Privacy ProtectionFor Video, Image and Text Transmission

1.Ms. Shraddha Bhatte ,
Student, Department of Computer Engineering, Shree L. R. Tiwari College of Engineering, Mumbai University, Thane, Maharashtra, 401107, India ,shraddhabhatte@yahoo.com

2. Dr. J. W. Bakal
Principal, Shivajirao S. JondhaleCollege of Engineering, Mumbai University, Thane, Maharashtra,421204, India ,bakaljw@gmail.com,

3. Mrs.MadhuriGedam
Assistant Professor, Department of Computer Engineering, Shree L. R. Tiwari College of Engineering, Mumbai University, Thane, Maharashtra, 401107, India

Abstract:

The issue of personal privacy is increasingly becoming prominent with the widespread use of large media (video, image, text) transmission systems. While the deployment of media transmission systems is justified by the perception of insecurity due to terrorist threats and high criminality rate, the rightful fear of privacy invasion is turning into a significant concern. In this project, we attempt to reconcile on the one hand the need for media transmission systems and on the other hand the concern of privacy protection.

***Key words**: privacy protection, Scrambling, media transfer, compression, encryption*

Introduction

Media (Video/Text/Image) transmission systems are becoming ubiquitous. Media transmission is used in areas like airports, banks, public transportation or busy city centre, military applications .Data which is to be transmit is very sensitive. Like data regarding financial transaction, data regarding to national security, medical data etc.. .There is often fear of, loss of privacy which comes along. Just providing security to network is not sufficient, there is also need of providing security to data which is transmitting on the network.

There are so many ways to providing security to multimedia data like providing password, water marking, encryption etc.As multimedia data is very huge it required very large processing. While processing multimedia data we have to think about various parameters like computational efficiency, speed, compression ratio, encryption ratio, security, format Compliance so on.As per application of multimedia data level, of security differs for example for video on demand, medical data required low level of security whereas military purpose or financial application demands for very high level of security.

In this project, we intend to provide a solution to the problem arising due to loss of privacy as a result of increase in media (video/image/text) surveillance systems..

Review of literature

In [1] survey they have presented, evaluated and discussed video encryption schemes. The choice of a video encryption scheme depends on the application-context, what are the security threats in this scenario and which functionality of the bit stream and video data has to be preserved in the encrypted domain .In [2] The diverse contributions cover a wide range of application scenarios and this survey provides a guide to find the appropriate H.264

encryption scheme for a target application. Privacy preservation is also a concern in the context of video encryption, e.g., a commonly referred application is privacy preserving video surveillance According to [3] As recent multimedia applications are growing rapidly, video compression requires higher performance as well as new features.H.264/AVC has gained more and more attention; mainly due to its high coding . This [4] article provides an overview of the technical features of H.264/AVC, describes profiles and applications for the standard, and outlines the history of the standardization process .Thomas Wiegand et al (2003), proposed an Overview of the H.264/AVC Video Coding Standard [14] H.264/AVC is newest video coding standard of the ITU-T Video Coding Experts Group and the ISO/IEC Moving Picture Experts Group .In order to protect the video [5] from unauthorized users, the encryption algorithms are needed.so that security of the multimedia data can become more and more tight. Z.Shahid et al (2009), proposed the Fast Protection of by Selective Encryption [10]. In this paper, proposes a new method for the protection of copyrighted multimedia data. W.Zeng et al (2003), proposed an Efficient Frequency Domain Selective Scrambling of Digital Video [13]. In this paper the author has proposed Multimedia data security is very important for multimedia commerce on the internet such as video, Real time video multicast. Traditional Cryptography algorithm is not provide the data security are not fast enough to process the vast amount of data generated by the multimedia application to meet the real time constraints. So, they use Selective Encryption compression in which video data are scrambled efficiently.Feng Dai et al (2011), proposed the Restricted H.264/AVC Video Coding for Privacy Protected Video Scrambling . Privacy region scrambling is an effective method to protect privacy in video.

