Modified AES Based Algorithm for MPEG Video Encryption

Ms. Pooja Deshmukh
PG Student, Department of Computer Engg, D. Y. Patil Engg College, Akurdi, Pune, University of Pune, India
poojadeshmukh121@gmail.com

Ms. Vaishali Kolhe
Department of Computer Engg, Faculty of Technical education, D. Y. Patil Engg College, Akurdi, Pune, University of Pune, India
vlkolhe@gmail.com

*Abstract***—** ***Advances in digital content transmission have increased in the past few years. Security of multimedia data is an imperative issue because of fast evolution of digital data exchanges over an unsecured network. Multimedia data security is achieved by methods of cryptography, which deals with encryption of data. Standard symmetric encryption algorithms provide better security for the multimedia data, but applying symmetric key encryption algorithm on more complex multimedia data, problem of computational overhead might be faced. Over the last few years, several encryption algorithms have applied to secure video transmission. While a large number of multimedia encryption schemes have been proposed in the literature and some have been used in real time applications, cryptanalytic work has shown the existence of security problems and other weaknesses in most of the proposed multimedia encryption schemes. Encryption is a common technique to uphold multimedia security. MPEG video stream is quite different from traditional textual data because interframe dependencies exist in MPEG video. Special MPEG video encryption algorithms are required because of their special characteristics, such as coding structure, large amount of data and real-time constraints. Image and video encryption have applications in various fields including internet communication, multimedia systems, medical imaging, and military communication. The Advanced Encryption Standard (AES) algorithm is used and modified it, to reduce the calculation of the algorithm and for improving the encryption performance.***

Keywords: **AES algorithm, MAES, video encryption and decryption.**

I. Introduction

Encryption is conversion of data from one form into another, called a cipher text that cannot be easily understood by unauthorized people. Whereas Decryption is the process of converting encrypted data back into its original form, so it can be understood. With the continuing development of both computer and Internet technology, multimedia data is being used more and more widely, in applications such as video-on-demand, video conferencing, computer forensics, and broadcasting. Now, multimedia data is also closely related to many aspects such as education, business, entertainment and politics.

The high amount of redundancy gives an attacker extra clues to reconstruct the original video. Normal data, such as program code or text, has much less redundancy in its structure. These redundancy factors present in MPEG video make providing secure MPEG video a challenge. Adding security to MPEG transmission usually involves encrypting some parts of videos (i.e. selective encryption) or the entire MPEG bit stream. The algorithms (DES, IDEA, and AES) involve complex computations. Heavy-weight encryption is performed on almost whole data while lightweight encryption is performed on partial or selective data. In this paper, heavy-weight encryption is used on MPEG video data.

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 acceptable 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.

II. Motivation

It is difficult to use encryption techniques directly in multimedia data. In multimedia data often of high idleness, of large volumes and require real-time interactions. So, there is a need of efficient video encryption algorithm which

ISBN No.978-1-4799-3834-6/14/$31.00©2014 IEEE

can provide better security and performance. Based on the state of the art in video encryption, can observe that:

- For complete and provable security of the video data, the entire video needs to be encrypted. However, a naive encryption of the complete video stream is computationally slow.
- To solve the problem of speed, there is a need of finding solutions to the naive encryption.
- The traditional naive encryption methods use conventional AES algorithm. There is a need of modification in an algorithm to reduce the time required for encryption.
- The encryption algorithm should not be susceptible to attacks like known-plaintext attack and cipher-text-only attack. Computational efficiency should not come at the cost of security.

III. RELATED WORK

There are several existing encryption algorithms based on AES/DES/IDEA for secure MPEG video transmission [6]. Each of them has its strength and weakness in terms of security level, speed and resulting stream size matrices. The existing algorithms are Naive algorithm, selective algorithm, Pure Permutation Algorithm and Video Encryption Algorithm (VEA).

The straight-forward method is to encrypt the entire MPEG stream using standard encryption method such as DES. This is called the Naive algorithm approach. Naive algorithm treats the MPEG bit-stream as the traditional text data and does not make use of the special MPEG structures. This is the most secure algorithm, but it is very slow. The size of the bitstream does not change because many standard encryption algorithms preserve the size [1].

In AES Encryption Technique by [15] showed that the AES encryption algorithm can be used effectively to encrypt MPEG-4. The performance of AES encryption frames is sufficient to display the received Frames on time. The encryptions delay overhead using AES is less than the overhead using RC4 and XOR algorithm. Also, AES can achieve satisfactory encryption results with little overhead.

Video Encryption Algorithm proposed in [10] discusses about the algorithm selectively encrypting a fraction of the whole video. It is faster than encrypting the whole video with AES.

