A New Video Encryption Scheme for H.264/AVC

Yibo Fan[1], Jidong Wang[1], Takeshi Ikenaga[1],
Yukiyasu Tsunoo[2], and Satoshi Goto[1]

[1] Graduate School of Information, Production and Systems, Waseda University
2-7 Hibikino, Wakamatsu, Kitakyushu, Fukuoka, 808-0135, Japan
[2] Internet Systems Research Laboratories, NEC Corp.
Kawasaki, Kanagawa 211-8666, Japan
fanyibo@ruri.waseda.jp, wangjidong@fuji.waseda.jp,
ikenaga@waseda.jp,
tsunoo@bl.jp.nec.com, goto@waseda.jp

Abstract. With the increase of video applications, the security of video data becomes more and more important. In this paper, we propose a new video encryption scheme for H.264/AVC video coding standard. We define Unequal Secure Encryption (USE) as an approach that applies different cryptographic algorithms (with different security strength) to different partitions of video data. The USE scheme includes two parts: video data classification and unequal secure video data encryption. For data classification, we propose 3 data classification methods and define 5 security levels in our scheme. For encryption, we propose a new stream cipher algorithm FLEX and XOR method to reduce computational cost. In this way, our scheme can achieve both high security and low computational cost. The experimental results show that the computational cost of the USE scheme is very low. In security level 0, the computational cost is about 18% of naive encryption. The USE scheme is very suitable for high security and low cost video encryption systems.

Keywords: Video, Encryption, H.264/AVC.

1 Introduction

With the increase of multimedia applications in communication, the data transmission and information security become more and more important. For video data compression, there are several important standards such as MPEG-1, MPEG-2/H.262, MPEG-4 and H.264/AVC. 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) [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 when distributing video over internet or other public communication channel. (2) Watermarking technology to achieve copyright protection, ownership trace, and authentication. (3) Access control

H.H.S. Ip et al. (Eds.): PCM 2007, LNCS 4810, pp. 246–255, 2007.

technology to prevent unauthorized access. In this paper, we focus on video data encryption technology, especially for H.264/AVC video data encryption.

Most of existing video encryption schemes is designed for previous video coding standards, and there are few video encryption schemes designed for H.264/AVC. According to these video encryption schemes, they can be classified into two major encryption types: whole video data encryption and selective video data encryption. The whole video data encryption method has two different approaches: (a) Video scrambling technology. Permuting the video in the time domain or the frequency domain, however, the security is low. (b) Encryption. Encrypting the entire video data using standard cryptographic algorithms, it is often referred to as "naive approach". This method can provide substantial high security. However, it needs huge computational cost.

Most of researches are about selective video data encryption, which can reduce computational cost as it just encrypts only a part of video data. However, the security becomes problem in many proposed schemes. Some schemes only achieved moderate to low security and only few of the proposed methods achieved substantial security.

In this paper, an Unequal Secure Encryption (USE) scheme is proposed for video secure systems. There are three major targets in the USE scheme: security, feasibility, and low computational cost. In the USE scheme, we encrypt the total video data using standard cryptographic algorithms to make our scheme highly secure. In order to make the USE scheme can be used in most of the video security systems, we perform all of the encryption operations after entropy coding. In this way, the video coding system and the video encryption system can be separated with each other. 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 [13] to encrypt important data partition and proposed FLEX algorithm to encrypt unimportant data partition. The computational cost of FLEX is only 1/5 of AES. In this way, we can keep our scheme highly secure with low computational cost.

The rest of this paper is organized as follows. The existing video encryption schemes are discussed in Section 2. The USE scheme is proposed in Section 3. Our experimental results are presented in Section 4. Finally, the conclusion is given in Section 5.

2 Video Encryption Methods

The most secure way of protecting video data is naive algorithm, which encrypts the entire video data by standard cryptosystem. However, larger computational overhead makes it inefficient or impossible in lots of applications. As a result, selective encryption becomes popular in most of the video encryption researches.

