ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 6, December 2012

Analysis and Comparison between AES and DES Cryptographic Algorithm

Shraddha Soni, Himani Agrawal, Dr. (Mrs.) Monisha Sharma

Abstract*—With the rapid development of various multimedia technologies, more and more multimedia data are generated and transmitted, also the internet allows wide distribution of digital media data. Now a days it is much easier to edit, modify and duplicate digital information .Besides that, digital documents are also easy to distribute, therefore it will be faced by many threats. Therefore, it becomes necessary to find appropriate protection as the data may include some sensitive information which should not be accessed by or can only be partially exposed to the general users. So in the recent world, security is a prime important issue, and encryption is one of the best alternative ways to ensure security. More over, many image encryption schemes have been proposed; each one of them has its own strength and weakness. This paper presents an analysis and comparison of various parameters of DES and AES encryption schemes.

***Keywords*— Advance Encryption Standard, Data Encryption Standard, Mean Squared Error, Number of Changing Pixel Rate, Peak Signal to Noise Ratio, Unified Average Changed Intensity.**

I. INTRODUCTION

Cryptography is basically the process of hiding information. Our ATM cards, Computer passwords and transferring data from one place to another are done with cryptography. Cryptography is the science of using mathematics to encrypt and decrypt data. It enables to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient.

Cryptography is the art and science of protecting information from undesirable individuals by converting it into a form non-recognizable by its attackers while stored and transmitted [1]. Data cryptography mainly is the scrambling of the content of data, such as text, image, audio, video and so forth to make the data unreadable, invisible or unintelligible during transmission or storage called Encryption. The main goal of cryptography is keeping data secure form unauthorized attackers. The reverse of data encryption is data Decryption.

Original data that to be transmitted or stored is called plaintext, the one that can be readable and understandable either by a person or by a computer. Whereas the data, which is unreadable, neither human nor machine is called cipher text. A system or product that provides encryption and decryption is called cryptosystem [3]. Cryptosystem uses an encryption algorithms which determines how simple or complex the encryption process will be, the necessary software component, and the key (usually a long string of bits), which works with the algorithm to encrypt and decrypt the data [3], [4]. The security level of an encryption algorithm is measured by the size of its key space [6]. The larger size of the key space is, the more time the attacker needs to do the exhaustive search of the key space, and thus the higher the security level is. In encryption, the key is piece of information (value of comprise a large sequence of random bits) which specifies the particular transformation of plaintext to cipher text, or vice versa during decryption. Encryption key based on the key space, which is the range of the values that can be used to assemble a key. The larger key space the more possible keys can be constructed (e.g. today we commonly use key sizes of 128,192,or 256 bit , so the key size of 256 would provide a 2256 key space) [5],[6]. The strength of the encryption algorithm relies on the secrecy of the key, length of the key, the initialization vector, and how they all work together [6].Cryptography algorithms are either symmetric algorithms, which use symmetric keys (also called secret keys), or asymmetric algorithms, which use asymmetric keys (also called public and private keys) .

II. CRYPTOGRAPHY WITH BLOCK CIPHER

In Cryptography, a block cipher is a symmetric key cipher .A block cipher is a method of encrypting data (to produce cipher text) in which a cryptographic key and algorithm are applied to a block of data (for example, 64 contiguous bits) at once as a group rather than to one bit at a time.

When encrypting, a block cipher might take a (for example) 128-bit block of plaintext as input, and outputs a corresponding 128-bit block of cipher text. The exact transformation is controlled using a second input — the secret key. Decryption is similar: the decryption algorithm takes, in this example, a 128-bit block of cipher text together with the secret key, and yields the original 128-bit block of plaintext. Block ciphers can be contrasted with stream ciphers; a stream cipher operates on individual digits one at a time and the transformation varies during the encryption.

A highly influential block cipher design in the advancement of modern cryptography is Data Encryption Standard (DES, a method for encrypting information). The National Institute of Standards and Technology (NIST) is a federal agency that approved the Data Encryption Standard (DES) block cipher an early encryption algorithm created in the mid 1970s. Initially controversies arose out of classified design elements, a relatively short key length of the symmetric-key block cipher design, and the involvement of the NSA, nourishing suspicions about a backdoor. DES is now considered to be insecure for many applications. This is chiefly due to the 56-bit key size being too small; in January, 1999, distributed.net and the Electronic Frontier Foundation collaborated to publicly break a DES key in 22 hours and 15 minutes . There are also some analytical results which demonstrate theoretical weaknesses in the cipher, although they are infeasible to mount in practice. The algorithm is believed to be practically secure in the form of Triple DES,

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 6, December 2012

although there are theoretical attacks. In recent years, the cipher has been superseded by the Advanced Encryption Standard (AES).

