JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue

JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)

An International Scholarly Open Access, Peer-reviewed, Refereed Journal

# Performance Evaluation Between DES and AES Algorithm for Image Transfer

Siddhant Nirhali[1], N.S. Nikam[2], Shubham Ghanekar[3], Aniket Kotkar[4]

*E&TC Department, SPPU Pune.*

[1]siddhant7362@gmail.com

[2]namrata.nikam_skncoe@sinhgad.edu

[3]ghanekarpk90@gmail.com

[4]aniketkotkar0907@gmail.com

***Abstract*****—** Data Encryption Standard was the most well-known utilized cryptographic scheme and it is a symmetric key block cipher algorithm. DES was a widely used cryptosystem for securing the classified data transmissions. There is a considerable increase in the exchange of data over the Internet and other media types. This Data may contain confidential information that needs to be secured from any third party access. Encryption algorithms play a main role for securing these types of data. The encryption algorithms are varied in their performance. This project evaluates the performance of the two encryption algorithms: AES and DES. The performance measure of encryption algorithms will be conducted in terms of processing time, CPU usage and encryption throughput on Windows platform for a different file size. Experimental results are given to demonstrate the performance of each algorithm. In this project DES and AES algorithms are utilized to image file encryption and decryption. The software implementations results are done with Netbeans using the Java programming language. With detailed analysis Experimental results are explained and the proposed plan has strength to resist the developing attacks on security of image file transmissions. The acquired results demonstrate which algorithm could be utilized as a highly secure algorithm.

***Keywords*****— Cryptography, DES, AES, Encryption, Decryption.**

## I. Introduction

In this globalization era, technology has become one of the essential things in life. Everything uses and needs technology. Technology has become an advantage to all of us. However, despite the advantage it brings, there are still some flaws that are uncovered. For instance, because of the vast and fast growth of technology, critical information such as images, data and audio can be leaked. Thus, it is very important to protect and secure the critical information. Cryptography is a widely used technique for hiding data in images for secure information transfer between sender and receiver. There are various cryptography techniques that can be used for protecting and securing information like Data Encryption Standard (DES), Triple DES (3DES), RC4, Blowfish and Advanced Encryption Standard (AES). An algorithm transforms the readable information into cipher-information and vice versa. The process is called encryption and decryption.

In this project, the algorithm used is the DES algorithm. This project focuses on protecting images that contain critical information, such as bank account number, that is transferred between a sender and receiver from being intercepted by an attacker during transmission. By using DES, images can be protected and secured. This is because DES is a block cipher. This means that it operates on fixed-length chunks of data (for example, blocks), applying the same transformation to each block. The transformation is controlled by use of the encryption key. Block ciphers (and thus DES) use symmetric keys, which mean that the same key used to encrypt data is also used to decrypt it.

In the current trends, the technologies have been advanced. Most of the individuals prefer using the internet as the primary medium to transfer data from one end to another across the internet. There are many possible ways to transmit data using the internet like: via e-mails, sending text and images, etc. In the present communication world, images are widely in use. However, one of the main problems with sending data over the Internet is the 'security' and authenticity. Data security basically means protection of data from unauthorized users or attackers. Encryption is one of the techniques for information security. Image encryption is a technique that converts the original image to another form that is difficult to understand. No one can access the content without knowing a decryption key. Image encryption has applications in the corporate world, health care, military operations, and multimedia systems. Encryption is the process of encoding a plain text message into a cipher text message whereas the reverse process of transforming cipher text to plain text is called decryption. Cryptography consists of encryption and decryption techniques. In this paper we have discussed the various encryption terminologies, purpose of cryptography and its types.

