IEICE TRANS. FUNDAMENTALS, VOL.E91–A, NO.1 JANUARY 2008

PAPER Special Section on Cryptography and Information Security

An Unequal Secure Encryption Scheme for H.264/AVC Video Compression Standard

Yibo FAN[†a)], **Jidong WANG**[†], *Nonmembers*, **Takeshi IKENAGA**[†], **Yukiyasu TSUNOO**[††], *Members*, *and* **Satoshi GOTO**[†], *Fellow*

SUMMARY H.264/AVC is the newest video coding standard. There are many new features in it which can be easily used for video encryption. In this paper, we propose a new scheme to do video encryption for H.264/AVC video compression standard. We define Unequal Secure Encryption (USE) as an approach that applies different encryption schemes (with different security strength) to different parts of compressed video data. This USE scheme includes two parts: *video data classification* and *unequal secure video data encryption*. Firstly, we classify the video data into two partitions: Important data partition and unimportant data partition. Important data partition has small size with high secure protection, while unimportant data partition has large size with low secure protection. Secondly, we use AES as a block cipher to encrypt the important data partition and use LEX as a stream cipher to encrypt the unimportant data partition. AES is the most widely used symmetric cryptography which can ensure high security. LEX is a new stream cipher which is based on AES and its computational cost is much lower than AES. In this way, our scheme can achieve both high security and low computational cost. Besides the USE scheme, we propose a low cost design of hybrid AES/LEX encryption module. Our experimental results show that the computational cost of the USE scheme is low (about 25% of naive encryption at *Level 0* with VEA used). The hardware cost for hybrid AES/LEX module is 4678 Gates and the AES encryption throughput is about 50 Mbps.

key words: *Unequal Secure Encryption, video encryption, selective encryption, H.264/AVC, AES, LEX*

1. Introduction

With the increase of multimedia applications in communication, the data transmission and information security become more and more important. For video, H.264/AVC video compression standard is the newest international video coding standard, which is jointly developed by ITU-T Video Coding Experts Group (VCEG) and the ISO/IEC Moving Picture Experts Group (MPEG). H.264/AVC can provide better peak signal-to-noise ratio (PSNR) and visual quality compared to previous video coding standards [1].

For information security, a common video encryption standard does not exist. To protect the video content, there are three major security technologies: (1) Encryption technology to provide end-to-end security. (2) Watermarking technology to achieve copyright protection. (3) Access control technology to prevent unauthorized access. In this paper, we focus on encryption technology, especially for H.264/AVC video data encryption.

A lot of video encryption methods have been proposed. And most of these methods are designed for previous video coding standards such as MPEG-1, MPEG-2/H.262, MPEG 4 and H.263. According to the existing video encryption technologies, they can be classified into two major encryption types: whole video data encryption and selective video data encryption.

Whole video data encryption method has two different approaches: (a) Video scrambling technology. Permuting the video in the time domain or the frequency domain, it can't provide substantial high security. (b) Cryptography. Encrypting the entire video data using standard cryptography such as DES [22] or AES [23], it is often referred to as "naive approach" and its computational cost is very high.

Most of researches are about selective video data encryption. The basic idea of selective encryption is to encrypt only a portion of the compressed bit-stream. According to the selected video data, these encryption methods can be further classified into three types: frequency domain scheme, spatial domain scheme and entropy coding scheme. Liu and Eskicioglu in [3], Furht, Socek and Eskicioglu in [6] have presented a comprehensive classification which includes most of the presented selective video encryption algorithms. Comprehensive survey studies of the selective video encryption techniques can be found in [2]–[6].

There are three main problems in these selective encryption schemes:

A. Security Problem

A lot of cryptanalysis work has been done in proposed video encryption schemes [5], [7]–[11]. From the view points of these works, the security of schemes which don't use standard cryptographic algorithms is very low. For example, permutation is highly risky shown in [5], [8]–[10]. Even using standard cryptographic algorithms such as DES and AES, many security problems are also existent. For example SCEMPEG scheme [12] and Aegis scheme [13], [14], their cryptanalysis can be found in [5], [7], [11].

B. Computation Problem

Some methods can provide substantial security. However, computational overhead and data overhead become worse. For example, VEA scheme [16] is "*very close to the security of encryption scheme E that is internally used*"

Manuscript received March 22, 2007.
Manuscript revised July 17, 2007.

[†]The authors are with the IPS, Waseda University, Kitakyushu-shi, 808-0135 Japan.
[††]The author is with the Internet Systems Research Laboratories, NEC Corp., Kawasaki-shi, 211-8666 Japan.
a) E-mail: fanyibo@ruri.waseda.jp

DOI: 10.1093/ietfec/e91–a.1.12

Copyright © 2008 The Institute of Electronics, Information and Communication Engineers

[6]. However, it needs to encrypt half of video data using internal encryption scheme E and transfer a large amount of additional keys to receiver.

C. Feasibility Problem

Feasibility is another problem existing in many schemes. A lot of existing schemes are so called "*Integrated video compression and encryption system*." It means that the video encryption module must be integrated into video compression system. For example, permutation of AC, DC coefficients should be done before entropy coding. In this way, the encryption should break the procedure of video compression, and the encryption module must be integrated into video compression system. That is why the standard decoder can't work when applying encrypted video data. The corresponding decoder to this kind of encoder should be "*Integrated video decompression and decryption decoder*." This causes such kind of scheme very hard to be really used in a commercial application.

In this paper, an Unequal Secure Encryption (USE) scheme is proposed for H.264/AVC video coding standard. There are three major targets in the USE scheme: security, feasibility, and low computational cost. In the USE scheme, we encrypt the entire video data using standard cryptography to make our scheme highly secure. We perform all of the encryption operations after entropy coding to separate the video coding system and encryption system. In this way, our USE scheme is feasible in any kind of video security applications. The remaining problem is computational cost. As computational cost of "naive approach" is huge, we need to make some optimization to reduce the computational cost. Here we use two methods: (1) *Data classification*. We classify the total video data into two data partitions, important data partition and unimportant data partition. Many new features in H.264/AVC make this procedure easy to implement. Normally, important data partition has smaller size than unimportant one. (2) *Unequal secure encryption*. We use AES to encrypt important data partition and use LEX [24] to encrypt unimportant data partition. LEX is a stream cipher based on AES. The computational cost of LEX is only 1/2.5 of AES. In this way, we can keep our scheme highly secure with low computational cost. Besides the USE scheme, we also propose a low cost design of hybrid AES/LEX encryption module. This module is a mixed bus width design, it targets low hardware cost with sufficient performance. The architecture of this design is very flexible, and we also proposed other 5 architectures to improve its performance.