Liu and Eskicioglu in [3], Furht, Socek and Eskicioglu in [6] have presented a comprehensive classification include most of the presented selective video encryption algorithms. According to their work, these encryption schemes can be further

classified into three types: frequency domain schemes, spatial domain schemes and entropy coding schemes. Frequency domain scheme selects frequency domain data in video such as motion vector, DCT coefficients, I blocks, I frames and so on. Most of the selective encryption methods are based on frequency domain. Spatial domain schemes make use of spatial information in video data. Entropy coding schemes use special entropy codec to do encryption.

There are three main problems in these 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 researches, 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 or AES in video encryption scheme, there are also many security problems existing. The corresponding cryptanalysis can be found in [5, 7, 11].

B. Computational Cost Problem

Some methods can provide substantial security. However, computational overhead and data overhead become worse. For example, VEA scheme [12] is *"very close to the security of encryption scheme E that is internally used"* [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 existed 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 decoding encrypted video data. The corresponding decoder to this secure encoder should be *"Integrated video decompression and decryption decoder"*. This causes such kind of scheme very hard to be widely used in commercial applications.

3 Unequal Secure Encryption (USE) Scheme

3.1 USE Scheme Introduction

The purpose of designing Unequal Secure Encryption scheme is to provide substantial security with low computational cost for video encryption. As discussed in Section 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 widely used in video security systems. Some proposed schemes can achieve high security level. However, the computational cost is bad.

Figure 1 shows the idea of the USE scheme.

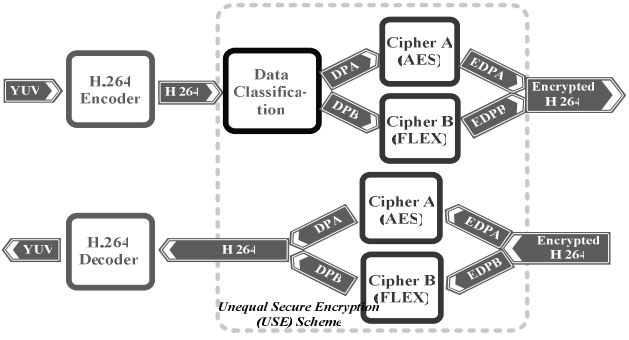

Fig. 1. Unequal Secure Encryption scheme

The USE scheme 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. The importance is evaluated by how difficult to reconstruct a picture. As shown in Figure 1, after data classification, H.264/AVC video data is parted into DPA (Data Partition A, important) and DPB (Data Partition B, unimportant).

The second step in the USE scheme is unequal secure encryption. Unlike the existing selective encryption scheme, the USE scheme encrypts total video data, and different cryptographic algorithms are selected to encrypt different part of video data. As discussed in Section 1, from the view points of cryptanalysis, the best way to keep security is to encrypt the total video data by standard cryptographic algorithms, other than some other methods whose security can not be approved. As shown in Figure 1, two algorithms are used in the USE scheme. DPA is encrypted by cipher A, and DPB is encrypted by cipher B. Different algorithm has different security level and computational cost. In the USE scheme, we use AES as cipher A, and FLEX as cipher B. FLEX is based on AES, the hardware implementations of AES can also support FLEX, and the speed of FLEX is faster than AES. Besides AES and FLEX, some other *cryptographic* algorithms also can be used in the USE scheme.

The computational cost for USE *scheme* depends on data classification and cryptographic algorithms.

3.2 Data Classification Methods

There are many data classification methods in the USE scheme. As the USE scheme is designed for H.264/AVC, some new features in H.264/AVC can be used in data classification.

Data Partitioning (Extended Profile): This is a new feature in H.264/AVC *Extended Profile*, which can do data partition automatically. As shown in Figure 2, 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 header data *for* MBs. Partition B contains

intra coding MBs' residual data, Partition C contains inter coding MBs' residual data. Obviously, the information in Partition A is more important than B and C. Normally, intra data (Partition B) is considered more important than inter data (Partition C).