The professors in [3] proposed Modified AES for Image encryption. Arguing that the full content of the video is not critical, selective encryption algorithms were proposed. These methods encrypt a selected portion of the video data using text-based encryption algorithms. This decreases encryption time. For real-time applications, light-weight encryption algorithms were also proposed. These methods encrypt using simple XOR or encrypt selected bits of the video data (sign bits of I frames, motion vectors, etc.). These encryption algorithms are much faster than selective algorithms. (Note that if encryption modifies the syntax of the MPEG bit stream, it adds overhead to the MPEG code.) Another category of algorithms is based on scramble (permutation) only methods, where the DCT coefficients are permuted to provide confusion. However, in most of these methods, computational efficiency comes at the cost of security.

IV. ADVANCED ENCRYPTION STANDARD ALGORITHM (AES)

The AES algorithm is used in some applications that require fast processing such as smart cards, cellular phones and image-video encryption. Rijndael is a block cipher developed by [23]. The Advanced Encryption Standard (AES) algorithm is capable of using cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt data in blocks of 128 bits [3]. The AES algorithm is divided into four different phases, which are executed in a sequential way forming rounds. These blocks operate on the array of bytes organized as 4x4 matrix that is called as state.

- Bytesub transformation: It is a non-linear byte Substitution, using a substation table (sbox), which is constructed by a multiplicative inverse and affine transformation.
- Shift rows transformation: It is a simple byte transposition, the bytes in the last three rows of the state are cyclically shifted; the offset of the left shift varies from one to three bytes.
- Mixcolumns transformation: It is equivalent to a matrix multiplication of columns of the states. Each column vector is multiplied by a set matrix. It should be noted that the bytes are treated as polynomials rather than numbers.
- Addroundkey transformation: It is a simple XOR between the round key and the working state. This transformation is its own inverse.

After an initial addroundkey, a round function is applied to the data block consisting of bytesub, shift rows, mix columns and addroundkey transformation, respectively. It is performed iteratively (N times) depending on the length of the key. The decryption structure has exactly the same sequence of transformations as the one in the encryption structure. The transformations Inv-Bytesub, Inv-Shiftrows, Inv-Mix columns, and Addroundkey allow the form of the key schedules to be identical for encryption and decryption. Based on the above analysis, a simpler design of perceptual encryption for MPEG videos, and attempt to overcome the problems in existing schemes.

V. PROPOSED METHODOLOGY

To overcome the problem of high calculation and computation overhead, analysis of Advanced Encryption Standard (AES) is done and modifies it, to improve the encryption performance and speed. In this paper, a new encryption scheme as a modification of AES algorithm for video encryption is proposed. The modification is mainly focused on ShiftRow Transformations. In the ShiftRow Transformation, the value in the first row and the first column is even, then the first and fourth row is unchanged, and each byte in the second and third row of the state is cyclically shifted right over different number, else the first and third row is unchanged, then each byte of the second and fourth row of the state is cyclically shifted left over different number of bytes. This modification allows for greater security and increased performance [5].

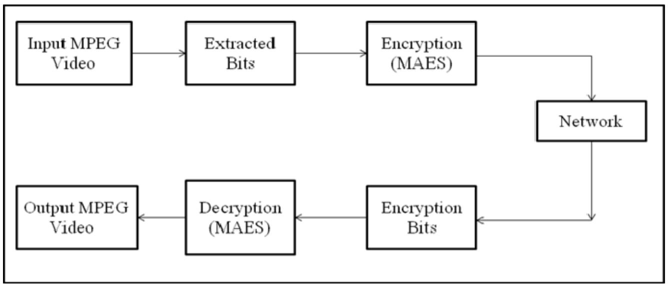

Figure 1: Proposed System Architecture.

Proposed Modified AES based video encryption algorithm contains extraction module i.e., Information Extractor and Encrypted and Decrypted module.

A. Modified AES

[3] modifies the AES to be more efficient and secure way by adjusting the ShiftRow Transformation for image encryption. For encryption of MPEG videos, Modified AES applied in efficient and secure way by adjusting the ShiftRow Transformation.

Steps to modify ShiftRows:

1. Observe the value in the first row and first column of state matrix, (state [0] [0]) is even or odd.

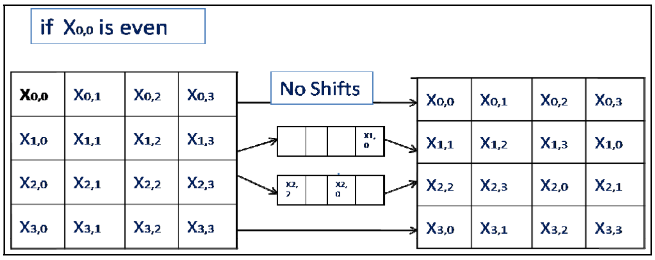

Figure 2: state ([0] [0]) is odd.