This paper is organized as follows. The H.264/AVC video compression standard is introduced in Sect. 2. The AES, LEX and VEA algorithm are introduced in Sect. 3. The proposed Unequal Secure Encryption scheme is introduced in Sect. 4. The hardware design of hybrid AES/LEX encryption module is presented in Sect. 5. The experimental results and analysis are presented in Sect. 6. Finally, conclusion is given in Sect. 7.

2. H.264 Video Compression Standard

H.264/AVC is the newest international video coding standard. It has been approved by ITU-T as Recommendation H.264 and by ISO/IEC as International Standard 14496-10 (MPEG-4 part 10) Advanced Video Coding (AVC).

There are a lot of new techniques used in H.264/AVC, which include new coding techniques, new data structure, new video storage and broadcast techniques. As the USE scheme is applied after video coding, the details of H.264/AVC coding, storage and transmission techniques needn't to be considered very much. The H.264/AVC video data structure has more impact on USE scheme. We need to do data classification by carefully studying the data structure of H.264/AVC.

In H.264/AVC, *profiles* and *levels* specify conformance points. A *profile* defines a set of coding tools or algorithms that can be used in generating a conforming bitstream, whereas a *level* places constraints on certain parameters of the bitstream. The first version of H.264/AVC defines a set of three profiles as shown in Fig. 1.

Some new features which can be used in the USE scheme are listed below:

Coded Data Format: H.264/AVC makes a distinction between a Video Coding Layer (VCL) and Network Abstraction Layer (NAL). The output of the encoding process is VCL data which are mapped to NAL units prior to transmission or storage. A coded video sequence is represented by a sequence of NAL units. The data format of NAL is shown in Fig. 2. One NAL unit contains one or more slices, each slice contains an integral number of macroblocks (MBs). Each MB contains a series of header elements and coded residual data.

Parameter sets: H.264 introduces the concept of parameter sets, which provides for robust and efficient conveyance header information. Parameter sets includes the key information such as sequence header, picture header, this

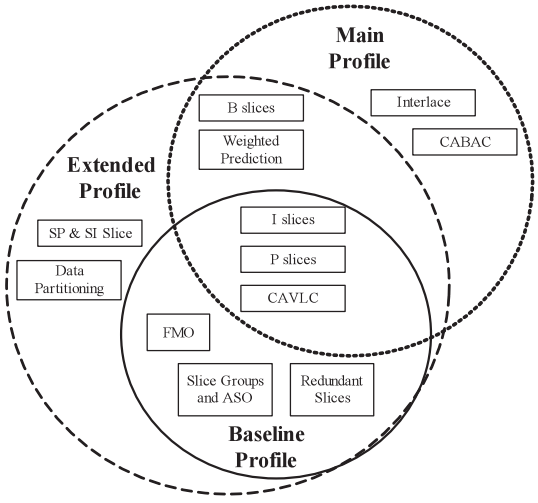


Fig. 1 H.264 baseline, main and extended profiles [20].

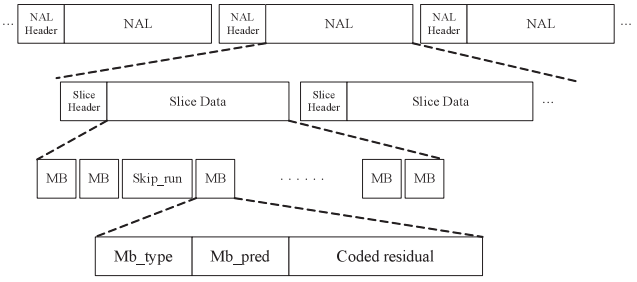


Fig. 2 H.264/AVC data format.

key information is separated for handling in a more flexible and specialized manner in H.264/AVC. This new feature is fully used in our USE scheme.

Flexible macroblock ordering (FMO): FMO is a new technique introduced by H.264/AVC which has ability to partition the picture into regions called slice groups. FMO can be used to enhance robustness to data losses in transmission. In the USE scheme, we provide two kinds of usage of FMO in video encryption scheme.

Data partitioning: As some coded information is more important than others for purpose of representing the video content, H.264/AVC allows syntax of each slice to be separated into three partitions. In the USE scheme, this data partition is used.

3. AES, LEX and VEA Algorithms

3.1 AES Algorithm

Advanced Encryption Standard (AES), also known as Rijndael, is a block cipher adopted as an encryption standard by the U.S. government in 2001. AES is the most popular algorithm used in symmetric key cryptography. AES has a fixed block size of 128 bits and a key size of 128, 192 or 256 bits. AES operates on a 4×4 array of bytes termed the *State*. For encryption, it will implement a round function 10, 12, 14 times (depends on the key length). Each round of AES (except the last round) consists of four stages, shown in Fig. 3:

1) SubBytes: The SubBytes transformation is a non-linear byte substitution that operates on each byte of the *State* using a substitution table.
2) ShiftRows: In the ShiftRows transformation, the bytes in the last three rows of the *State* are cyclically shifted over different numbers of bytes.
3) MixColumns: Mixing operation which operates on the columns of the *State* using a linear transformation.
4) AddRoundKey: A Round Key is added to the *State* by a simple bitwise XOR operation.

Besides round function, AES algorithm also performs a Key Expansion routine to generate a key schedule. More details about AES can be found in [23].

