MODIFICATION IN ADVANCED ENCRYPTION STANDARD

[1] VANDANA C. KORADIA

[1] Student, Department of Computer & Science, Noble Engineering College, Junagadh, Gujarat.

Koradiavandana88@gmail.com

ABSTRACT: *It is important aspect to protect the confidential multimedia data from unauthorized access. Multimedia content can be text, audio, still images, animation and video. Such contents are protected by multimedia security method. Commonly, this is attained by techniques that are profoundly based on cryptography.in this paper first I will give basic approach of symmetric key encryption technique. then I have taken concept of existed advanced encryption standard algorithm. after I give my proposed structure for modified advanced encryption standard algorithm which will provide high speed and security.*

KEYWORDS: *Advanced Encryption standard (AES), cryptography, DES, and symmetric key algorithms.*

1.INTRODUCTION

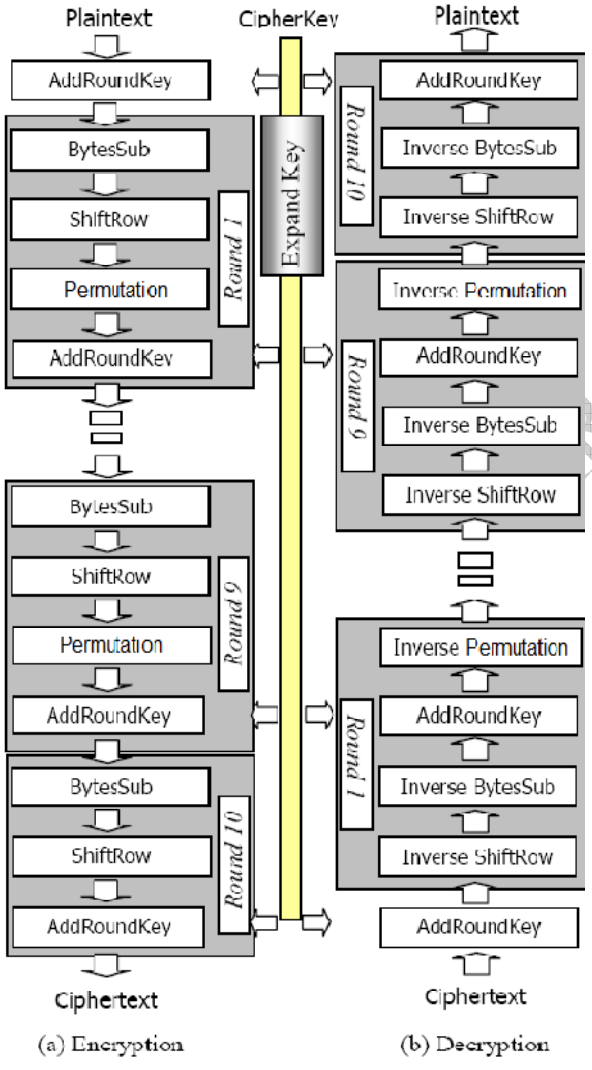
It is an important aspect to protect the confidential multimedia data from unauthorized access. Multimedia content can be text, audio, still images, animation and video. Suchcontents are protected by multimedia security method.this is attained by techniques that are based on cryptography.These schemes facilitatecommunication security, piracy and shelter. [2]Large size of images causes certain challenges for encryption. Normally a typicalimage has a very large size. Using traditional encryption algorithm will make encryptiondifficult for large volume of multimedia data. For the encryption of any multimedia datawe need such algorithms that require less computation because of large size of data. [1, 2,3] Symmetric-key algorithms are fewer computationally serious than any Asymmetrickey algorithms. Typically, symmetric key algorithms are thousands times sooner thanthose of the asymmetric algorithms. [6] So the better suitable method to encrypt themultimedia data is, to encrypt it with symmetric key encryption algorithms.As a consequence of hardware implementation AES is very fast symmetric blockalgorithm. This method is known as naïve approach. Applying the naïve approach onenormous amount of data takes large computation and makes the encryption speed veryslow due to variety of restrictions. [2, 3] But when we apply these techniques on more complex multimedia (mostly images)or when the size of text data is very large, it produces significant computational overhead.[1, 2, 3]

Our research is concerned with optimizing the existing standards of cryptography for the images and text data encryption. It is also slanting towards exploiting thehuge amount of data, in order to attain preferred speed. This edited AES is referred to asModified-AES algorithm. The modification is done by totaling the Initial Permutationstep, takes from DES , in order to enlarge the encryptionperformance. This modification indubitably increases the efficiency of encryption andmakes the algorithm speedier than the existing one.

2.PROPOSED TECHNIQUE

To overcome the problem of high calculation and computational overhead, we analyzethe Advanced Encryption Standard (AES) and modify it, to reduce the calculation ofalgorithm and for improving the encryption performance. So we develop and implement amodified AES based Algorithm for all kind of data. The basic aim to modify AES is toprovide less computation and better security for data. The modify AES algorithm adjuststo provide better encryption speed.In Modified-AES the block length and the key length are specified according to AESspecification: three key length alternatives 128, 192, or 256 bits and block length of 128bits. We assume a key length of 128 bits, which is most commonly implemented.In Modified-AES encryption and decryption process resembles to that of AES, inaccount of number of rounds, data and key size. The round function consists of fourstages. To overcome the problem of high calculation we skip the Mixcolumn step and addthe permutation. Mixcolumn gives better security but it takes large calculation that makesthe encryption algorithm slow [8]. The other three

junctures remain unbothered as it is inSumira et al: Modified Advanced Encryption Standard For Text And Images123the AES. A single 128-bit block is the input to the encryption and decryption algorithms.This block is a 4×4 square matrix consisting of bytes. This block is copied into the statearray. The state array is modified at each stage of encryption or decryption. Similarly the128-bit key is also depicted into a square matrix.The 128-bit key is expressed into an array of key schedule words: each word is offour bytes. The totals key schedule words for ten rounds are 44 words; each round key issimilar to one state. The block diagram of the Modified-AES algorithm with 128 bitsdata is shown below.