2. If that value is odd, The ShiftRows 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. Likewise, the fourth row is shifted by three to the left correspondingly as shown in figure.

3. If it is even, The ShiftRows 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 unchanged, and each byte of the second row is shifted three to the right. Similarly, the third row is shifted by two correspondingly on to the right as shown in figure.

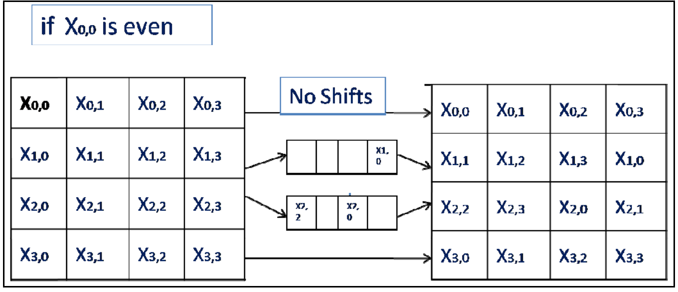

Figure 3: state ([0] [0]) is even.

VI. SIMULATION RESULTS

The results are obtained in three cases of the security analysis:

- Correlation of Two Adjacent Pixels.
- Information analysis.
- Performance of AES and MAES Encryption

A. Correlation of Two Adjacent Pixels:

Test is done on the correlation between two vertically adjacent pixels, and two horizontally adjacent pixels respectively, in a ciphered video frame [17]. First, randomly select n pairs of two adjacent pixels from plain video frame. Then, calculate the correlation coefficient of each pair by using the following formula:

$$\mathrm{cov}(x; y) = E(x - E(x))(y - E(y))$$

$$r_{xy} = \frac{\mathrm{cov}(x; y)}{D(x)\,D(y)} \qquad (1)$$

Where x and y are grey-scale values of two adjacent pixels in the video frame. In arithmetical computations, the following discrete formulas were used:

$$E(x) = \frac{1}{N} \sum_{i=N} x_i$$

$$D(x) = \frac{1}{N} \sum_{i=N} (x_i - E(x))^2; \qquad (2)$$

$$\mathrm{cov}(x; y) = \frac{1}{N} \sum_{i=N} (x_i - E(x))(y_i - E(y)) \qquad (3)$$

Table 1 shows the correlation distribution of two horizontally adjacent pixels in plain video cipher video for the modified cipher. The correlation coefficients are 0.9452 and -0.0112 respectively for both plain video frame and cipher video frame, which are far apart. Similar results for diagonal and vertical directions were obtained as shown in Table 1. It is clear that from the table that there is negligible correlation between the two adjacent pixels in the cipher frame. However, the two adjacent pixels in the plaintext are highly correlated.

Table 1: Correlation Coefficients of Two Adjacent Pixels in Plain & Cipher frame.

	Direction	Horizontal	Vertical	Diagonal
Frame1 Foreman.mpeg	Plain video frame	0.9452	0.9471	0.9127
	Cipher video frame	-0.0112	-0.0813	0.0009
Frame2 Aircrash.mpeg	Plain video frame	0.978	0.981	0.9176
	Cipher video frame	0.0124	0.0832	0.0041
Frame3 Tennis.mpeg	Plain video frame	0.962	0.9831	0.9231
	Cipher video frame	-0.0134	-0.0734	0.0045

B. *Information analysis:*

Information theory is the numerical theory of data communication and storage. Modern information theory is concerned with error-correction, data compression, cryptography, and related topics. To calculate the entropy H (m) of a source m:

$$H(m) = \sum_{i=0}^{(2^N-1)} P(m_i)\ \log_2 \frac{1}{P(m_i)} \text{ bits} \qquad (4)$$

Where $P(m_i)$ indicates the probability of symbol m_i and the entropy is represented in bits. Let us assume that the source emits 28 symbols with equal probability, i.e., $m = m_1\ m_2 \ldots m2^8$ after evaluating Equation (4), result obtain for entropy H(m) = 8, related to a truly random source. Essentially, given that a practical information source hardly ever generates arbitrary messages, in general its entropy value is smaller than the ideal one. Conversely, when the messages are encrypted, their entropy should ideally be 8. If the output of such a cipher releases symbols with entropy less than 8, there exists certain degree of predictability, which threatens its security. Table 2 indicates the various values of the entropies for encrypted videos.

Table 2: Entropy of encrypted Videos

Video	Size	Entropy Value with MAES
Foreman.mpeg	1.26 MB	7.941
Panasonic.mpeg	4.45 MB	7.951
Balcony.mpeg	1.11 MB	7.952
Aircrash.mpeg	675 KB	7.961
Tennis.mpeg	924 KB	7.930
DG_4.mpeg	153 KB	7.9436

C. *Performance of AES and MAES Encryption:*

Table 3 shows Performance of AES Encryption on mpeg video of different sizes.