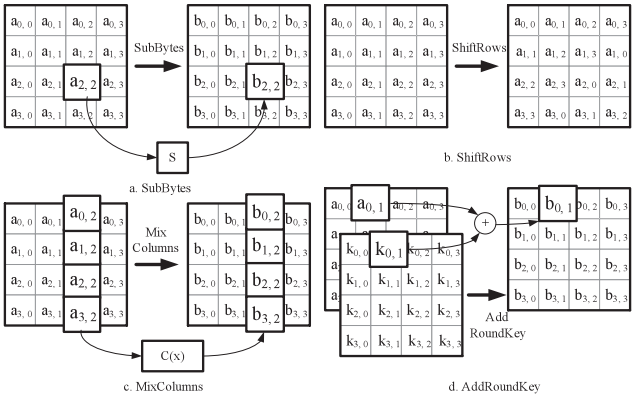


Fig. 3 Operations in AES.

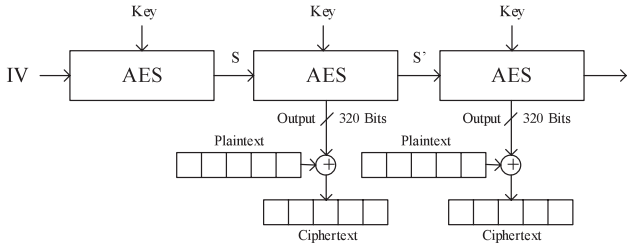


Fig. 4 LEX encryption algorithm.

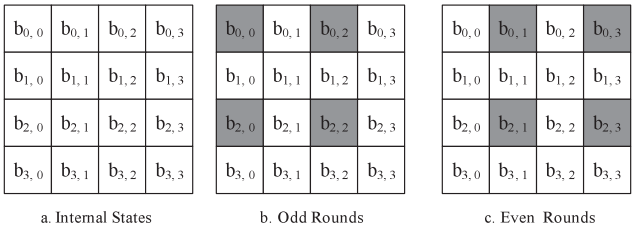


Fig. 5 Leak position in the even and odd rounds.

3.2 LEX Algorithm

LEX is a stream cipher based on the round transformation of AES. It is a candidate algorithm in eSTREAM project which is organized by the EU ECRYPT network. LEX provides the same key agility and short message block performance as AES while handling longer messages faster than AES. In addition, it has the same hardware and software flexibility as AES, and hardware implementations of LEX can share resources with AES implementations.

The LEX algorithm is shown in Fig. 4.

Firstly, the given IV is encrypted by AES invocation: $S=AES_{Key}(IV)$. The 128-bit result S together with encryption Key K constitutes a 256-bit secret state of the stream cipher. Secondly, use result S as a new input data to AES: $S'=AES_{Key}(S)$. The cipher stream will be generated as this process continues. The output of LEX is not S or S′, it comes from internal states of AES. As shown in Fig. 5, 4×4 array of bytes constitutes the internal state of AES. In every round function of AES, a part of AES State is output. In

LEX algorithm, $b_{0,0}$, $b_{0,2}$, $b_{2,0}$, $b_{2,2}$ are output in odd rounds, $b_{0,1}$, $b_{0,3}$, $b_{2,1}$, $b_{2,3}$ are output in even rounds. It totally outputs 40 states of AES (320 bits) in every AES encryption round, and the speed of LEX is exactly 2.5 times faster than AES.

3.3 VEA Algorithm

The Video Encryption Algorithm (VEA) is proposed by Qiao and Nahrstedt [16] in 1997. The basic idea of this algorithm includes three steps:

1). Divide total plaintext into two partitions A and B (with the same size).
2). XOR partition A with partition B bit by bit into a new partition C.
3). Apply the chosen cryptographic algorithm E to encrypt partition A to get the encrypted partition D.

The final ciphertext is partition C and D. VEA algorithm saves computational cost. Only half of video data needs to be encrypted by algorithm E. The security of total plaintext is equal to partition A.

4. Unequal Secure Encryption Scheme

The purpose of designing Unequal Secure Encryption scheme is to provide substantial security with low computational cost for video encryption. As discussed in Sect. 1, a lot of existing video encryption schemes target low computational cost while ignoring security problems, many proposed schemes are so called "*Integrated video compression and encryption system*" which is hard to be really used in a video security system. Some proposed schemes can achieve high security level. However, the computational cost is bad. The target application of the USE scheme is H.264/AVC based video security system.

The USE scheme is shown in Fig. 6. It includes two major steps: The first step is video data classification. The purpose of classification is to divide video data into two partitions: important video data partition and unimportant video data partition. If the data in important partition is lost, the total video content can also be reconstructed just with quality reduction. Therefore, the important video data group needs to be protected more securely than unimportant one. As shown in Fig. 6, after data classification, H.264/AVC video data is parted into DPA (Data Partition A, important) and DPB (Data Partition B, unimportant).

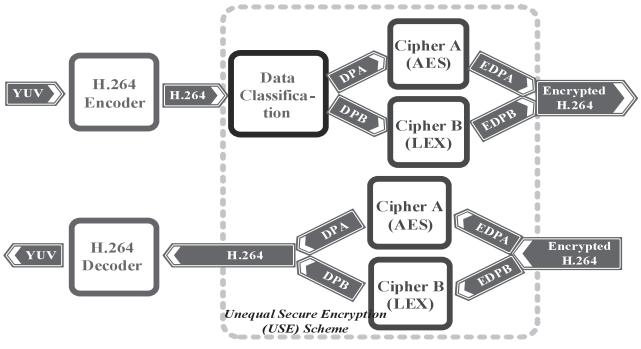


Fig. 6 Unequal secure encryption scheme.

The second step in the USE scheme is unequal secure encryption. Unlike the existing selective encryption scheme, the USE scheme encrypts entire video data, and different cryptographies are selected to encrypt different part of video data. As discussed in Sect. 1, from the view points of cryptanalysis, the best way to keep security is to encrypt the entire video data, and use the standard cryptography to do encryption other than some other methods whose security can not be approved. As shown in Fig. 6, two cryptographies are used in the USE scheme. We choose AES (block cipher) as cipher A, and LEX (stream cipher) as cipher B. As LEX is based on AES, the hardware implementations of AES can also support LEX, and the speed of LEX is faster than AES. Besides AES and LEX, some other cryptographic algorithms also can be used in the USE scheme.

