ISSN: 2455 - 1597

ijergs
Open Access

International Journal of Engineering Research and Generic Science (IJERGS)
Available Online at www.ijergs.in

Volume - 5, Issue - 2, March – April - 2019, Page No. 114 - 119

Review on: Different Cryptography Algorithm for Video

Pradeep Jha, Karuna Soni, Shalini Joshi

Assistant Professor, Department of CSE, Arya College of Engineering and Research Centre, Jaipur

Abstract

As the various multimedia technologies are rapidly developing, more and more multimedia data are generated and transmitted in the medical ,commercial and military fields which may include some sensitive information which should not be accessed by or can only be partially exposed to the general users. In this paper, a description and comparison between encryption methods and representative video algorithms were presented. With respect not only to their encryption speed but also their security level and stream size.

Keyword*:* MAES, AES, RSA, VIDEO, 3DES

Introduction

Encryption is the process of encoding information so it cannot be read by hackers. The information is encrypted using AES algorithm and is converted into a form unreadable, which is called a cipher text . The authorized person will decode the information using decryption algorithms. The cryptography algorithms are of three types symmetric cryptography (using 1 key), asymmetric cryptography (using 2 different keys), and cryptographic hash functions using no keys. Symmetric algorithms are faster than asymmetric algorithms since the CPU cycles needed for symmetric encryption are fewer than for asymmetric encryption. Advanced Encryption Standard (AES), Data Encryption Standard (DES), Triple DES, Rivest Cipher (RC2), Rivest Cipher (RC6), and Blowfish are some of the symmetric algorithms. Users are eager to not only enjoy the convenience of real-time video streaming also share various media information in a rather cheap way without awareness of possibly violating copyrights. In view of these, encryption and watermarking technologies have been recognized as a helpful way in dealing with the copyright protection problem in the past decade. Encryption allows secure end –end communication of data while digital watermarking allowing still faces some challenging difficulties for practical uses; there are no other techniques that are ready to substitute it. Within the signal processing and multimedia communities, many schemes have been proposed for protecting sensitive information while allowing certain legitimate operations to be performed. These schemes typically lack a rigorous model of privacy, and their protection becomes questionable when scaled to large datasets. The cryptography community has long developed rigorous privacy models and provably secure procedures for data manipulations. However, these procedures are primarily designed for generic data. As a result, they usually lead to a blow up in computational costs and overheads when applied to real-life multimedia applications. In a real time, the transmitted frames are sent within a minimum delay. Also, video frames need to be displayed at a certain rate; therefore, sending and receiving encrypted data must be sent at a certain amount of time so as to utilize the a cceptable delay such as Video on-Demand requires that the video stream needs to be played whenever the receiver asks. So, there are no buffer or playback concepts for the video stream (i.e. it runs in real time). The size of a two - hour MPEG video is about 1 GB. Performance of processing multimedia

streams should be acceptable. The encryption techniques should be fast enough and require a small overhead in comparison to compression techniques. The security of video data is needed for many applications such as Computer forensics and Distance education. Computer forensics require secured good quality video for presenting digital evidence in the courtroom, and Distant education and training needs encryption for no alteration of information.

Background Theory

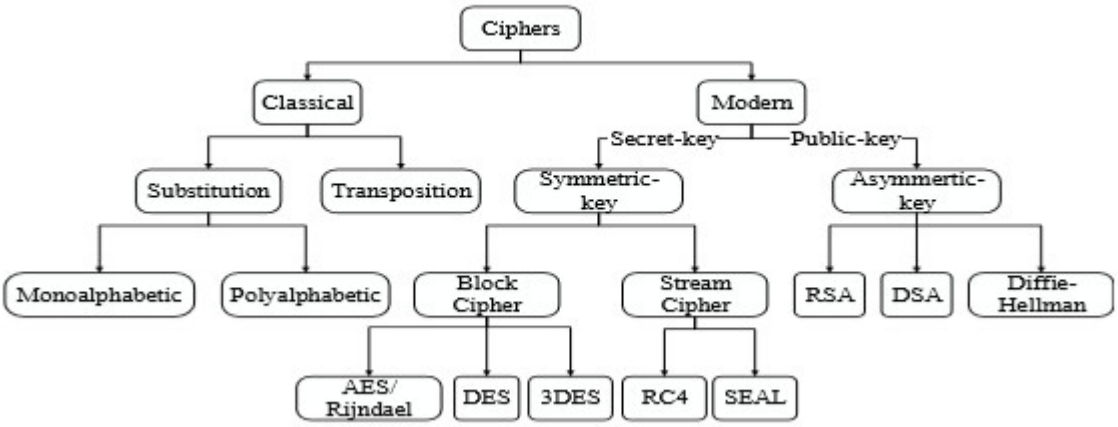

Fig.1: Different Algorithms [8].

