International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

# A Survey Paper Based On Image Encryption and Decryption Using Modified Advanced Encryption Standard

**Yogita Verma[1], Neerja Dharmale[2]**

[1]M Tech Scholar Digital Electronics RCET Bhilai, India

[2]Assistant Professor (ET&T) RCET Bhilai, India

**Abstract:** ***Now Days the multimedia data protection is becoming very important. The encryption technique is used to protect multimedia data. There are different techniques used to protect confidential image data from unauthorized access. In this paper, we have a tendency to survey on existing work that is employed totally different techniques for image encryption and that we additionally provide general introduction regarding cryptography.***

**Keywords:** Encryption, Decryption, Data Encryption Standard (DES),Advanced Encryption Standard (AES), Blowfish, Modified Advanced Encryption Standard (MAES).

## 1. Introduction

With the ever-increasing growth of multimedia applications, Important issue for communication and storage of images is security, and encryption is one the technique to ensure security. encryption techniques convert original image to another image that is hard to understand; to keep the image confidential between users, in other word, it is essential that nobody could get to know the confidential message without a key for decryption. Their different encryption techniques are used to protect the confidential message from unauthorized user. Encryption is a very common technique for promoting the information security. The evolution of encryption is moving towards a future of endless possibilities.

## 2. Literature Survey

Some of the concepts used in cryptography are Described here [1,2]:

### 2.1 Cryptography

- Plain Text: Any communication in the language that we speak- that is the human language, takes the form of plain text. It is understood by the sender, the recipient and also by anyone who gets an access to that message.
- Cipher Text: Cipher means a code or a secret Message. When a plain text is codified using any Suitable scheme the resulting message is called as Cipher text.
- Encryption: The process of converting of plain text Messages into cipher text messages are called Encryption.
- Decryption: The reverse process of encryption i.e. Cipher text messages back to plain text is called as Decryption.
- Key: An important element of performing encryption and decryption is the key. It is the key used for Encryption and decryption that makes the process of Cryptography secure.

### 2.2 Purpose of Cryptography

- Authentication: Authentication mechanisms facilitate to determine proof of identities. This method ensures that the origin of the message is properly known.
- Integrity: The integrity mechanism ensures that the contents of the message stay an equivalent once it reaches the meant recipient as sent by the sender.

### 2.3 Types of Cryptography

Two types of cryptography:

- Symmetric Key Cryptography: When the similar key is used for both encryption and decryption, then that Mechanism is known as symmetric key cryptography.
- Asymmetric Key Cryptography: When two different keys are used, that is one key for encryption and another key for decryption, then that mechanism is known as asymmetric key cryptography.

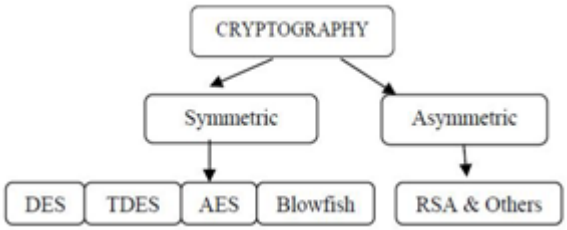


**Figure 1**: Classification of Cryptography

### A. Data Encryption Standard (DES)

DES is a block cipher that uses shared secret key for encryption and decryption. DES encryption technique is described by Davis R. [3] takes a fixed-length string of plaintext bits and transforms it through a series of complicated operations into cipher text bit string of the same length. In the case of DES, each block size is 64 bits. DES uses a key of 56 bits for encryption, so that decryption process can only be performed by those who know the key which is used for encrypt the message. There are 16 stages of

processing all stages are identical, termed rounds. There is also an initial and final permutation, termed IP and FP, which are inverses (IP "undoes" the action of FP, and vice versa). The Broad level steps in DES are as follows [1]:

1) In the first step, the 64-bit plain text message is handed over to an Initial permutation (IP) function.
2) The initial permutation is performed on plain text.
3) The IP produces two halves of the permuted message; Left Plain Text (LPT) and Right Plain Text (RPT).
4) Now, each of LPT and RPT go through 16 rounds of encryption process.
5) In the end, LPT and RPT are rejoined and a final Permutation (FP) is performed on the combined block.
6) The result of this process produces 64-bit cipher text. Rounds: Each of the 16 stages, in turn, consists of the broad level steps and shown in Figure 2.