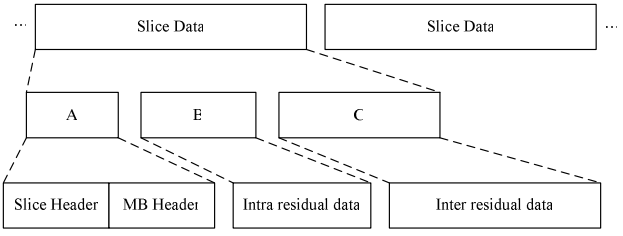

Fig. 2. Slice syntax of H.264/AVC Extended Profile

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 types. All of these types make it easy to partition pictures. In the USE scheme, there are two kinds of partition modes (shown in Figure 3). The 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. 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. As Intra MBs is more important than Inter MBs to reconstruct picture, the Intra MBs should use highly secure encryption algorithms.

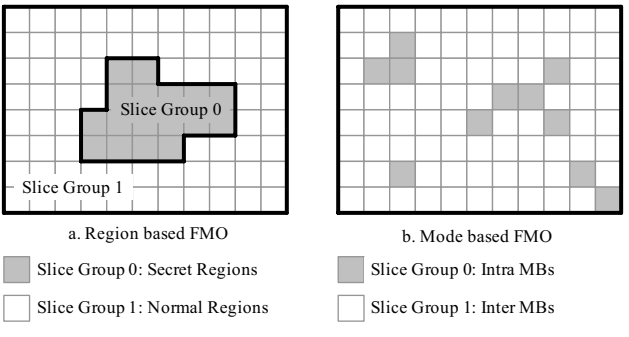

Fig. 3. Data Partitioned Slices by FMO

Parameters Extraction (All Profiles): Since *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 Figure 4 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 codec.

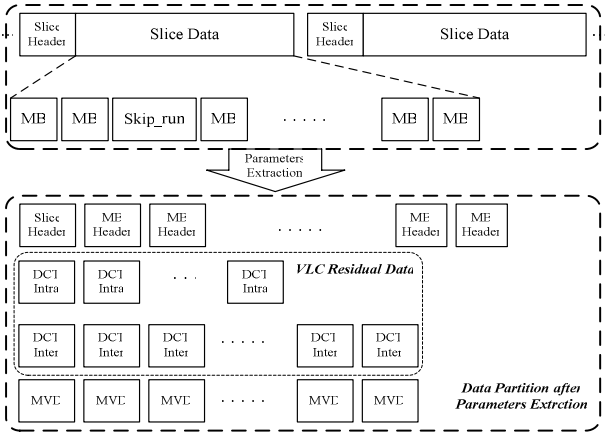

Fig. 4. Data Partitioning by Parameters Extraction

3.3 Security Levels

There are 5 security levels in the USE scheme (Shown in Table 1). The definitions are listed as following:

Level 0: Headers are encrypted by AES, and the remained data are encrypted by FLEX. In level 0, the computational cost is the lowest. The *Parameters Extraction* method can be used in this level.

Level 1: Headers and MVDs (in H.264/AVC, MVD corresponds to motion vector) are encrypted by AES, and the remained data are encrypted by FLEX. The *Data Partitioning* method and *Parameters Extraction* method can be used in this level.

Level 2: Headers, MVD and Intra MBs are encrypted by AES, and Inter MBs are encrypted by FLEX. All of three data classification methods can be used in this level.

Level 3: The entire video is encrypted by AES. Level 3 has the highest computational cost and security.

Level x: This is an extra security levels for the USE scheme. Only FMO methods can be used in this level. It can be used in object-based encryption applications.

3.4 Encryption Methods

A. FLEX Algorithm

FLEX (which stands for Fast Leak EXtraction) is a stream cipher algorithm based on the round transformation of AES. FLEX 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 FLEX can share resources with AES implementations. The FLEX algorithm is shown in Figure 5.