## II. LITERATURE SURVEY

| Sr.no | Reference Paper | Authors | Description |
|---|---|---|---|
| 1 | The Design And Implementation of A Symmetric Encryption Algorithm Based On Des | Zhou Yingling | This paper analyzed the weakness that existed in des and proposed two new methods that concurrently operated with two single des processes. The first method swapped the round results which added confusion to the cipher text; the second method alternated the sub key between the two parts to obtain an effect of employing a doubled key length (112-bit) to encrypt a 64-bit block. The simulation results indicated that in terms of operational efficiency, new methods distinctly outperformed 3des and kept the same level as des. With respect to security, new methods provided a more secure performance than des did and at the least as secure as 3des did. |
| 2 | Improved Design of Des Algorithm Based on Symmetric Encryption Algorithm | Wang Yihan | The improved des algorithm proposed here increases the security of the algorithm from the three aspects of increasing the packet length, key length, and the exchange of each round of iterative results. |
| 3 | A Trade-Off Between Security And Throughput In Wireless Channels Using Des Algorithm | Walid Y. Zibideh And Mustafa M. Matalgah | The author introduced new modes for encryption by increasing the block and key lengths. we analyzed the security of the proposed modes in terms of their strength to applicable attacks, we proved that the proposed algorithm is immune to those attacks, by showing that the probability of such successful attacks is almost zero. |
| 4 | Finding the Best Simple FPGA Mentation Of The Des Algorithm To Secure Smart Cards | M'hamed Bougara | In this research, they compared different fpga implementations of the des cryptographic algorithm in order to find the best one for a smart card, their applications demand security hardware with more restrictions on area and power and less on throughput. These results can be helpful for selecting the right fpga for our des implementation according to the application. |
| 5 | Evaluating The Effects of Cryptography Algorithms on Power Consumption For Wireless Devices. | D. S. Abdul. Elminaam Et.Al | The following points are concluded by him from his experimental result. 1) if packet size is changing with or without transmission of data using various wlan protocols and different architectures. It was concluded from the result that blowfish and aes have better performance than other common encryption algorithms used, followed by rc6.wormholes are present in the security mechanism of des and 3des; blowfish and aes do not have such wormholes so far [4]. |

| | | | |
|---|---|---|---|
| 6 | Energy Consumption of Rc4 and AES Algorithms in Wireless Lans | P.Prasithsangaree, P.Krishnamurthy- | rc4 and aes encryption algorithms performance evaluation is made by their research. The matrics for such evaluation are as follows: cpu workload, encryption throughput, key size variation, and energy cost. experimental results conclude that for encrypting large packets the rc4 is energy efficient and fast. However, for a smaller packet size encryption, aes was more efficient than rc4. therefore it appears that by using a combination of rc4 and aes we can save energy to provide encryption for any packet size |
| 7 | A New Modified Version of Advanced Encryption Standard (AES) Based Algorithm For Image Encryption | Seyed Hossein Kamali, Reza Shakerian, Maysam Hedayati, Mohsen Rahmani | The authors proposed an enhanced model of advanced encryption standard to possess a good level of security and a better range of image encryption. the modification process can be carried out by adjusting the shift row transformation. As the result showed, a comparison has been made between the original aes encryption algorithm and the modified algorithm which produces very good encryption results focusing on the security against statistical attacks. |
| 8 | Secure Integration for Both of IOT and Cloud Computing | Christos Stergiou Et Al | This paper proposes that the decode and forward (DF) and amplify-and-forward (AF) model be used instead of the truth relay. df and af provide a strong key in aes which is beneficial security use of the encryption in an integrated model. AES implementation needs less memory which makes it a limited-memory environment. |
| 9 | Performance Evaluation of Symmetric Encryption Algorithms | Mayank Kumar Rusia | Is proposed here to analyze the time-consuming of the known cryptographic algorithms: triple-des, aes and blow-fish and idea. In this model for evaluation, there is one evaluating mode: different plaintexts in the same key (dpsk). as the basis of the evaluating model, the plaintext and the corresponding key are both generated by random numbers" is discussed. |

## III. BLOCK DIAGRAM

### CRYPTOGRAPHY

Cryptography is the Science of information security which is derived from the Greek kryptos, meaning hidden . It is the process of protecting data, converting data into unreadable cipher format. The process of changing data into cipher format is known as encryption while the process of converting back data that is in cipher format to the original data is known as decryption. The purposes of cryptography are as follows:

1) Confidentiality: Assures that private data remains private.
2) Integrity: Assures that an object is not distorted illegitimately.
3) Non-repudiation: Assures against a party denying an information or interaction that they initiated.
4) Authentication: Assure that the characteristic of all parties attempting access.

Cryptography algorithms play an important role in information security. They can be divided into Symmetric and Asymmetric key cryptography. Symmetric algorithms are of two types [3]: block ciphers and stream ciphers. The block ciphers are operating on data in groups or blocks. For instance, Data Encryption Standard (DES), Advanced Encryption Standard (AES) and Blowfish. Stream ciphers are operating on a single bit at a time. RC4 is a stream cipher algorithm. Asymmetric key (or public key) encryption is used to solve the problem of key distribution. In Asymmetric key encryption, two keys are used; private keys and public keys. Public key is used for encryption and private key is used for decryption (e.g. Digital Signatures). Public key is known to the public and private key is known only to the user.