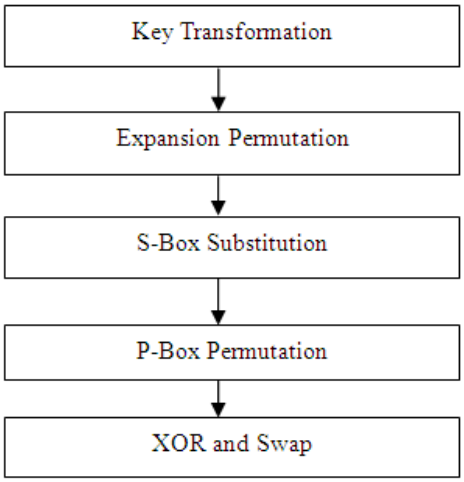


**Figure 2:** Details of One Round in DES

### B. 3DES

3DES (Triple DES) is an enhancement of DES; it is 64 bit block size with 192 bits key size. In this standard the encryption method is same as original DES but applied 3 times to increase the encryption level and the average safe time. It is a known fact that 3DES is take more time DES i.e. 3DES is slower than other block cipher methods. It uses either two or three 56 bit keys in the sequence Encrypt-Decrypt-Encrypt (EDE). Initially, three different keys are used for the encryption algorithm to generate cipher text on plaintext message t,

$$C(t) = Ek1(Dk2(Ek3(t))) \quad (1)$$

Where C (t) is cipher text produced from plain text t, Ek1 is the encryption method using key k1 Dk2 is the decryption method using key k2 Ek3 is the encryption method using key k3 Another option is to use two different keys for the encryption algorithm which reduces the memory requirement of keys in TDES. TDES

$$C(t) = Ek1(Dk2(Ek3(t))) \quad (2)$$

TDES algorithm with three keys requires i.e. 2^168 possible combinations and with two keys requires 2^112 combinations. It is practically not possible to try such a huge combination so TDES is a strongest encryption algorithm. The disadvantage of this algorithm it is too time consuming.

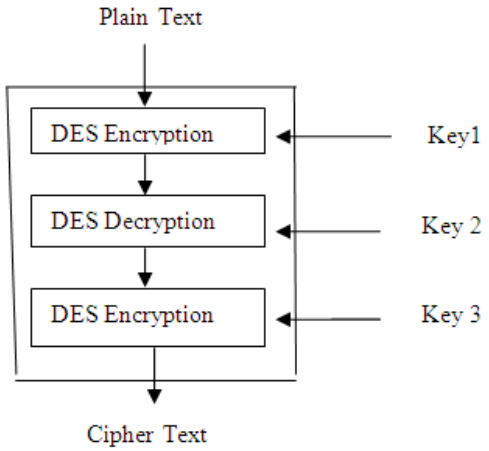


**Figure 3:** 3DES algorithm

### C. Advanced Encryption Standard ( AES)

The AES cipher [4] is almost identical to the block cipher Rijndael cipher developed by two Belgian cryptographers, Joan Daemen and Vincent Rijmen. The AES algorithm is a symmetric-key algorithm, means the same key is used for both encrypting and decrypting the data. The number of internal rounds of the cipher is a function of the key length. The number of rounds for 128-Bit key is 10. Unlike its predecessor DES, AES does not use a Feistel network. Feistel networks do not encrypt an entire block per iteration, e.g., in DES, 64/2 = 32 bits are encrypted in one round. AES, on the other hand, encrypts all 128 bits in one iteration. This is one reason why it has a comparably small number of rounds.AES algorithm shown in figure 4.