A. Data Encryption Standard (DES)

DES is a block cipher, with a 64-bit block size and a 56-bit key.DES consists of a16-round series of substitution and permutation. In each round, data and key bits are shifted, permutated, XORed, and sent through, 8 s-boxes, a set of lookup tables that are essential to the DES algorithm. Decryption is essentially the same process, performed in reverse [3].

B. Advanced Encryption Standard (AES)

AES uses 10, 12, or 14 rounds. The key size that can be 128,192 or 256 bits depends on the number of rounds. AES uses several rounds in which each round is made of several stages. To provide security AES uses types of transformation. Substitution permutation, mixing and key adding each round of AES except the last uses the four transformations.

III. COMPARISON BETWEEN AES AND DES

In the table below a comparative study between DES and AES is presented in to nine factors, Which are key length, cipher type, block size, developed, cryptanalysis resistance, security, possibility key, possible ACSII printable character keys, time required to check all possible key.

TABLE I
COMPARISON BETWEEN AES AND DES

FACTORS	DES	AES
Key Length	56 bits	128,192 or 256 bits
Block Size	64 bits	128,192 or 256 bits
Cipher Text	Symmetric block cipher	Symmetric block cipher
Developed	1977	2000
Security	Proven inadequate	Considered secure
Cryptanalysis Resistance	Vulnerable to differential and linear cryptanalysis; weak substitution tables	Strong against differential, truncated differential, linear, interpolation and square attacks
Possible Keys	2^{56}	2^{128}, 2^{192} and 2^{256}
Possible ASCII Printable Character Key	95^{7}	95^{16}, 95^{24} or 95^{32}

IV. EXPERIMENTAL RESULTS

An image size of 128*128 (e.g. cameraman, pepper, aero, etc.,) is considered as plain (Original) image and DES and AES encryption and decryption is performed using MATLAB. The visual inspection shown below shows the possibility of applying the algorithm successfully in both encryption and decryption of DES as well as AES. In addition, it reveals its effectiveness in hiding the information contained in it.

V. CORRELATION CO EFFICIENT ANALYSIS

In addition to the theoretical comparisons between DES and AES we have analyzed the correlation between two vertically adjacent pixels, two horizontally adjacent pixels and two diagonally adjacent pixels in plain image and cipher image respectively for both the algorithms. The correlation coefficient can provide the quantitative measure on the randomness of the encrypted images for both the algorithms.

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 6, December 2012

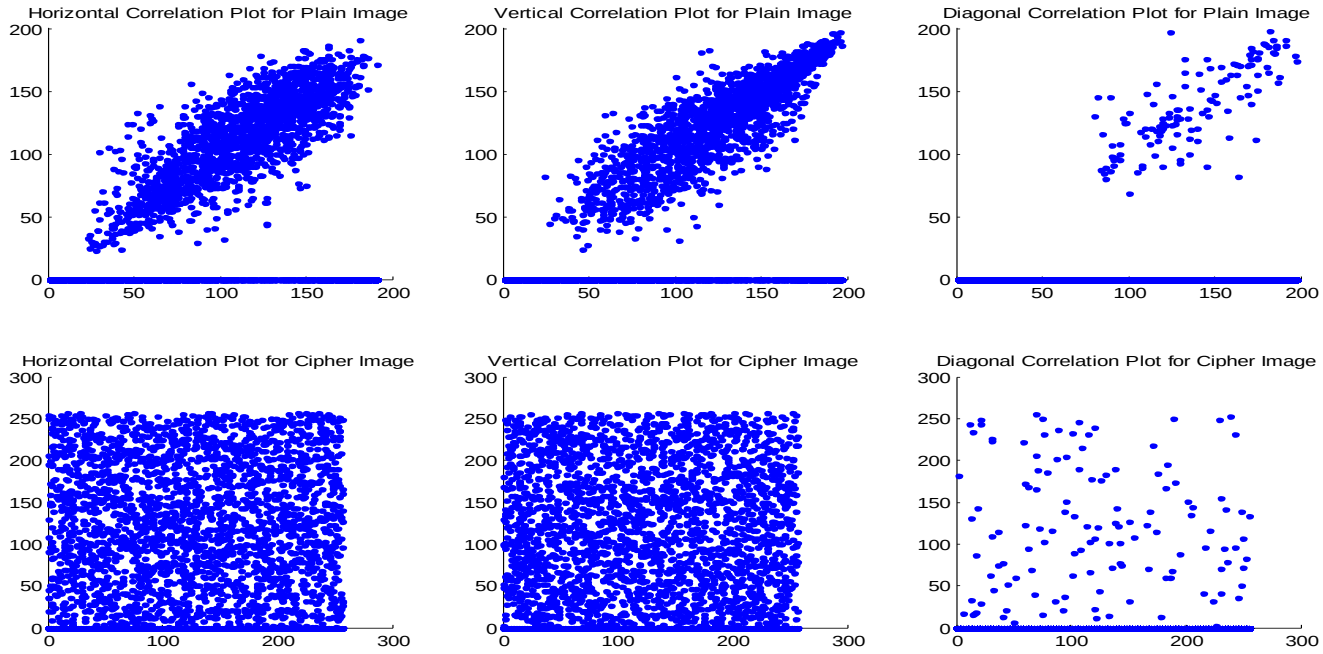

Fig.1 Horizontal, vertical and diagonal correlation of plain and cipher image for DES