Figure[2]:modified advanced encryption standard

The algorithm is divided into four operational blocks where we observe the data ateither bytes or bit levels and the algorithm is designed to treat any combination of dataand is flexible for key size of 128 bits. These four operational blocks represent one roundof Modified-AES. [7, 8]

Rounds of Modified-AES Algorithm

There are 10 rounds for full encryption. The four different stages that we use for
Modified-AES Algorithm are:

- Substitution bytes
- ShiftRows
- Permutation
- AddRoundKey

Substitution Bytes, ShiftRows and AddRoundKey remain unaffected as it is in theAES. Here the important function is Permutation which is used instead of Mixcolumn.These rounds are managed by the following the conversions shown in Fig.1Permutation is widely used in cryptographic algorithms. Permutation operations areinteresting and important from both cryptographic and architectural points of view.Tables characterize the permutation and its contrary; the DES algorithm will provide uspermutation tables. The inputs to the IP table consist of 64 bits. Modified-AES algorithmtakes 128 bits as input. The functions Substitution Bytes and ShiftRows are alsointerpreted as 128 bits whereas the Permutation function takes 64 bits. We divide theconsequential bits of ShiftRows function into two parts of 64 bits and then take each partof 64 bits as input of permutation tables and shift bits one by one according to that table.We fetch one bit from the source, and put it into the correct position in the destination.Each bit of a block is subject to initial permutation, which can be represented by thefollowing initial permutation (IP) table

IP

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

In the permutation table each entry indicates a specific position of a numbered inputbit consisting of 64 bits in the output. While reading the table from left to right and thenfrom top to bottom, we

observe that the 58th bit of the 64-bit block is in first position,the 50th is in second position and so forth.

3.TEST ON TEXT FILES

To test the algorithm we take the different size of text and image files and compare the calculated time of both the Modified-AES with Advanced Encryption Standard .Table shows the comparison results performed on different sizes of text files using Modified-AES and the AES algorithm.

File size	AES	Modified-AES
10kb	00:00:01:9624000	00:00:00:7332000
20kb	00:00:05:9436000	00:00:01:3884000
30kb	00:00:09:2040000	00:00:02:4180000
40kb	00:00:12:0276000	00:00:03:8064000
50kb	00:00:16:7232000	00:00:06:0998000
60kb	00:00:20:2488000	00:00:08:8296000
70kb	00:00:25:3812000	00:00:10:6080000
80kb	00:00:30:0786000	00:00:14:1180000
90kb	00:00:36:0098000	00:00:17.113200

TABLE.1 ENCRYPTION RESULTS FOR TEXT FILES

4. CONCLUSION

Usually lightweight encryption algorithms are very attractive for multimediaapplications. Luckily I have achieved through our research a fast lightweightencryption algorithm to secure our multimedia data from unauthorized access. For thesecurity of multimedia data, we have proposed an encryption algorithm that is based onAES using symmetric key encryption algorithm. In version of security analysis andexperimental results our proposed encryption scheme is fast and on the other hand itprovides good security and adds very less overhead on the data, this today is therequirement of most of the multimedia applications. Theoretical analysis andexperimental results of the achievement makes it very suitable for high rate and lessoverhead on the data. For all these compensation it is suitable for any large scale text andimage transfer.

,

5. REFERENCES

1. Dominik Engel Thomas stutz,AndreasUhl,"A survey on JPEF2000 encryption", Multimediasystems[online] SpringerLinkVerlag pp.1 -29, ,2008.

2. Shtewi,A.M. "An Efficient Modified Advanced Encryption Standard (MAES) adapted forimage cryptosystems" IJCSNS International Journal of Computer Science and NetworkSecurity, VOL.10 No.2, pp 226-232 February 2010Sumira

3. ShiguoLian," Quasi-commutative watermarking and encryption for secure media content distribution",[online], Multimedia Tools and Applications Volume 43, Number 1 / May,2009

4. Tanya E. Seidel, Daniel Socek, Designs, Codes and Cryptography [EBOOK], Volume 32 Issue 1-3 (May-July 2004) Kluwer Academic Publishers Norwell, MA, USA

5. "Announcing the ADVANCED ENCRYPTION STANDARD (AES)", Federal InformationProcessing Standards Publication 197 November 26, 2000.

6. Fahad Bin Muhaya." Modified AES Using Chaotic Key Generator for Satellite ImageryEncryption", Emerging Intelligent Computing Technology and Applications Volume5754/2009 PP 1014-1024, 2009.

7. Krishnamurthy G N, V Ramaswamy. "Making AES Stronger: AES with Key Dependent SBox,"IJCSNS International Journal of Computer Science and Network Security, VOL.8No.9, pp 388-398, September 2008.

8. P. Noo-intara, S. Chantarawong, and S. Choomchuay "Architectures for MixColumnTransform for the AES" Department of Electronics, Faculty of Engineering, and ResearchCenter for Communications and Information Technology (ReCCIT) King Mongkut's Instituteof Technology Ladkrabang (KMITL), Bangkok 10520