The computational cost for USE scheme depends on data classification and cryptographies. As the cryptographies have been decided, the data classification plays a more important role. There are three data classification methods in the USE scheme. As the USE scheme is designed for H.264/AVC, two of these classification methods use the new features of H.264/AVC.

A. Data classification methods

The purpose of data classification is to partition video data based on importance. There isn't standard definition of importance for video data. Normally, the difficulty to reconstruct the picture caused by data loss is used to evaluate the importance of data. In H.264, Header data (includes parameter sets and MVD) loss causes most difficult to reconstruct the picture. VLC data (includes Intra and Inter residual data) loss causes video quality reduction. Intra data is independent between each frame while Inter data is dependent with neighboring frames, so the reconstruction of Intra loss is much more difficult than Inter loss.

There are three data classification methods in the USE scheme. All of them are performed after video encoding. The video coding scheme and video encryption scheme are totally separated in our USE scheme.

Data Partitioning **(Extended Profile):** This is a new feature in H.264/AVC *Extended Profile*. It can do data partition automatically. As shown in Fig. 7, the coded data that makes up a slice is placed in three separate Data Partitions (A, B and C). Partition A contains the slice header and MB headers. Partition B contains intra coding MB's residual data, Partition C contains inter coding MB's residual data.

FMO **(Baseline Profile, Extended Profile):** FMO is a new feature in H.264/AVC. It has ability to partition the picture into regions called slice groups. In H.264/AVC standard, FMO consists of seven different partition modes. In the USE scheme, we use two modes. As shown in Fig. 8, the

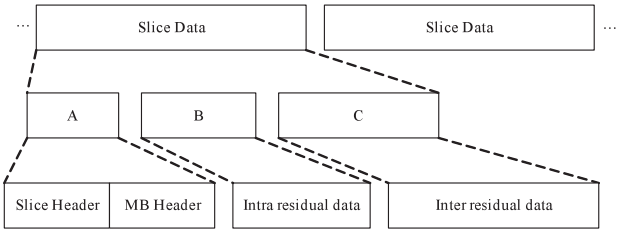


Fig. 7 Slice syntax of H.264/AVC extended profile.

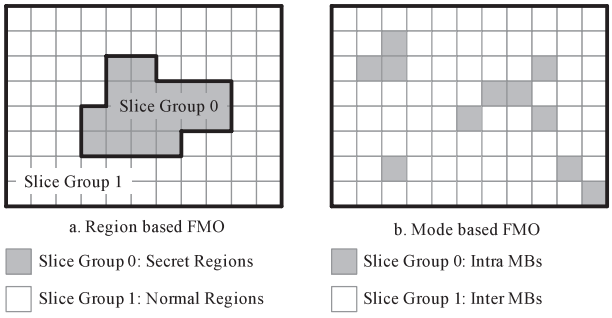


Fig. 8 Data partitioned slices by FMO.

first partition mode is *Region Based FMO*. In this mode, the picture is partitioned into two slice groups: Secret regions and Normal regions. The shape of secret regions can be decided by other pre-processing tools such as object recognition and extraction tools. This mode can support extraction of any interesting shapes in picture, so object based encryption can be realized. The second partition mode is *Mode Based FMO*. In this mode, the picture is partitioned into two slice groups: Intra MBs and Inter MBs.

***Parameters Extraction* (All Profiles):** This method is not intrinsic feature in H.264/AVC. It needs extra computational cost to implement. As *Data Partitioning* method and *FMO* method are profile limited methods, a common method which can be used in any profiles is needed. The *Parameter Extraction* method which is shown in Fig. 9 is such kind of method. The effect of this method is like *Data Partitioning* method. The difference is that *Data Partitioning* method can be automatically done by encoder, and each partition can be placed in a separate NAL unit, and then be transported separately.

B. Security levels

Different cipher has different security level, stream cipher LEX is a light encryption method compared to block cipher AES. However, the computational cost becomes worse if just using AES to do encryption. It is necessary to make a balance between computational cost and security, and this balance can be achieved by security levels definition in the USE scheme.

There are four security levels in the USE scheme. The definitions are listed in Table 1. Different security level selects different data partition to be encrypted by AES and LEX. The security is increased from Level 0 to Level 3, and the corresponding computational cost also increased.

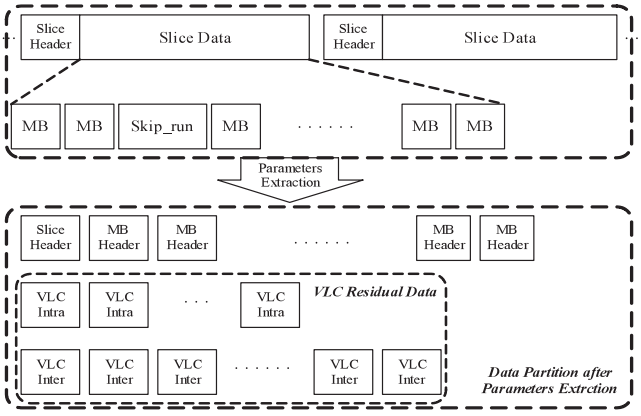


Fig. 9 Data partitioning by parameters extraction.

Table 1 Encryption scheme under different security levels.

Levels	Encryption Methods	Video content under different Data Classification Methods		
		Data Partitioning	FMO	Parameters Extraction
Level 0	AES	A - MVD	-	Hearders - MVD
	LEX	MVD, B, C	-	MVD, VLCs
Level 1	AES	A	-	Headers
	LEX	B, C	-	VLCs
Level 2	AES	A, B	Slice Group 0	Headers, Intra VLCs
	LEX	C	Slice Group 1	Inter VLCs
Level 3	AES	All	All	All

5. Hybrid AES/LEX Encryption Module

As discussed in Sect. 3, LEX is based on AES. The hardware of AES can also support LEX. We can use one hybrid encryption module to support both AES and LEX encryption, and most of the proposed design of AES can be used in the USE scheme.