Existing system

The system in [11] is based on an object-based representation of the scene. Basically, an altered rendering of the video is produced .where some objects are masked out depending on the user authorizations, preventing the transmission of privacy-sensitive objects .In [6,5], wavelet-domain and code stream-domain conditional access control techniques are proposed for JPEG 2000 to scramble code-blocks corresponding to Regions of Interest. In [1], it is extended to a region-based transaction. More Specifically, AC transform coefficients corresponding to ROI are scrambled by pseudo-randomly inverting their signs, concealing any privacy-sensitive data. Similarly, encryption is used to conceal faces. A secret encryption key is required in order to invert the process, thus guaranteeing privacy protection.

Problems with existing system systems

- There is no combine system for all types of media (Video ,Image, Text)
- For protection either encryption or compression is used not both
- For compression and decryption there is different algo. used on each sides
- Encryption efficiency is less
- Compression ratio is less
- Degradation in product Quality
- Security is less
- Bandwidth required is more.
- Speed is very less

Problemstatement

To ensure the security of electronic data while transferring through networks, different security techniques are used. Like every process, encryption and decryption processes

involve use of CPU recourses like CPU cycle memory. These processes require good amount of time for I/O, encryption and decryption operation. Hence these security algorithms consume a good amount of resources for encrypting and decrypting the data. So it is essential for an encryption algorithm to have good performance along with the security. Hence there is a need to analyse different compression and encryption and scrambling algorithms for various parameters so as to understand the factors that can affect the performance of this algorithms. Compression, Scrambling and Encryption play an important role in securing this confidential data against unauthorized attacks.

Along with security, factors like implementation cost and performance of different Compression, Scrambling and Encryption algorithms also need to be considered for practical implementation. Parameters like data type, data size, compression ratio, key size, key strength, encryption time, decryption time affects the selection of algorithm and therefore we need some benchmark for selection of security algorithm.

The main aim of project is privacy protection of multimedia transmission .here focus is mainly on video, image and text. According to literature survey most of the existing systems used one layer of protection that is either scrambling or compression otherwise only encryption .But as per the recent market need only one layer protection for maintain privacy of the media (video, image, text) transfer is not sufficient.So proposed system provide security to media (video, image, text) transmission in three layers.Along with security important to maintain all basic parameters like bandwidth, compression ratio, time duration of transmission, quality of product after transmission, and total cast of transmission adequate.

In proposed system H.264/AVC algorithm is use for scrambling and compression of video, image.Encryption is done using SHA-1 and AES/DES algorithms.