### DATA ENCRYPTION STANDARDS (DES)

DES (and most of the other major symmetric ciphers) is based on a cipher known as the Feistel block cipher. This was a block cipher developed by the IBM cryptography researcher Horst Feistel in the early 70's. It consists of a number of rounds where each round contains bit-shuffling, non-linear substitutions (S-boxes) and exclusive OR operations. Most symmetric encryption schemes today are based on this structure (known as a feistel network). As with most encryption schemes, DES expects two inputs: the plain text to be encrypted and the secret key. The manner in which the plain text is accepted, and the key arrangement used for encryption and decryption, both determine the type of cipher it is. DES is therefore a symmetric, 64 bit block cipher as it uses the same key for both encryption and decryption and only operates on 64 bit blocks of data at a time 5 (be they plain text or cipher text). The key size used is 56 bits, however a 64 bit (or eight-byte) key is actually input. The least significant bit of each byte is either used for parity (odd for DES) or set arbitrarily and does not increase the security in any way. All blocks are numbered from left to right which makes the eight bit of each byte the parity bit. Once a plain-text message is received to be encrypted, it is arranged into 64 bit blocks required for input. If the number of bits in the message is not evenly divisible by 64, then the last block will be padded. Multiple permutations and substitutions are incorporated throughout in order to increase the difficulty of performing a cryptanalysis on the cipher. However, it is generally accepted that the initial and final permutations offer little or no contribution to the security of DES and in fact some software implementations omit them (although strictly speaking these are not DES as they do not adhere to the standard).

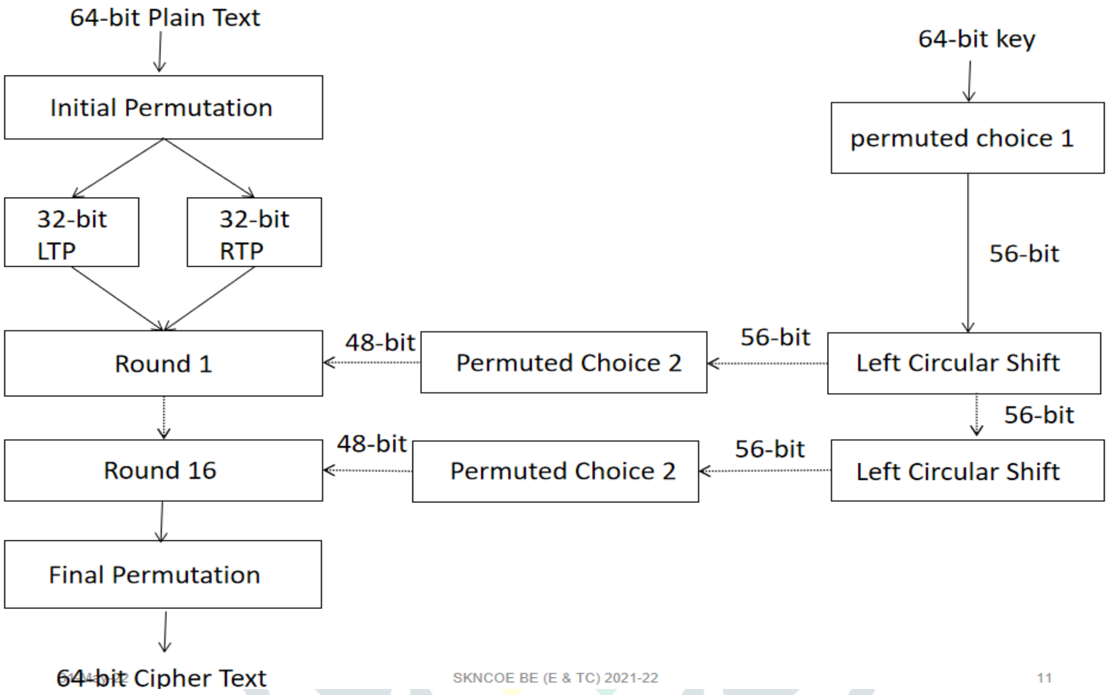

Fig. 1 Block diagram of DES

## IV. IMPLEMENTATION

### Image Encryption

In the encryption method we considered two inputs, one is the encryption secret key and another one is the original color image. Image file can be reshaped or divided by a pixel block of the original image and express the DES encryption process and define the key for encryption that is the secret key. By using the DES algorithm procedure finally the original image is encrypted with security, this is an encrypted image. Image file encryption practice is presented in figure 5.