There are a lot of proposed AES designs, whose performance is from kbps to Gbps. For video encryption, it needn't very high performance because the bit rate of compressed video is not so high, from 64 kbps (Level 1) to 80 Mbps (Level 4) [27]. In this way, area problem should be considered more than speed.

In this paper, we propose a new design of AES/LEX module. The architecture is shown in Fig. 10. It referred Satoh's work in [25], Feldhofer's work in [28] and Canright's work in [26]. However, this architecture is different from all of them. Satoh's design uses 32-bit bus width, and Feldhofer's design uses 8-bit bus width. The implementation results show that the speed of Satoh's design is too high (more than 300 Mbps), and Feldhofer's design is too slow (less than 100 kbps). The hardware cost of Satoh's design is more than Feldhofer's.

The architecture shown in Fig. 10 is a mixed bus width design. As discussed in Sect. 3.1, AES encryption includes four stages: *SubBytes*, *ShiftRows*, *MixColumns* and *Ad-*

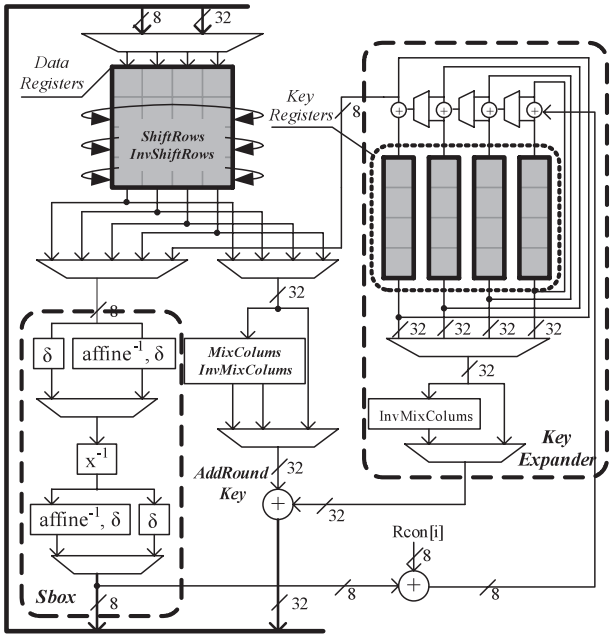


Fig. 10 Data path architecture of AES.

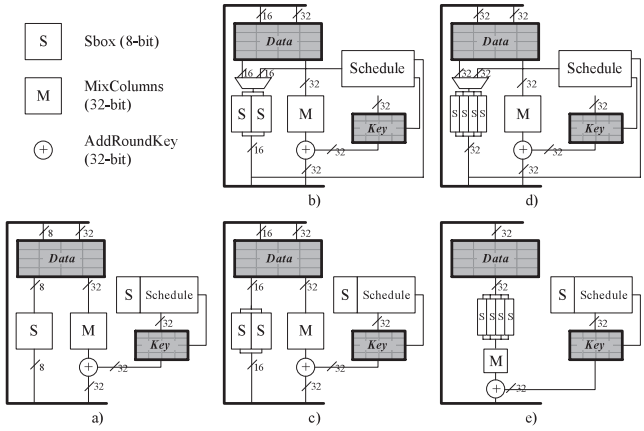


Fig. 11 Other data path architectures for AES.

dRoundKey. For decryption, the corresponding stages are: *InvSubBytes*, *InvShiftRows*, *InvMixColumns* and *AddRoundKey*. The corresponding modules are shown in Fig. 10 (Sbox can support both *SubBytes* and *InvSubBytes*). The key points of this architecture include:

1. One Sbox (8-bit bus width): As Sbox costs more hardware resource than other modules, there is only one Sbox in this architecture and the bus width for Sbox is 8-bit. The Sbox's design is referred from Canright's work which is the most compact design until now. The Satoh's design includes 4 Sboxes, and the lowest speed is more than 300 Mbps which is beyond the requirement for video encryption.

2. 32-bit Mixcolumns: The operation of *MixColumns/ InvMixColumns* is 32-bit, so the most efficient bus width for Mixcolums is 32-bit. Feldhofer proposed an 8-bit solution to do this operation. However, 3 additional 8-bit registers and 28 clock cycles are needed. This result is too bad to be used in video encryption.

3. Parallel architecture in data path: The MixColumns module and Sbox module can execute in parallel. This parallel design can accelerate the speed, and shorten the critical path. Satoh's architecture is a serial design, which can not reduce the number of Sbox from 4 to 1. In this way, our design has much shorter critical path than Satoh's and our design is more flexible than Satoh's. Feldhofer's design also can't support parallel operation and the performance of his design is bad.

There are other 5 data path architectures for our design. Figure 11 shows these 5 data path architectures. All of these architectures have parallel data path same as Fig. 10 (except e). The difference includes:

1. The Number of Sbox: For example, b) has two Sboxes and d) has 4 Sboxes. The different number of Sboxes makes the bus width for Sbox be different. In Fig. 11, b) is 16-bit and d) is 32-bit. When using more Sboxes, it needs less clock cycles to do *SubBytes,* and result in higher speed.

2. The independent Sbox for Key Expander: In Fig. 11, a), c) and e) have an independent Sbox. The effect of this additional Sbox is clock cycles saving.

6. Experimental Results

The experimental results include three parts: data classification evaluation, hybrid AES/LEX encryption module evaluation and the USE scheme evaluation.

A. Data classification evaluation

Table 2 shows the experimental results for several H.264/AVC QCIF sequences. Here we list the header information size (in H.264/AVC, header includes MVD which is corresponding to motion vectors in MPEG or H.263), Intra MBs residue and Inter MBs residue. Here we use 10 QCIF test sequences, 100 frames for each sequence and all of the sequences are beginning with I frame, followed by P or B frames. From these 10 sequences, the average ratios for Header (not include MVD) is about 20%, MVD is about 20%, Intra residue is about 15%, and Inter residue is about 45%.

Table 3 shows the ratios of data partition for different video sequences under different security levels. In level 0, about 20% video data is encrypted by AES and 80% video data is encrypted by LEX. In level 1, the percentage is 40% and 60%, and level 2 is 55% and 45%.