Proposed system

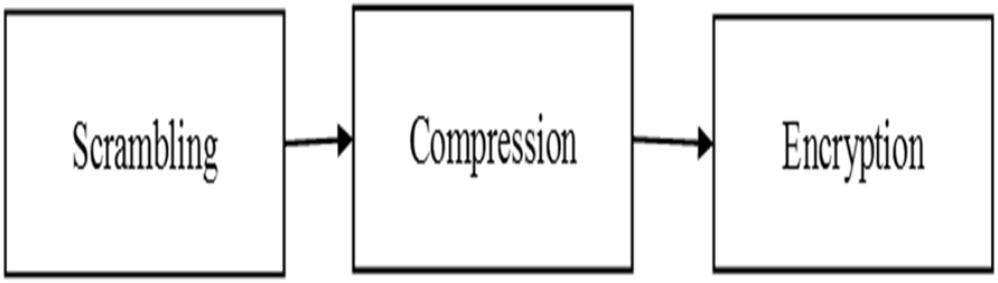
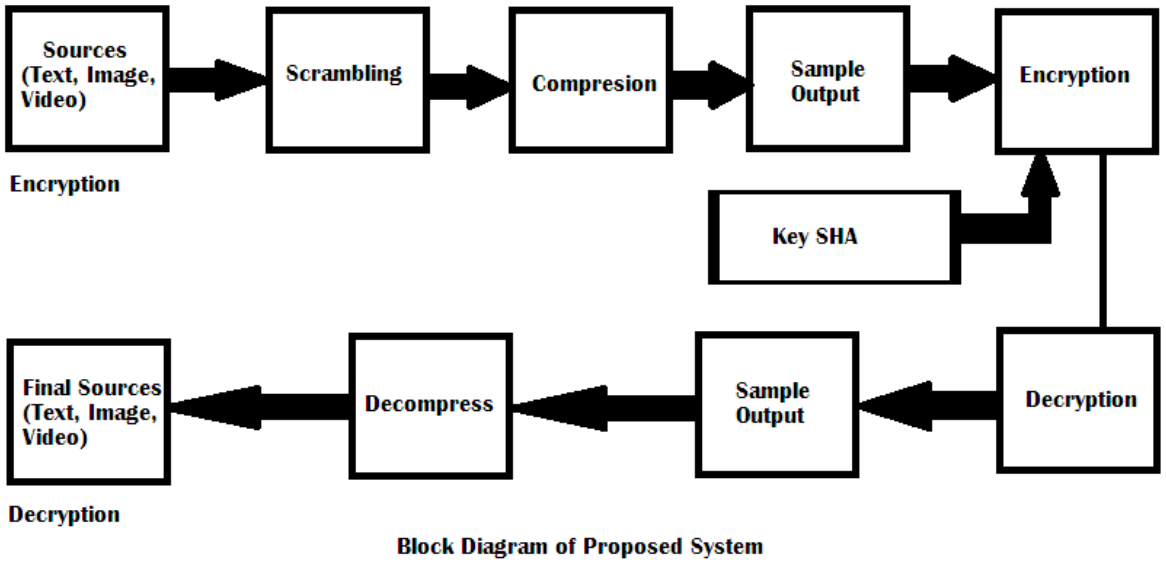


Fig 1: Block diagram of proposed system

Detail block diagram of proposed system



Block Diagram of Proposed System

What is scrambling?

A scrambling approach is a method which is employed on almost all commercially manufactured system including image and video systems.Image and video scrambling is general way to hide unwanted information and disclose un interpretable image and video