There are several ways of classifying cryptographic algorithms. For purposes of this paper, they will be categorized based on the number of keys that are employed for encryption and decryption, and further defined by their application and use. Three types of algorithms that will be discussed here.

- Symmetric Key Cryptography (Secret Key Cryptography)
- Asymmetric Key Cryptography (Public Key Cryptography)
- Hash Function

Symmetric Key Cryptography (Secret Key Cryptography)

- Same Key is used by both parties
- Simpler and Faster

Asymmetric Key Cryptography (Public Key Cryptography **)**

- Two different keys are used Users get the Key from a Certificate Authority**.**
- Authentication in asymmetric cryptography is more secured but the process is relatively more complex as the certificate has to be obtained from certification authority

Modern cryptography concerns itself with the following four objectives:

- Confidentiality (the information cannot be understood by anyone for whom it was unintended)
- Integrity (the information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected)
- Non-repudiation (the creator/sender of the information cannot deny at a later stage his or her intentions in the

creation or transmission of the information)

- Authentication (the sender and receiver can confirm each other's identity and the origin/destination of the information)

Modern cryptography concerns itself with the following four objectives:

- Confidentiality (the information cannot be understood by anyone for whom it was unintended)
- Integrity (the information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected)
- Non-repudiation (the creator/sender of the information cannot deny at a later stage his or her intentions in the creation or transmission of the information)
- Authentication (the sender and receiver can confirm each other's identity and the origin/destination of the information)

Table 1: Comparison between Different Algorithms:

Factors	RSA	DES	3DES	AES
Created By	Ron Rivest, Adi Shamir, and Leonard Adleman In 1978	IBM in 1975	IBM IN 1978	Vincent Rijmen, Joan Daemen in 2001
Key Length	Depends on number of bits in the modulus n where n=p*q	56 bits	168 bits (k1, k2 and k3) 112 bits (k1 and k2)	128, 192, or 256 bits
Round(s)	1	16	48	10 - 128 bit key,12 - 192 bit key,14 - 256 bit key
Block Size	Variable	64 bits	64 bits	128 bits
Cipher Type	Asymmetric Block Cipher	Symmetric Block Cipher	Symmetric Block Cipher	Symmetric Block Cipher
Speed	Slowest	Slow	Very Slow	Fast
Security	Least Secure	Not Secure Enough	Adequate Security	Excellent Security

MAES (Modified Advanced Encryption Standard) Algorithm:

This standard specifies the Rijndael algorithm, a symmetric block cipher that can process data blocks of 128 bits, using cipher keys with lengths of 384, 512, 768 and 1024 bits. Rijndael was designed to handle additional block sizes and key lengths. AES used with the key length of 128,192 and 256 bits. The algorithm may be used with the three different key lengths indicated above, and therefore these different "flavors" may be referred to as "MAES-384", "MAES-512" and "MAES-768" "MAES- 1024". But MAES algorithm can be used with more number of bits.

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

- Substitution bytes
- Shift Rows
- Permutation
- Add Round Key

Substitution Bytes, Shift Rows and AddRoundKey remain unaffected as it is in the AES. Here the important function is Permutation which is used instead of Mix column. These rounds are managed by the IP table. Permutation is widely used in cryptographic algorithms. Permutation operations are

interesting and important from both cryptographic and architectural points of view. The DES algorithm will provide us permutation tables. The inputs to the IP table consist of 128 bits. Modified -AES algorithm takes 128 bits as input. The functions Substitution Bytes and Shift Rows are also interpreted as 128 bits whereas the Permutation function also takes 128 bits. In the permutation table each entry indicates a specific position of a numbered input bit may also consist o f 256 bits in the output. While reading the table from left to right and then from top to bottom, we observe that the 242th bit of the 256-bit block is in first position, second position and so forth. After applying permutation on 128 bits we again complete set of 128 bits and then perform next remaining functions of algorithm. If we take the inverse permutation it gives again the original bits, the output result is a 128-bit cipher text. For the full decryption of Modified-AES algorithm the transformation processes are, Inv-Bytesub, Inv-Shift rows, Inv-Permutation, and the Addroundkey, which are performed in 10 rounds as it is in the encryption process.