Table 4 shows the comparison of our USE scheme with other's proposals. The comparison is under experimental results listed in Table 2. We use the average ratios from all of the 10 sequences listed in Table 2. The region based FMO is excluded from level 2 of our scheme, because its computation depends on the object recognition and extraction techniques. In H.264/AVC, header includes MVD, and most of the existing schemes don't include motion vectors in their header.

Table 2 Video data partition size (QCIF@100 Frames, I frame followed by P or B frames).

Video Sequence	Header (Includes MVD)				Intra MBs Residue		Inter MBs Residue		Total size of compressed H.264 File (bits)
	Header (bits)	Header/Total (%)	MVD (bits)	MVD/Total (%)	VLC (bits)	VLC/Total (%)	VLC (bits)	VLC/Total (%)	
Canoa	676577	26.04%	300816	11.58%	769777	29.62%	1152357	44.34%	2608088
CarPhone	314675	51.84%	150868	24.85%	55551	9.15%	236802	39.01%	616672
Claire	95326	57.69%	38300	23.18%	10801	6.54%	59111	35.77%	175640
Container	96239	46.49%	32468	15.68%	23877	11.53%	86899	41.98%	217832
Football	825441	30.14%	390128	14.25%	866291	31.64%	1046531	38.22%	2747592
Foreman	375985	55.99%	195606	29.13%	43971	6.55%	251588	37.46%	680648
Grandma	99382	52.85%	39218	20.86%	17903	9.52%	70763	37.63%	198600
Mobile	454322	36.29%	207090	16.54%	54242	4.33%	743504	59.38%	1261768
News	183186	41.21%	86012	19.35%	55332	12.45%	206017	46.34%	454736
Table	312751	39.18%	165196	21.03%	78360	9.98%	394422	50.21%	795512

Table 3 Video data partition for different security levels.

Video Sequence	Level 0		Level 1		Level 2	
	AES	LEX	AES	LEX	AES	LEX
Canoa	14.41%	85.59%	26.04%	73.96%	55.66%	44.34%
CarPhone	26.56%	73.44%	51.84%	48.16%	60.99%	39.01%
Claire	32.47%	67.53%	57.69%	42.31%	64.23%	35.77%
Container	29.28%	70.72%	46.49%	53.51%	58.02%	41.98%
Football	15.84%	84.16%	30.14%	69.86%	61.78%	38.22%
Foreman	26.50%	73.50%	55.99%	44.01%	62.54%	37.46%
Grandma	30.29%	69.71%	52.85%	47.15%	62.37%	37.63%
Mobile	19.59%	80.41%	36.29%	63.71%	40.62%	59.38%
News	21.37%	78.63%	41.21%	58.79%	53.66%	46.34%
Table	18.55%	81.45%	39.18%	60.82%	49.1%	50.84%

Table 4 Comparison with other symmetric cryptography based video encryption schemes (1 @ AES = 2.5 @ LEX).

Encryption Schemes		Content to be encrypted	Computational overhead (@ AES)	Encrypted Data
SEC MPEG [12]	Level 1	Header	20% @ AES	20%
	Level 3	Header and Intra	35% @ AES	35%
	Level 4	All	100% @ AES	100%
Aegis [13,14]		Header, I frame	35% @ AES	35%
VEA by Qiao [16]		Half of video data	50% @ AES	100%
RVEA [17, 18]		Sign Bit of DCT and motion vectors	10% @ AES	10%
Alat -tar [19]	Method 0	Header, Intra and MVD	55% @ AES	55%
	Method 1	Every n^{th} I MB	1/n*15%@AES	1/n*15%
	Method 2	+ Header	+ 40% @ AES	+40%
	Method 3	+ n^{th} Header	+1/n*40%@ AES	+1/n*40%
Ours	**Level 0**	All	50% @ AES	100%
	+VEA		25%@AES	
	Level 1	All	60% @ AES	100%
	+VEA		30% @ AES	
	Level 2 Except FMO	All	70% @ AES	100%
	+VEA		35% @ AES	
	Level 3	All	100% @ AES	100%
	+VEA		50% @ AES	

In Table 4, we compare the computational cost and the encrypted data percentage among all of listed schemes. The computational cost is measured by @AES. We consider that the "naive encryption" using AES is 100%@AES. For example, the computational cost for SECMPEG level 1 is 20%@AES. It means that the computational cost of SECMPEG level 1 is 20% of "naive encryption." In order to further reduce computational cost, we combine VEA algorithm with our scheme and list the results of +VEA in Table 4. From this table, it can be seen that our scheme achieves both high security and low computational cost compared to others' work.

B. Hybrid AES/LEX encryption module evaluation

Table 5 shows the hardware cost and clock cycles for different architectures (Fig. 10 and Fig. 11). The main difference between these architectures is the number of Sbox. Architecture in Fig. 10 uses the least hardware cost (1 Sbox) and needs the most clock cycles (204 cycles) to complete a round of AES encryption. Architecture in Fig. 11.e is same as Satoh's. It only needs 4 clock cycles for each round in AES.

Table 6 shows the synthesis results of the architecture shown in Fig. 10. Here we use TSMC 0.18 μm standard cell library, and use Synopsys Design Compiler to do synthesis. As the speed requirement for video encryption is not very high, we don't try to constraint the design to a high frequency. Instead, we devote more effort to optimize the area cost.

Table 5 Hardware cost and clock cycles for different architectures.

Architecture	Hardware Resource (Sbox)	Clock Cycles	
		Round	AES/LEX
Figure 10	1	20	204
Figure 11.a	2	17	174
Figure 11.b	2	10	104
Figure 11.c	3	9	94
Figure 11.d	4	5	54
Figure 11.e	5	4	44

Table 7 shows the comparison of our design with oth-

Table 6 Hardware Cost @ 80 MHz, TSMC 0.18 μm.

Components	Gates	%
ShiftRows + Data Registers	1386	29.6%
Sbox	358	7.7%
MixColumns/InvMixcolumns	376	8.0%
Key Expander + Key Registers	1935	41.4%
Controller	247	5.3%
Others	376	8.0%
Total	4678	100%

Table 7 Comparison with other's work.