Table 3: Performance of AES and MAES Encryption and Decryption.

File Name	Size (MB)	AES time(ms)		MAES Time(ms)	
		Encrypt	Decrypt	Encrypt	Decrypt
Foreman. mpeg	1.26 MB	1245	2361	1122	2540
Panasonic.mpeg	4.45 MB	2576	4903	2476	4823
Space. mpeg	1.11 MB	925	2101	917	2011

VII. Conclusion

Through this paper, we 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.

References

[1] Yaobin Mao Huan Jian and Zhiquan Wang. A novel chaos-based video encryption algorithm. 2004.

[2] M. B. Manjunath Shashikant Chaudhari T. R. Ramamohan Jayshri Nehete, K. Bhagyalakshmi. Mpeg video encryption in real-time using secret key cryptography. In Central Research Laboratory Bharat Electronics Ltd., Bangalore, 2011.

[3] Seyed Hossein Kamali, Reza Shakerian, Maysam Hedayati, and Mohsen Rahmani. A new modified version of advanced encryption standard based algorithm for image encryption. International Conference on Electronics and Information Engineering (ICEIE 2010).

[4] T. B. Maples and G. A. Spanos. Performance study of a selective encryption scheme for the security of networked, real-time video.

[5] L. Qiao and K. Nahrstedt. A new algorithm for mpeg video encryption, 1997.

[6] Jolly Shah and Vikas Saxena. Video encryption: A survey. CoRR, abs/1104.0800, 2011.

[7] K. John Singh, Clinton Chee, and R. Manimegalai. Fast random bit encryption technique for video data. European Journal of Scientific Research, 2011.

[8] Daniel Socek. Comparison and analysis of selected video encryption algorithms implemented for mpeg-2 streams, 2004.

[9] Riaz Moghal Gulraiz Akhtar Anil Ahmed Abdul Ghafoor Da Sumira Hameed, Faisal Riaz. Modified advanced encryption standard for text and images. 2011

[10] Varalakshmi.L.M. Dr. Florence Sudha. G. Vijayalakshmi. Light weight video encryption algorithms, 2011.

[11] M. Zeghid, M. Machhout, L. Khriji, A. Baganne, and R. Tourki. A modified aes based algorithm for image encryption. In Proceeding of theWorld Academy of Science, Engineering and Technololgy, May, WASET Organization, USA, pages 206–211, 2007.

[12] Daniel Socek. Comparison and analysis of selected video encryption algorithms implemented for mpeg-2 streams, 2004.

[13] Riaz Moghal Gulraiz Akhtar Anil Ahmed Abdul Ghafoor Da Sumira Hameed, Faisal Riaz. Modified advanced encryption standard for text and images. 2011.

[14] Ben Adida, Susan Hohenberger, and Ronald L. Rivest. Lightweight encryption for email. In Proceedings of the Steps to Reducing Unwanted Traffic on the Internet on Steps to Reducing Unwanted Traffic on the Internet Workshop, SRUTI'05, pages 13– 13, Berkeley, CA, USA, 2005. USENIX Association.

[15] Wail S. Elkilani, Hatem M. Abdul-Kader Faculty of Computers and Information, Minufya University, IEEE 2009, pp 130-134

[16] China drm goldenshield video encryption tool. http://en.china-drm.com/. Accessed: 30/09/2012.

[17] Socek D, Magliveras S, Culibrk D, Marques O, Kalva H, Furt B. Digital video encryption algorithms based on corealation preserving permutations. EURASIP journal on Information Security January 2007;2007(1)

[18] L. Tang. Methods for encrypting and decrypting MPEG video data efficiently. In: proceedings of the ACM International Multimedia Conference, Boston,MA,1996.

[19] S. Li, G. Chen, and X. Zheng, Multimedia Security Handbook, vol. 4 of Internet and Communications Series, ch. Chaos-Based Encryption for Digital Images and Videos, pp. 133{167. CRC Press, December 2004.

[20] A. Uhl and A. Pommer, Image and Video Encryption: From Digital Rights Management to Secured Personal Communication, vol. 15 of Advances in Information Security. Springer, 2005.

[21] P. Hamalainen, T. Alho, M. Hannikainen, and T. D. Hamalainen. Design and implementation of low-area and low-power AES encryption hardware core. In *Digital System Design: Architectures, Methods and Tools, 2006. DSD 2006. 9th EUROMICRO Conference on*, pages 577–583. IEEE, 2006.

[22] B. Furht and D. Socek, "Multimedia Security: Encryption Techniques," *IEC Comprehensive Report on Information Security*, International Engineering Consortium, Chicago, IL, 2003.

[23] Joan Daemen, Vincent Rijmen, "The Design of Rijndael: AES – The Advanced Encryption Standard." Springer, 2002. ISBN 3-540-42580-2.