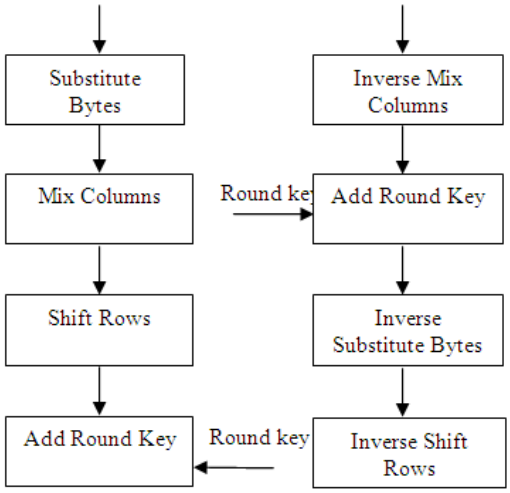


**Figure 4:** One Round of encryption and Decryption in AES

Encryption Round Decryption Round Each processing Round involves four steps:-

- Substitute byte: A non-linear substitution step wherever every byte is replaced with another byte using lookup table.
- Shift rows: A transposition step in this step each row of the state is shifted cyclically a certain number of steps.
- Mix column: In mixing operation the columns of the state, combining the four bytes in each column.
- Add round key: each byte of the state is XOR With the round key using bitwise.

- Decryption: Decryption involves reversing of all the steps taken in encryption using inverse functions like InvSubBytes, InvShiftRows, InvMixColumns.

### D. Blowfish

Blowfish [5] is one of the most common public domain Encryption algorithms provided by Bruce Schneier. The blowfish Encryption is shown in figure5 below, Blowfish encrypts 64-bit block cipher with variable length from 32 bits to 448 bits Key. It contains two parts

- Sub key Generation: This process converts the key up to 448 bits long to subkeys to totaling 4168 bits.
- Data Encryption: In this part the iteration of a simple function of 16 rounds. Each iteration contains a key dependent permutation and key- and data dependent substitution. Blowfish suits the applications where the key remain constant for a long time (e.g. communication link encryption) but not where the key changes frequently (e.g. packet switching).

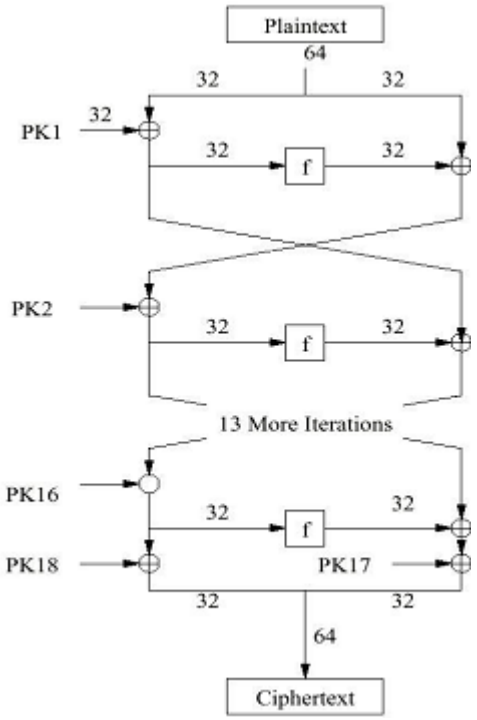


**Figure 5:** Blowfish Encryption

## 3. Comparison

E. Thambiraja, G.Ramesh and Dr. R. Umarani in [8] Have done survey on most common encryption Techniques. Monika Agrawal and Pradeep Mishra in [9] have also done a comparative survey on Symmetric Key Encryption Techniques. Gurjeevan Singh, Ashwani Kumar Singla and K.S.Sandha in [4] have provided comparison of various cryptographic algorithms.

**Table 1**: Comparison Table

| *Algorithm* | *Key Size (Bits)* | *Block Size (Bits)* | *Average Encryption Time (Ms)* |
|---|---|---|---|
| DES | **56** | **64** | 663.31 |
| 3DES | 112 or 168 | **64** | 742.31 |
| AES | 256 | **128** | 542.38 |
| BLOWFISH | 32 - 448 | **64** | 91.92 |

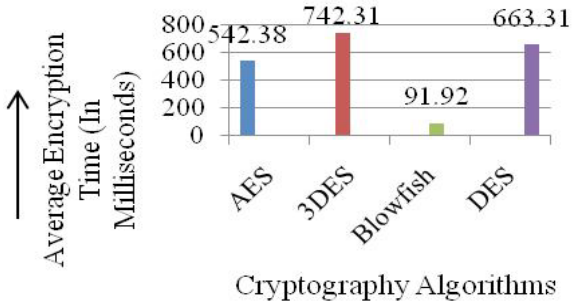


**Figure 6:** Encryption Time of Each Algorithm (In ms)

## 4. Methodology

**Modified Advanced Encryption standard**

The algorithm is divided into four operational blocks where we observe the data at either bytes or bit levels and the algorithm is designed to treat any combination of data and 128 bits of key size is flexible. The four stages that we use for Modified-AES Algorithm are:

- Substitution bytes
- Mix columns
- Shift Row
- Add Round Key

For decryption, each round consists of the following four steps:

- Inverse shift rows
- Inverse substitute bytes
- Add round key
- Inverse mix columns.