Ref	Tech	Gates	Freq.	Throughput	Cycles/AES
[25]	0.11um	5398	131MHz	311 Mbps	54
[28]	0.35um	3595	100KHz	12.6Kbps	1016
Ours	0.18um	4678	80MHz	50 Mbps	204

Table 8 Max bit-rate and resolution of selected H.264 levels.

H.264 Levels	Max bit rate (bps)				Resolution @ frame rate
	Baseline Main Extend Profile	High Profile	High 10 Profile	High 4:2:2 4:4:4 Profile	
1	64 K	80 K	192 K	256 K	SQCIF@30
1.1	192 K	240 K	576 K	768 K	QCIF@30
2	2 M	2.5 M	6 M	8 M	CIF@30
3	10 M	12.5 M	30 M	40 M	525 SD@30
4	20 M	25 M	60 M	80 M	1080HD@30
4.1	50 M	62.5 M	150 M	200 M	2kx1k@30
4.2	50 M	62.5 M	150 M	200 M	2kx1080@60
5	135 M	168.75 M	405 M	540 M	16VGA@30

Table 9 Max throughput of AES/LEX module.

Security Level	Max Throughput	Security Level	Max Throughput
Level 0	100 Mbps	Level 0 +VEA	200 Mbps
Level 1	83 Mbps	Level 1 +VEA	166 Mbps
Level 2	71 Mbps	Level 2 +VEA	142 Mbps
Level 3	50 Mbps	Level 3 +VEA	100 Mbps

ers.' Our design can save about 13% hardware cost compare to Satoh's design. As the bit rate of most multimedia application is not very high, our design is more attractive than Satoh's. And for some high speed applications, we can use other 5 architectures listed in Fig. 11 to improve the performance.

C. USE Scheme evaluation

Table 8 shows the maximum bit-rate and the resolution of selected levels in H.264 [27]. Table 9 shows the maximum throughput of AES/LEX module under different security levels.

The very high resolution such as 16 VGA is not used currently, and 1080HD is the most popular used now. From these two tables, it can be seen that by using proposed encryption module, our USE scheme can support very high resolution video encryption (up to level 5). It largely improves the throughput of encryption module compared to naive encryption and covers the most frequently used levels in H.264/AVC.

7. Conclusion

In this paper, an unequal secure encryption scheme for H.264/AVC is proposed. In order to maintain high security, our scheme uses "naive approach" to encrypt the entire video data. In order to reduce computational overhead, our scheme uses two methods:
(1) Data classification: There are three classification methods in the USE scheme. After data classification, the entire video data are divided into two partitions: the important data partition and unimportant data partition.
(2) Unequal secure encryption: This method can also be called as selective cryptography method. As different cryptography has different security level and different computational cost. In the USE scheme, we choose AES to encrypt the important data partition and choose LEX to encrypt the unimportant data partition.

Besides the USE scheme, we also proposed the design of hybrid AES/LEX encryption module. As most of the proposed AES designs target either high speed (> 1 Gbps) or low speed/low power (< 100 kbps). Our design targets video encryption whose speed is not so high (64 kbps–80 Mbps).

The experimental results show that our scheme can achieve both high security and low computational cost. The hybrid AES/LEX encryption architecture achieves very low hardware cost and sufficient performance. It also can be easily updated to adapt to a higher speed application.

Acknowledgement

This research is supported by CREST, JST.

References

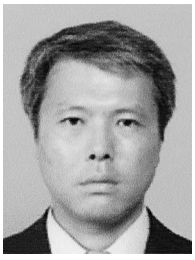
[1] J. Ostermann, J. Bormans, P. List, D. Marpe, M. Narroschke, F. Pereira, T. Stockhammer, and T. Wedi, "Video coding with H.264/AVC: Tools, performance, and complexity," IEEE Circuits Syst. Mag., vol.4, no.1, pp.7–28, First Quarter, 2004.
[2] B. Furht and D. Socek, "Multimedia security: Encryption techniques," IEC Comprehensive Report on Information Security, International Engineering Consortium, pp.335–349, Chicago, IL, 2004.
[3] X. Liu and A.M. Eskicioglu, "Selective encryption of multimedia content in distribution networks: Challenges and new directions," IASTED International Conference on Communications, Internet and Information Technology (CIIT 2003), pp.527–533, Scottsdale, AZ, Nov. 2003.
[4] T. Lookabaugh, D.C. Sicker, D.M. Keaton, W.Y. Guo, and I. Vedula, "Security analysis of selectively encrypted MPEG-2 streams," Multimedia Systems and Applications VI Conference, pp.10–21, Orlando, FL, Sept. 2003.
[5] L. Qiao and K. Nahrstedt, "Comparison of MPEG encryption algorithms," International Journal on Computer and Graphics, vol.22, no.3, pp.437–448, 1998.
[6] B. Furht, D. Socek, and A.M. Eskicioglu, "Fundamentals of multimedia encryption techniques," in Multimedia Security Handbook, Ch. 3, pp.93–131, CRC Press, LLC, Dec. 2004.
[7] I. Agi and L. Gong, "An empirical study of secure MPEG video