Table 1. Security levels in the USE scheme

Secure Levels	Algorithm	Video content	Data Classification Methods
Level 0	AES	Headers	Parameters Extraction
	FLEX	Inter, Intra, MVD	
Level 1	AES	Headers, MVD	Data Partitioning Parameters Extraction
	FLEX	Inter, Intra	
Level 2	AES	Headers, MVD, Intra	Data Partitioning Parameters Extraction FMO
	FLEX	Inter	
Level 3	AES	All	-
Level x	AES	Secret Region	FMO
	FLEX	Normal Region	

Firstly, the given IV is encrypted by AES invocation: $S=AES_{Key}(IV)$. The 128-bit result S together with encryption Key constitutes a 256-bit secret state of the stream cipher. Secondly, we 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 FLEX is not S or S', it comes from internal states of AES. As shown in Figure 6, 4×4 array of bytes constitutes the internal state of AES. In every round function of AES, a part of AES *States* is output. In FLEX algorithm, $b_{0,0}$, $b_{0,2}$, $b_{1,1}$, $b_{1,3}$, $b_{2,0}$, $b_{2,2}$, $b_{3,1}$, $b_{3,3}$ are output in odd rounds, $b_{0,1}$, $b_{0,3}$, $b_{1,1}$, $b_{1,3}$, $b_{2,1}$, $b_{2,3}$, $b_{3,1}$, $b_{3,3}$ are output in even rounds. It totally outputs 80 *States* of AES (640 bits) in every AES encryption round. The speed of FLEX is exactly 5 times faster than AES.

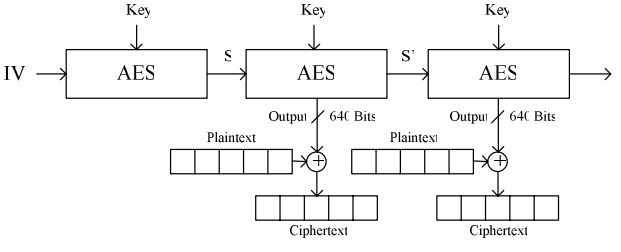

Fig. 5. FLEX encryption algorithm

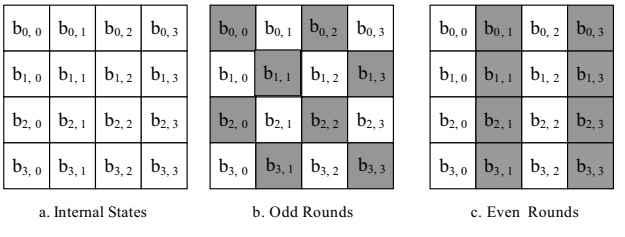

Fig. 6. Leak position in the even and odd rounds

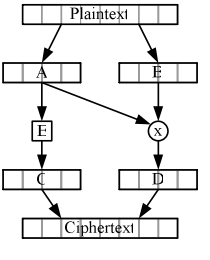

Fig. 7. XOR Method

B. XOR Method

In order to further reduce computational cost, we use XOR method to reduce 50% of computational cost. This method is shown in Figure 7. There are three steps of this method:

Step 1: Divide total plaintext into two partitions A and B (with the same size),
Step 2: Encrypt partition A while XOR partition A with partition B bits by bits,
Step 3: Partition C and D are ciphertext.

By using XOR method, we can just encrypt half of video data to achieve low computational cost. The security of total plaintext is equal to partition A.

6 Experimental Results

Table 2 shows the experimental results for several H.264/AVC QCIF sequences. It lists the header information size, MVD size, Intra MBs residue size and Inter MBs residue size in 10 QCIF test sequences. In every test sequence, it begin with I frame, followed by P or B frames. Totally 100 frames are included in each test sequence.

From these 10 sequences, the average ratios of data size for Header is about 20%, MVD is about 20%, Intra residue is about 15%, and Inter residue is about 45%.