We try to modify the AES to be more efficient and secure way by adjusting the Shift Row phase. Shift Row Phase: Instead of the original Shift row, we modify it as:

a) Check the value in the first row and first Column,(state [0][0]) is even or odd.
b) If it is odd, The Shift Rows step operates on the Rows of the state; it cyclically shifts the bytes in Each row by a certain offset. For MAES, the first And third rows are unchanged and each byte of The second row is shifted one to the left. Similarly, the fourth row is shifted by three to the left respectively.
c) If it is even, The Shift Rows step operates on the Rows of the state; it cyclically shifts the bytes in each row by a certain offset. The first and fourth Rows are remains same and each byte of the second Row is shifted three to the right. Similarly, the Third row is shifted by tow respectively on to the Right.

## 5. Conclusion

Cryptography is technique for secure communication, in this paper, it has been surveyed about the existing works on the encryption techniques are AES, 3DES, Blowfish and DES.DES key size is too small as compare to other techniques. 3DES is slower than other block cipher methods and has poor performance. AES is supposed to be better algorithm which was Compared to original Blowfish Algorithm. And the adjacent pixels in an image are of close

relation which cannot be removed by AES algorithm. Besides the security issue, encrypting images with these ciphers directly is time consuming and not suitable for real-time applications. To improving this problems modified advanced encryption Standard method is proposed. This modification may improve the security and also increased performance.

## References

**[1]** William Stallings "Network Security Essentials(Applications and Standards)", Pearson Education, 2004.
[2] Bruce Schneier"Applied Cryptography, Second Edition, John Wiley & Sons1996.
[3] Davis, R., "The Data Encryption Standard in Perspective," Proceeding of Communication Society magazine, IEEE, Volume 16 No 6, pp. 5-6, Nov. 1978.
[4] Manoj. B, Manjula N Harihar , "Image Encryption and Decryption using AES " International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-1, Issue-5, June 2012.
[5] Pratap Chnadra Mandal "Superiority of Blowfish Algorithm," International Journal Of Advanced Research in Computers Science and Software Engineering Vol 2 Issue 9, September 2012.
[6] Kundankumar Rameshwar Saraf, Vishal Prakash Jagtap, Amit Kumar Mishra,"Text and Image Encryption Decryption Using Advanced Encryption Standard", International Journal of Emerging Trends & Technology in Computer Science, May – June 2014
[7] Gurjeevan Singh, Ashwani Kumar Singla, K.S.Sandha " Performance Evaluation of Symmetric Cryptography Algorithms," International Journal of Electronics and Communication Technology Volume 2 Issue 3, September 2011.
[8] E. Thambiraja, G.Ramesh, Dr. R. Umarani, "A survey on various most common encryption techniques," International Journal of Advanced Research in ComputerScience and Software Engineering, Vol 2, Issue 7, July 2012.
[9] Monika Agrawal, Pradeep Mishra,"A Comparative Survey on Symmetric Key Encryption Techniques," International Journal on Computer Science and Engineering (IJCSE), Vol. 4 No. 05 May 2012, PP877-882.
[10] Salma Hesham, Mohamed A. Abd El Ghany and Klaus Hofmann,"High Throughput Architecture for the Advanced Encryption Standard Algorithm" IEEE 2014.
[11] Pravin Kawle, Avinash Hiwase, Gautam Bagde, Ekant Tekam, Rahul Kalbande, "Modified Advanced Encryption Standard", International Journal of Soft Computing and Engineering (IJSCE), Volume-4, Issue-1, March 2014.
[12] Sruthi B. Asok , P. Karthigaikumar, Sandhya R, Naveen Jarold K, N.M Siva Mangai,"A Secure Cryptographic Scheme For Audio Signals" IEEE 2013.