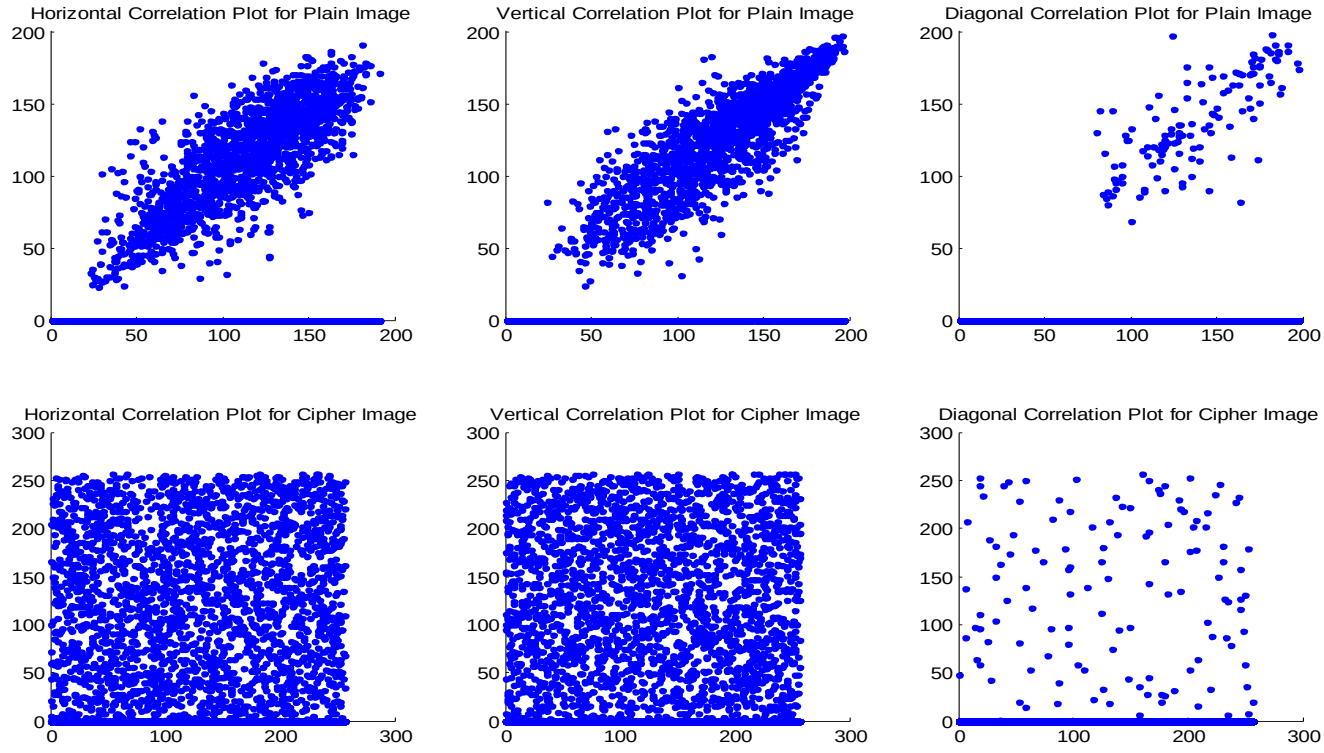

Fig 2 Horizontal, vertical and diagonal correlation of plain and cipher image for AES

Evaluation Parameter

Performance of encryption algorithm is evaluated considering the following parameters.

A. Computation Time

B. Mean Squared Error

C. NPCR

D. PSNR (dB)

E. UAIC

The encryption time is considered the time that an encryption algorithm takes to produces a cipher text from a plain text. Encryption time is used to calculate the throughput of an encryption scheme, is calculated as the total plaintext in bytes encrypted divided by the encryption time. Mean Squared Error is the average squared difference

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 6, December 2012

between a reference image and a distorted image. It is computed pixel-by-pixel by adding up the squared differences of all the pixels and dividing by the total pixel count. The NPCR and UACI are designed to test the number of changing pixels and the number of averaged changed intensity between cipher text images, respectively, when the difference between plaintext images is subtle (usually a single pixel). Peak Signal-to-Noise Ratio is the ratio between the reference signal and the distortion signal in an image, given in decibels. The higher the PSNR, the closer the distorted image is to the original. Comparative analyses of the results of the selected different encryption scheme are performed.