Literature Survey

They presented a powerful algorithm for video encryption. Using a modified version of AES, a secure symmetric video encryption system is designed. The modification is done by adjusting ShiftRow Transformation step of AES algorithm. The proposed scheme does not require any additional operations or hardware rather than the original AES. MAES gives better encryption results in terms of security against statistical attacks for videos. Modified AES takes less time to encrypt and decrypt the video than simple AES. By Experimental tests results are given to demonstrate the efficiency of the scheme. Experimental tests include correlation coefficients, entropy and performance with respect to time. The visual inspection of applying the proposed Modified AES is done in both encryption and decryption. The Advanced Encryption Standard is a specification for the encryption of electronic data. It is the modified algorithm of DES (Data Encryption Standard). The Data Encryption Standard is a previously predominant symmetric-key algorithm for the encryption of electronic data. AES algorithm consumes least encryption and decryption time and buffer usage compared to DES algorithm. It was highly influential in the advancement of modern cryptography in the academic world. : In this paper, a high throughput modified Advanced Encryption Standard (AES)-128 bit algorithm is implemented. A new increased parallelism technique is introduced in modified AES architecture in Mix Column round which increases the overall throughput of AES algorithm. This technique is implemented in XC5VLX50T FPGA device Virtex-5. Using this technique throughput is increased 5 % and area is decreased by 30 % when compared to parallel mix column.

Researchers	**Year And Publication**	**Method Used**	**Advantages**	**Disadvantages**
Dhananjay Dumbere' Nitin janwae	2014 IEEE	AES Encryption used	Fast more efficient and robust	May not Robust for high number of bits

Ms. Pooja Deshmukh, Ms.vaishali khole	2014 IEEE	Uses of secure modified AES algorithms	Most secure than AES	High Computational Required
S.Sridevi sathya Priya, P.Karthigai Kumar, N.M. SivaMangai, V.Rejula	2015 IEEE	Parallelism Technique used with MAES Algorithm	More Robust and accurate for maes	It also required more number of bits for computational.
JG pandey, S gurunarayan	2014 IEEE	It Present FPGA and Video encryption for HD video	Easy More Efficient	High Quality Image is required
Z. Alaoui-Ismaili, Moussa, Mourabit K. Amechnoue	2009 IEEE	Optimal processor is used.	More accurate when high level occlusion and low feature dimensions	Not optimal

Table 2: Analysis of different Research paper of Algorithms for Image

Conclusions

According to literature review observe that number of Algorithm method and Technique available for security and encrypting message but still some limitation for security and privacy of data us ing proposed. We observed that modified advanced encryption algorithm is most reliable and accurate from other algorithms.

References

1. Dhananjay M. Dumbere, Nitin j janwae “Video Encryption Using AES Algorithm” 2nd International Conference on Current Trends in Engineering and Technology, ICCTET’14 © IEEE 2014 IEEE Conference Number - 33344 July 8, 2014, Coimbatore, India.

2. Ms. Pooja Deshmukh ,Ms.vaishali khole “Modified AES Based Algorithm for M PEG Video Encryption” ICICES2014 - S.A.Engineering College, Chennai, Tamil Nadu, India. ISBN No.978-1-4799- 3834-6/14/$31.00©2014 IEEE.

3. S.Sridevi sathya Priya,P.Karthigai Kumar, N.M. SivaMangai, V.Rejula "FPGA Implementation of Efficient AES Encryption "IEEE Sponsored 2nd International Conference on Innovations in Information Embedded and Communication Systems ICIIECS'15 978-1-4799-6818-3/ 15/$31.00 © 2015 IEEE

4. JG pandey, S gurunarayan "Architectures and Algorithms for Image and Video Processing using FPGA-based Platform "978-1-4799-4006-6/14/$31.00 ©2014 IEEE.

5. Vakkayil Megha Gopinath "MAES Base Data Encryption and Description Using VHDL" © 2015 IJEDR | Volume 3, Issue 2 | ISSN: 2321-9939.

6. Pravin Kawle, Avinash Hiwase, Gautam Bagde, Ekant Tekam, Rahul Kalbande "Modified Advanced Encryption Standard" ISSN: 2231-2307, Volume-4, Issue-1, March 2014

7. Gurupeet singh and supriya "A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security" International Journal of Computer Applications (0975 – 8887) Volume 67– No.19, April 2013.

8. Shraddha Soni, Himani Agrawal, Dr. (Mrs.) Monisha Sharma "Analysis and Comparison between AES and DES Cryptographic Algorithm" International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 6, December 2012 ISSN: 2277-3754

9. Ranjeet Masram, Vivek Shahare, Jibi Abraham, Rajni Moona "ANALYSIS AND COMPARISON OF SYMMETRIC KEY CRYPTOGRAPHIC ALGORITHMS BASED ON VARIOUS FILE FEATURES" DOI : 10.5121/ijnsa.2014.6404.

10. A.Romeo, G.Romdotti, M.Mattavelli and D.Mlynek."Cryptosystem Architecture for Very High Throughput Multimedia Encryption: The PRK Solution.The 6th IEEE International Conference on Electronic,Circuit and System,September 5-8.Procedding of ICECS 99,Vol .1, 261- 264