transmission," Proc. Symposium on Network and Distributed Systems Security, pp.137–144, IEEE, 1996.
[8] L. Qiao, K. Nahrstedt, and I. Tam, "Is MPEG encryption by using random list instead of zigzag order secure?," IEEE International Symposium on Consumer Electronics, pp.226–229, Singapore, Dec. 1997.
[9] B. Bhargava, C. Shi, and Y. Wang, "MEPG video encryption algorithms," Aug. 2002, available at http://raidlab.cs.purdue.edu/papers/mm.ps
[10] T. Seidel, D. Socek, and M. Sramka, "Cryptanalysis of video encryption algorithms," Proc. 3rd Central European Conference on Cryptology TATRACRYPT 2003, pp.79–87, Bratislava, Slovak Republic, 2004.
[11] A. Alattar and G. Al-Regib, "Evaluation of selective encryption techniques for secure transmission of MPEG video bit-streams," Proc. IEEE International Symposium on Circuits and Systems, vol.4, pp.IV-340–IV-343, 1999.
[12] J. Meyer and F. Gadegast, "Security mechanisms for multimedia data with the example MPEG-1 video," Project Description of SECMPEG, Technical University of Berlin, Germany, May 1995.
[13] T.B. Maples and G.A. Spanos, "Performance study of selective encryption scheme for the security of networked real-time video," Proc. 4th International Conference on Computer and Communications, pp.2–10, Las Vegas, NV, 1995.
[14] G.A. Spanos and T.B. Maples, "Security for real-time MPEG compressed video in distributed multimedia applications," Conference on Computers and Communications, pp.72–78, 1996.
[15] L. Tang, "Methods for encrypting and decrypting MPEG video data efficiently," Proc. 4th ACM International Multimedia Conference, pp.219–230, Boston, MA, Nov. 1996.
[16] L. Qiao and K. Nahrstedt, "A new algorithm for MPEG video encryption," Proc. 1st International Conference on Imaging Science, Systems and Technology (CISST'97), pp.21–29, Las Vegas, NV, July 1997.
[17] C. Shi and B. Bhargava, "A fast MPEG video encryption algorithm," Proc. 6th International Multimedia Conference, pp.81–88, Bristol, UK, Sept. 1998.
[18] C. Shi, S.-Y. Wang, and B. Bhargava, "MPEG video encryption in real-time using secret key cryptography," 1999 International Conference on Parallel and Distributed Processing Techniques and Applications (PDPTA'99), pp.2822–2828, Las Vegas, NV, June/July 1999.
[19] A.M. Alattar, G.I. Al-Regib, and S.A. Al-Semari, "Improved selective encryption techniques for secure transmission of MPEG video bit-streams," Proc. 1999 International Conference on Image Processing (ICIP'99), vol.4, pp.256–260, Kobe, Japan, Oct. 1999.
[20] I.E.G. Richardson, H.264 and MPEG-4 Video Compression, Video coding for next-generation multimedia, pp.159–223, John Wiley & Sons, 2003.
[21] T. Wiegand, G.J. Sullivan, G. Bjntegaard, and A. Luthra, "Overview of the H.264/AVC video coding standard," IEEE Trans. Circuits Syst. Video Technol., vol.13, no.7, pp.560–576, July 2003.
[22] National Institute of Standards and Technology (U.S.). Data Encryption Standard (DES). FIPS Publication 46-3, NIST, 1999.
[23] National Institute of Standards and Technology (U.S.). Advanced Encryption Standards (AES). FIPS Publication 197, 2001.
[24] A. Biryukov, "A new 128-bit stream cipher LEX," ECRYPT Stream Cipher Project Report, 2005, Available at http://www.ecrypt.eu.org/stream/lex.html
[25] A. Satoh, S. Morioka, K. Takano, and S. Munetoh, "A compact Rijndael hardware architecture with S-Box optimization," Advances in Cryptology — ASIACRYPT 2001, 7th International Conference on the Theory and Application of Cryptology and Information Security, pp.239–254, Gold Coast, Australia, Dec. 2001.
[26] D. Canright, "A very compact S-Box for AES," Cryptographic Hardware and Embedded Systems — CHES, pp.441–455, Sept. 2005.
[27] Wikipedia, "H.264/MPEG-4 AVC," available at http://en.wikipedia.org/wiki/H.264/MPEG-4_AVC
[28] M. Feldhofer, S. Dominikus, and J. Wolkerstorfer, "Strong authentication for RFID systems using the AES algorithm," Cryptographic Hardware and Embedded Systems — CHES 2004, vol.3156, pp.357–370, 2004.

Yibo Fan received the B.E. degree in electronic engineering from Zhejiang University, China in 2003 and M.S. degree in Microelectronics from Fudan University, China in 2006. Currently, he is a Ph.D. candidate in Graduate School of Information, Production and Systems, Waseda University, Japan. His research interests include information security, video coding and associated VLSI architecture.

Jidong Wang received the B.E. degree in communication engineering from Xi'an Institute of Post & Telecommunica-tions, Xi'an, China, in 2004. Currently, he is working towards the M.S. degree in Graduate School of Information, Production and Systems, Waseda University, Japan. His research interests include H.264 video encryption algorithms and associated VLSI implementation.

Takeshi Ikenaga received the B.E. and M.E. degrees in electrical en- gineering and the Ph.D. degree in information & computer science from Waseda University, Tokyo, Japan, in 1988, 1990, and 2002, respectively. He joined LSI Laboratories, Nippon Telegraph and Telephone Corporation (NTT) in 1990, where he has been undertaking research on the design and test methodologies for high-performance ASICs, a real-time MPEG2 encoder chip set, and a highly parallel LSI & System design for image-understanding processing. He is presently an associate professor in the system LSI field of the Graduate School of Information, Production and Systems, Waseda University. His current interests are application SOC for image, security and network processing. Dr. Ikenaga is a member of the IPSJ and the IEEE. He received the IEICE Research Encouragement Award in 1992.



Yukiyasu Tsunoo received his B.E. degree from Waseda University in 1982, M.S. degree from JAIST, and Dr.Eng. from Chuo University. He joined NEC Software Hokuriku, Ltd. in 1985. He is now a Research Fellow of NEC Internet Systems Research Laboratories. He is engaged in the design of common key ciphers and the study of evaluation techniques. Dr. Tsunoo is a member of the Expert Commission of Information Security Research, The Institute of Electronics, Information and Communication Engineers, the Information Processing Society of Japan, the Japan Society for Security Management and the Atomic Energy Society of Japan.

Satoshi Goto was born on January 3rd, 1945 in Hiroshima, Japan. He received the B.E. and M.E. degrees in Electronics and Communication Engineering from Waseda University in 1968 and 1970, respectively. He also received the Dr. of Engineering from the same university in 1981. He is IEEE fellow, member of Academy Engineering Society of Japan and professor of Waseda University. His research interests include LSI system and Multimedia System.