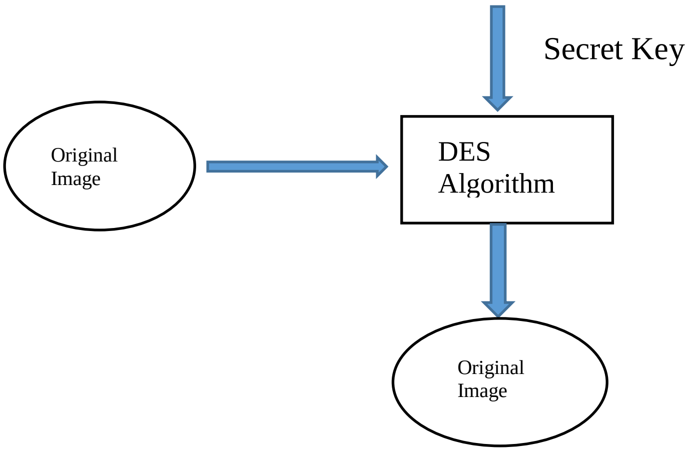

Fig.2 Encryption

**Image Decryption**

It is a reverse process of Image encryption. In this method encrypted image is considered as input for DES algorithm structure for decryption. Encrypted image is divided again into pixel blocks that are the same as DES algorithm block length. Primarily function blocks of 64-bit size are entered. Then the same secrecy key that is the decryption key used for the process of decryption which one is used for encryption. Here we follow a reverse ordered procedure of encryption. After completion of decryption, obtained output is considered as a decrypted image, it follows the same characteristic of the original image.

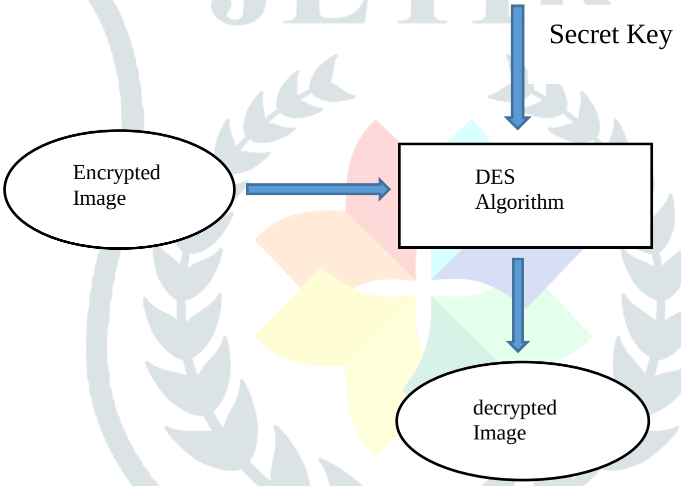

Fig.3 Decryption

## V. RESULT

This part will discuss and focus on the framework of the project. Figure 3 below shows the Result for secure images that contain critical information, account bank number in chat application using DES algorithm. Based on the problem stated in 1.2, this project uses the DES algorithm as a technique to protect data such as images that contain critical information such as bank account number from attackers. In DES, it involves the process of encryption and decryption. Encryption process will change the original image into a cipher-image using a secret key. Meanwhile, the decryption process will convert back the cipher image into the original image using the same secret key as the sender used in the encryption process. The secret key is shared during both encryption and decryption processes. The secret key is only known by sender and receiver who communicate through the chat application. If the image is intercepted during the process of image transfer, the attacker cannot see the original image because the attacker does not know the key used for the encryption and decryption. The image can be exposed to the attacker once only his/her know/ eavesdrops on the secret key used by the sender and receiver. Sender will send the encrypted image to the receiver while the receiver will decrypt the encrypted image to see/get the original image.

