based cryptosystem*,* Int. J. Bifurcat. Chaos,16, 8 (2006) 2129–2151.

Alvarez, G., Montoya, F., Romera, M.& Pastor, G. (2000). Cryptanalysis of a chaotic secure communication system, *Physics Letters A, 276 (2000)* 191-196.

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.

Bhat, B., Ali, A. W., & Gupta, A. (2015, May). DES and AES performance evaluation. In *International Conference on Computing, Communication & Automation* (pp. 887-890). IEEE.

Bensikaddour, E. H., Bentoutou, Y., & Taleb, N. (2020). Embedded implementation of multispectral satellite image encryption using a chaos-based block cipher. *Journal of King Saud University-Computer and Information Sciences*, *32*(1), 50-56.

Bruce, S. (1996). Applied cryptography: protocols, algorithms, and source code in C. El Fishawy, N. F., & Zaid, O. M. A. (2007). Quality of encryption measurement of bitmap images with RC6, MRC6, and Rijndael block cipher algorithms. *Int. J. Netw. Secur.*, *5*(3), 241-251.

Enayatifar, R. (2011) Image encryption via logistic map function and heap tree, *Int. J. Phys. Sci, vol. 6, no. 2, p. 221*

Enayatifar, R.& Abdullah, A.H. Isnin, I.F. (2014). Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence. *Opt Lasers Eng 56:83–93*

Enayatifar, R., Sadaei, H.,Abdullah, A.H., Lee, M. & Isnin, I.F. (2015). A novel chaotic based image encryption using a hybrid model of deoxyribonucleic acid and cellular automata. *Opt Lasers Eng 71:33–41*

FIPS 197, (2001). *Advanced Encryption Standard,* US Department of Commerce, Washington D. C,

Forouzan, B.A. & Mukhopadhyay, D. (2011). *Cryptography and network security (Sie).* McGraw-Hill Education, New York

Gu, G., & Ling, J. (2014). A fast image encryption method by using chaotic 3D cat maps. *Optik*, *125*(17), 4700-4705.

Hasselblatt, B. & Katok, A. (2003). *First Course in Dynamics: With a panorama of recent developments*. Cambridge University Press, Cambridge

Heys, H. M. (2002). A tutorial on linear and differential cryptanalysis. *Cryptologia*, *26*(3), 189-221.

Huang, X., & Ye, G. (2014). An efficient self-adaptive model for chaotic image encryption algorithm. *Communications in Nonlinear Science and Numerical Simulation*, *19*(12), 4094-4104.

Jin, H., Liao, Z., Zou, D., & Li, C. (2008, February). An Asymmetrical Encryption Based automated trust negotiation model. In *2008 2nd IEEE International Conference on Digital Ecosystems and Technologies* (pp. 363-368). IEEE.

Khan, M., & Shah, T. (2014). A literature review on image encryption techniques. *3D Research, 5(4), 1-25.*

Kocarev, L. (2001). Chaos-based cryptography: a brief overview. *IEEE Circuits and Systems Magazine*, *1*(3), 6-21.

Kuo, C. J. (1993). Novel image encryption technique and its application in progressive transmission. *Journal of Electronic Imaging*, *2*(4), 345-351.

Küsters, R., & Tuengerthal, M.(2009, July). Universally composable symmetric encryption. In *2009 22nd IEEE Computer Security Foundations Symposium* (pp. 293-307). IEEE.

Li, S. J. (2003). *Analyses and new designs of digital chaotic ciphers* (Doctoral dissertation, Xi'an Jiaotong University).

Li, S., Chen, G. ve Zheng, X., (2004*). Multimedia Security Handbook*, CRC Press LLC, Boca Raton, 2004.

Li, S., Mou, X. & Cai, Y. (2001) Pseudo-Random Bit Generator Based on Couple Chaotic Systems and Its Applications in Stream Cipher Cryptography, *Indocrypt, Berlin, Springer-Verlag LNCS, 316-329 Shujun Li Xuanqin Mou*

Mao, Y. (2003). Research on chaos-based image encryption and watermarking technology. *Ph. D. thesis*.

Mao, Y., Chen, G., & Lian, S. (2004). A novel fast image encryption scheme based on 3D chaotic baker maps. *International Journal of Bifurcation and chaos*, *14*(10), 3613-3624.

Mao, Y. & Wu, M. (2006). A Joint Signal Processing and Cryptographic Approach to Multimedia Encryption , *IEEE Transactions on Image Processing, 15, 7 (2006)* 2061-2075.

Mohamed, F.K. (2014). A parallel block-based encryption schema for digital images using reversible cellular automata. *Eng Sci Technol Int J 17*(2):85–94

Newton, D. E. (1997) *Encyclopedia of Cryptology,* ABC-CLIO, Santa Barbara, CA

Qiao, L. (1998). *Multimedia security and copyright protection*. University of Illinois at Urbana-Champaign.

Standard, D. E. (1999). Data encryption standard. *Federal Information Processing Standards Publication*, *112*.

Saha, A. & Majumdar, R. (2021). Overview of Multimedia Security. *Retrieved from http://www.academia.edu/8199308/Overview_of_Multimedia_Security.*

Seo, H., Choi, J., Kim, H., Park, T., & Kim, H. (2014, March). Pseudo random number generator and hash function for embedded microprocessors. In *2014 IEEE World Forum on Internet of Things (WF-IoT)* (pp. 37-40). IEEE.

Shannon, C. E. (1949). Communication theory of secrecy systems. *The Bell system technical journal*, *28*(4), 656-715.

Stallings, W. (1999). Secure hash algorithm. *Cryptography and Network Security: Principles and Practice*, 193-197.

Stinson, D. (2002) *Cryptography: Theory and Practice* , Second Edition. Boca Raton: Chapman & Hall / CRC;

Souici, I., Seridi, H., & Akdag, H. (2011). Images encryption by the use of evolutionary algorithms. *Analog Integrated Circuits and Signal Processing*, *69*(1), 49-58.

Umamageswari, A. & Suresh, G. (2013). Security in medical image communication with Arnold's cat map method and reversible watermarking. *International conference on circuits, power and computing technologies (ICCPCT). IEEE, pp* 1116–1121.

Wang, X.& Luan, D. (2013) A novel image encryption algorithm using chaos and reversible cellular automata. *Commun Non-linear Sci Numer Simul 18*(11):3075–3085

Wang, X. Y., Gu, S. X., & Zhang, Y. Q. (2015). Novel image encryption algorithm based on cycle shift and chaotic system. *Optics and Lasers in Engineering*, *68*, 126-134.

Yeung, S.A., Zhu, S. & Zeng, B.(2010). Quality Assessment for a Perceptual Video Encryption System*, Proceedings of the IEEE Wireless Communications, Networking and Information Security (WCNIS) Conference, pp.* 102–106

Zhang, Q., Liu, L. & Wei, X. (2014). Improved algorithm for image encryption based on DNA encoding and multi-chaotic maps. *AEU Int J Electron Commun 68*(3):186–192

Zeng, W., Yu, H., & Lin, C. Y. (Eds.). (2011). *Multimedia security technologies for digital rights management*. Elsevier.

Zhou, J., Au, O., Fan, X. & Wong, P. (2008). Joint security and performance enhancement for secure arithmetic coding, in image processing, *ICIP 2008. 15th IEEE International Conference on. IEEE, 2008, pp.* 3120–3123.