Table 3 shows the computational cost and encrypted data percentage comparison of our USE scheme with other's proposals. The comparison is under the experimental results listed in table 2. We use the average percentage of 10 sequences. The computational cost is measured by n@AES. We consider that the "naive encryption" by 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". The encrypted data percentage reflects the security strength of

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

Video Sequence	Header		MVD		Intra MBs Residue		Inter MBs Residue		Total size (bits)
	Header (bits)	Header/Total (bits)	MVD (bits)	MVD/Total (%)	Intra (bits)	Intra/Total (%)	Inter (bits)	Inter/Total (%)	
Canoa	375761	14.41%	300816	11.58%	769777	29.62%	1152357	44.34%	2608088
CarPhone	163807	26.56%	150868	24.85%	55551	9.15%	236802	39.01%	616672
Claire	57026	32.47%	38300	23.18%	10801	6.54%	59111	35.77%	175640
Container	63771	29.28%	32468	15.68%	23877	11.53%	86899	41.98%	217832
Football	435313	15.84%	390128	14.25%	866291	31.64%	1046531	38.22%	2747592
Foreman	180379	26.50%	195606	29.13%	43971	6.55%	251588	37.46%	680648
Grandma	60164	30.29%	39218	20.86%	17903	9.52%	70763	37.63%	198600
Mobile	247232	19.59%	207090	16.54%	54242	4.33%	743504	59.38%	1261768
News	97174	21.37%	86012	19.35%	55332	12.45%	206017	46.34%	454736
Table	147555	18.55%	165196	21.03%	78360	9.98%	394422	50.21%	795512

Table 3. Comparison with other symmetric cryptographic algorithms based video encryption schemes

Encryption Schemes		Content to be encrypted	Computational overhead (@ AES)	Encrypted Data
SEC MPEG [15]	Level 1	Header	20% @ AES	20%
	Level 3	Header and Intra	35% @ AES	35%
	Level 4	All	100% @ AES	100%
Aegis [16,17]		Header, I frame	35% @ AES	35%
VEA [12]		All	50% @ AES	100%
RVEA [18, 19]		Sign Bit of DCT and motion vectors	10% @ AES	10%
Alattar [20]	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	(1/n*15 + 40)% @ AES	(1/n*15 + 40)%
	Method 3	+ n^{th} Header	(1/n*15 +1/n*40)%@ AES	(1/n*15 +1/n*40)%
Ours	Level 0	All	18% @ AES	100%
	Level 1	All	26% @ AES	100%
	Level 2	All	32% @ AES	100%
	Level 3	All	50% @ AES	100%

each video encryption schemes. As all of the schemes use AES to encrypt the selected important data, the security can be evaluated by the amount of encrypted data.

From table 3, it can be seen that our scheme can achieve both high security and low computational cost compared to others' work. For example, the computational cost of Level 0 in our USE scheme is just about 18% of naive encryption, and the encrypted data percentage is 100%.

7 Conclusion

In this paper, an unequal secure encryption scheme for H.264/AVC is proposed. This scheme mainly includes two parts: *Data classification* and *Unequal secure encryption*. Some new ideas are proposed in this scheme, such as Data classification methods, FLEX algorithm, XOR method and so on. The experimental results show that our scheme can achieve both high security and low computational cost. It is very suitable to be used in low power and high security video encryption systems.

Acknowledgement

This research is supported by CREST, JST.

References

1. Ostermann, J., Bormans, J., List, P., Marpe, D., Narroschke, M., Pereira, F., Stockhammer, T., Wedi, T.: Video coding with H.264/AVC: tools, performance, and complexity. IEEE Circuits and Systems Magazine 4(1), 7–28 (2004)
2. Furht, B., Socek, D.: Multimedia Security: Encryption Techniques, IEC Comprehensive Report on Information Security, International Engineering Consortium, Chicago, IL (2003)
3. Liu, X., Eskicioglu, A.M.: Selective Encryption of Multimedia Content in Distribution Networks: Challenges and New Directions. In: CIIT 2003. IASTED International Conference on Communications, Internet and Information Technology, Scottsdale, AZ, (November 17-19, 2003) pp. 17–19 (2003)