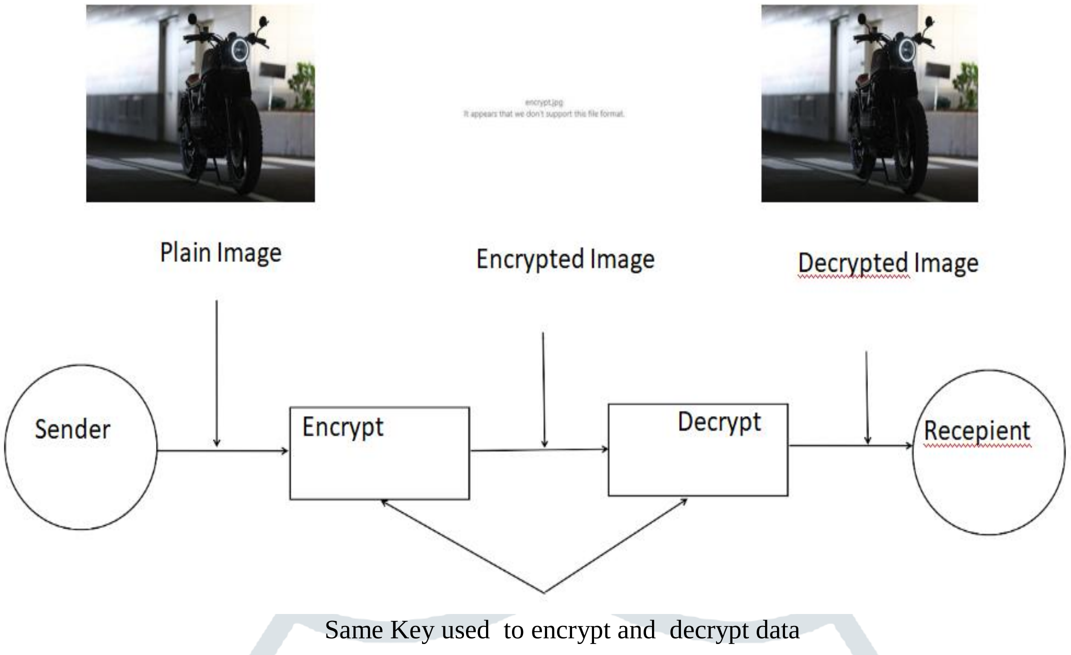
encrypt.jpg
It appears that we don't support this file format.
Plain Image
Encrypted Image
Decrypted Image
Sender
Encrypt
Decrypt
Recepient
Same Key used to encrypt and decrypt data

Fig.4 Result

## VI. CONCLUSIONS

Encryption algorithms play a very important role in communication security. Our research evaluates the performance of the two encryption algorithms AES and DES. The performance measure of encryption algorithms is conducted in terms of processing time, Memory usage and encryption throughput on Windows platform for a different file size. The simulation results conclude that AES is faster than DES in the execution time. AES consumes less Memory usage than DES. Our further research will focus on comparing and analyzing the existing other cryptographic algorithms. It will include experiments on image data and it will focus on improving encryption time.

## ACKNOWLEDGMENT

It gives us great pleasure and satisfaction in presenting this project report on “An Image Encryption and Decryption”. We are thankful to and fortunate enough to get constant encouragement, support and guidance from all Teaching staff of [E & TC Dept] which helped us in successfully completing our project work. Also, We would like to extend our sincere esteems to all staff in the laboratory for their timely support. We have furthermore to thank E & TC Department HOD Dr. S.K. Jagtap and guide Mrs. S.M. Ingawale, Ms. S. S. Palnitkar & Ms. N.S. Nikam encourages us to go ahead and for continuous guidance. We would also like to thank our project team members who showed immense patience and understanding throughout the project. We would like to thank all those, who have directly or indirectly helped us for the completion of the work during this project.

## REFERENCES

[1] Mohammad Amjad, “Security Enhancement of IPV6 Using Advanced Encryption Standard and Diffie Hellman”, International Journal of Scientific Research in Network Security and Communication, Vol.5, Issue.3, pp.182-187, 2017

[2] Roshni Padate, Aamna Patel, “Image Encryption and Decryption Using AES Algorithm”, International Journal of Electronics and Communication Engineering & Technology (IJECET), Vol.6, Issue.3, pp.23-29, 2015.

[3] Joseph Albahari, Ben Albahari C# 5.0 in a Nutshell: The Definitive Reference, 2015.Andrew Troelsen Pro C# 5.0 and the .NET 4.5 Framework (Expert’s Voice in .NET 2014.

[4] A K Mandal, C Prakash and Mrs. A Tiwari, “Performance Evaluation of Cryptographic Algorithms: DES and AES”, IEEE Students’ Conference on E and E,C S, pp. 1-5, 2012.

[5] Sumitra, “Comparative Analysis of AES and DES security Algorithms” (International Journal of Scientific and Research Publications), Volume 3, Issue 1, January 2013 1 ISSN 2250-3153.

[6] Joseph Albahari, Ben Albahari C# 5.0 in a Nutshell: The Definitive Reference, 2015.Andrew Troelsen Pro C# 5.0 and the .NET 4.5 Framework (Expert’s Voice in .NET 2014.

[7] R. Huang and K. Sakurai,“A robust and compression combined digital image encryption method based on compressive sensing,”.The7t International Conference on IIH-MSP, Dalian, Oct.2014–16 2011, pp. 105–108.

[8] A K Mandal, C Prakash and Mrs. A Tiwari, “Performance Evaluation of Cryptographic Algorithms: DES and AES”, IEEE Students’ Conference on E and E,C S, pp. 1-5, 2012.