Table II Experimental Analysis of DES and AES

Parameters	DES Algorithm	AES Algorithm
Encryption Time (in sec)	215.9359	99.871
Decryption Time (in sec)	183.5455	84.8904
MSE	8185.4343	8149.8396
NPCR	99.6643	99.6399
PSNR(dB)	7.6057	7.5523
UACI	51.2496	50.8584

VI. CONCLUSION

In this paper a new comparative study between DES and AES were presented. With the theoretical comparisons, experimental analysis and comparison is done for DES and AES algorithms. Based on the text files used and the experimental result it was concluded that AES algorithm consumes least encryption and decryption time as compared to DES algorithm.

REFERENCES

[1] DiaasalamaAbdElminaam, HatemMohamadAbdual Kader, Mohly Mohamed Hadhoud, "Evalution the Performance of Symmetric Encryption Algorithms", international journal of network security vol.10,No.3,pp,216-222,May 2010.

[2] N.K. Pareek., Vinod Patida., K.K. Sud.: Image encryption using chaotic logistic map. Image and Vision Computing 24, PP. 926–934 (2006).

[3] Anoop MS, "Public key Cryptography (Applications Algorithm and Mathematical Explanations)".

[4] Ham, K., Chien, Y. R., Kiesler, K., "An Extended Cryptographic Key Generation Scheme for Multilevel Data Security", Fifth Annual Computer Security Applications Conference, Tucson, AZ, USA 1989.

[5] Kiesler, T., Harn, L., "Cryptographic master key- generation scheme and its application to public key distribution", IEE Proceedings E Computers and Digital Techniques, 1992.

[6] Posch, K. C., Posh, R., "Designing a new encryption method for optimum parallel performance", IEEE First International Conference on Algorithms and Architectures for Parallel Processing, Brisbane, Qld., Australia 1995.

[7] Pieprzyk, J., & Point cheval, D., " Parallel Authentication & Public-Key-Encryption", ACISP'03 Proceedings of the 8th Australasian conference on Information security and privacy, Springer-Verlag Berlin, Heidelberg, 2003.

[8] Dongara, P., Vijay Kumar, T. N., "Accelerating Private-Key Cryptography via Multithreading on Symmetric Multiprocessors", IEEE International Symposium on Performance Analysis of Systems and Software, ISPASS. 2003.

[9] Waheed, F., Muhiuddin, S., Ilyas, S. M., "Multilevel Security for Wireless LAN", Student Conference on Engineering Sciences and Technology, 2005. SCONEST 2005.

[10] Xian, Y., Sun, B., Chen, H, Guizani, S., Wang, R., "Performance Analysis of AES", In Proceedings: GLOBECOM, 2006.

[11] Trinca, D., "Sequential and Parallel Cascaded Convolutional Encryption with Local Propagation: Toward Future Directions in Symmetric Cryptography", IACR Eprint archive, 2006.

[12] Li, X. Chen, J., Qin, D. , Wan, W., "Research & realization based on Hybrid Encryption Algorithm of improved AES & ECC", International Conference on Audio Language and Image Processing (ICALIP), 2010.

[13] Goodwin, J., Wilson, P. R., "Advanced Encryption Standard (AES) Implementation with Increased DPA Resistance & low overhead", IEEE International Symposium on Circuits and Systems, 2008. ISCAS 2008.

[14] Li, H., Li., J., "A New Compact Dual Core Architecture for AES Encryption & Decryption", Canadian Journal of Electrical and Computer Engineering, 2008.

[15] Islam, Md., N., Mia, Md. M. H., Chowdhury, Md. F. I. C., Matin, M. A., "Effect of Security Increment to Symmetric Data Encryption through AES Methodology", Ninth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, 2008. SNPD '08.

[16] Alaidaros, Md. H., Othman, Md., Rasid, Md. F. A., "Improving Security Performance with Parallel Crypto Operations in SSL Bulk Data Transfer", IEEE International Conference on Telecommunications and Malaysia International Conference on Communications, 2007. ICTMICC 2007.

[17] Li, X.,, Chen, J., Lin, W., Wan, W., "An improved AES Encryption Algorithm" IET International Communication Conference on Wireless Mobile and Computing (CCWMC 2009).

[18] Teng, P. Y., Huang, S. I., "Multilevel Data Encryption & Decryption System and Method Thereof", Industrial Technology Research Institute, 2009.