4. Lookabaugh, T., Sicker, D.C., Keaton, D.M., Guo, W.Y., Vedula, I.: Security Analysis of Selectively Encrypted MPEG-2 Streams. In: Multimedia Systems and Applications VI Conference, Orlando, FL (September 7-11, 2003)
5. Qiao, L., Nahrstedt, K.: Comparison of MPEG Encryption Algorithms, International Journal on Computer and Graphics. Special Issue on Data Security in Image Communication and Network 22(3) (1998)
6. Furht, B., Socek, D., Eskicioglu, A.M.: Fundamentals of multimedia encryption techniques. In: Multimedia Security Handbook, ch. 3, pp. 93–131. CRC Press, Boca Raton (2004)
7. Agi, I., Gong, L.: An Empirical Study of Secure MPEG Video Transmission. In: Proceedings of the Symposium on Network and Distributed Systems Security, IEEE, Los Alamitos (1996)
8. Qiao, L., Nahrstedt, K., Tam, I.: Is MPEG Encryption by Using Random List Instead of Zigzag Order Secure? In: IEEE International Symposium on Consumer Electronics, Singapore (December 1997)
9. Bhargava, B., Shi, C., Wang, Y.: MEPG: Video Encryption Algorithms (August 2002), available at http://raidlab.cs.purdue.edu/papers/mm.ps
10. Seidel, T., Socek, D., Sramka, M.: Cryptanalysis of Video Encryption Algorithms. In: TATRACRYPT 2003. Proceedings of The 3rd Central European Conference on Cryptology, Bratislava, Slovak Republic (2003)
11. Alattar, A., Al-Regib, G.: Evaluation of selective encryption techniques for secure transmission of MPEG video bit-streams. In: Proceedings of the IEEE International Symposium on Circuits and Systems, vol. 4, pp IV-340-IV-343, (1999)
12. Qiao, L., Nahrstedt, K.: A New Algorithm for MPEG Video Encryption. In: CISST 1997. Proceedings of the 1st International Conference on Imaging Science, Systems and Technology, Las Vegas, NV, pp. 21–29 (July 1997)
13. National Institute of Standards and Technology (U.S.). Advanced Encryption Standards (AES). FIPS Publication 197 (2001)
14. Biryukov, A.: A New 128-bit Stream Cipher LEX, ECRYPT Stream Cipher Project Report, 2005, Available at http://www.ecrypt.eu.org/stream/lex.html
15. Meyer, J., Gadegast, F.: Security Mechanisms for Multimedia Data with the Example MPEG-1Video, Project Description of SECMPEG, Technical University of Berlin, Germany (May 1995)
16. Maples, T.B., Spanos, G.A.: Performance study of selective encryption scheme for the security f networked real-time video. In: Proceedings of the 4th International Conference on Computer and Communications, Las Vegas, NV (1995)
17. Spanos, G.A., Maples, T.B.: Security for Real-Time MPEG Compressed Video in Distributed Multimedia Applications. In: Conference on Computers and Communications, pp. 72–78 (1996)
18. Shi, C., Bhargava, B.: A Fast MPEG Video Encryption Algorithm. In: Proceedings of the 6th International Multimedia Conference, Bristol, UK (September 12-16, 1998)
19. Shi, C., Wang, S.-Y., Bhargava, B.: MPEG Video Encryption in Real-Time Using Secret key Cryptography. In: PDPTA 1999. 1999 International Conference on Parallel and Distributed Processing Techniques and Applications, Las Vegas, NV (June 28 - July 1, 1999)
20. Alattar, A.M., Al-Regib, G.I., Al-Semari, S.A.: Improved Selective Encryption techniques for Secure Transmission of MPEG Video Bit-Streams. In: ICIP 1999. Proceedings of the 1999 International Conference on Image Processing, Kobe, Japan (October 24-28, 1999) vol. 4, pp. 256–260 (1999)