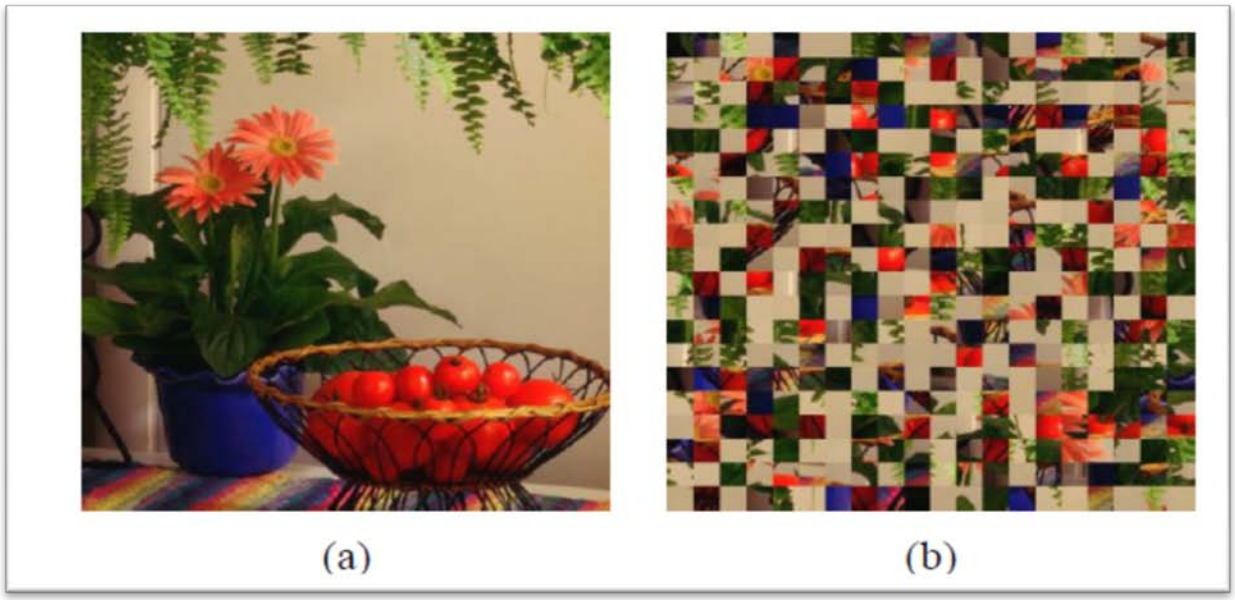
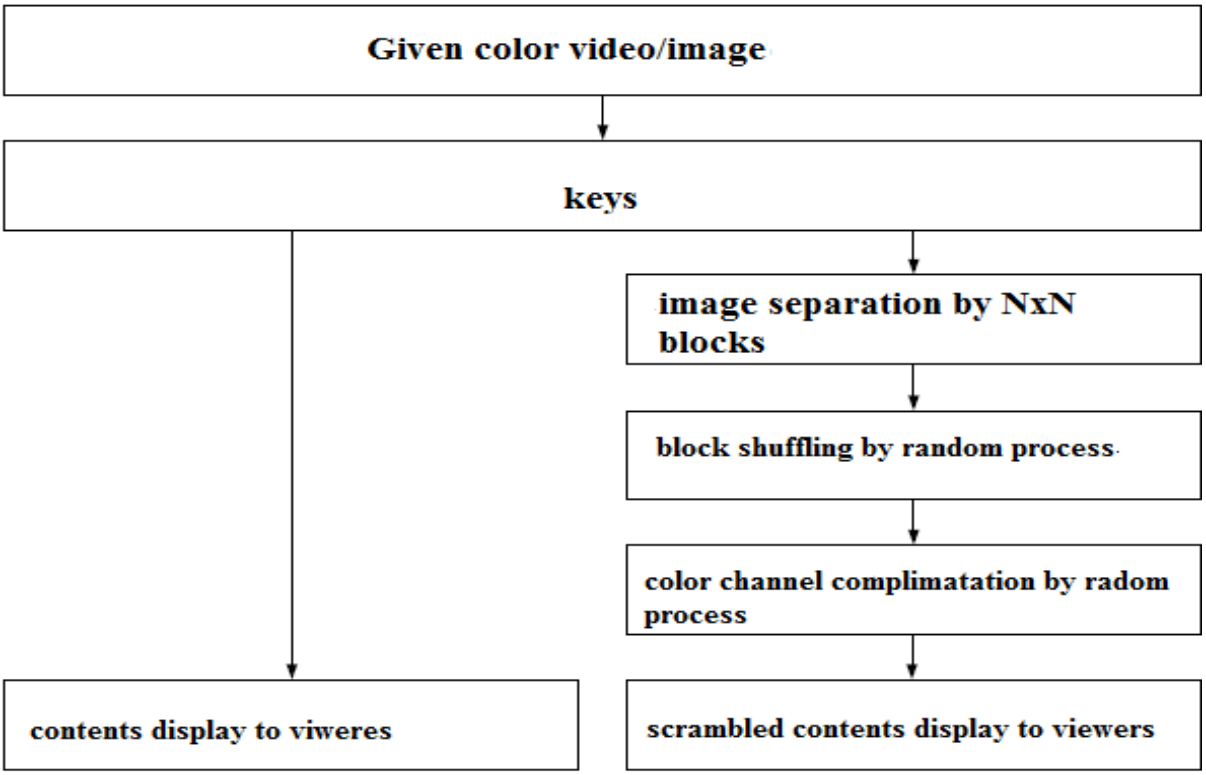


Fig 3: (a) original image (b) image after scrambling

Block diagram for Video, image scrambling:



Compression:

Compression is the act or process of compacting data into a smaller number of bits. Video compression (video coding) is the process of converting digital video into a format suitable for transmission or storage, whilst typically reducing the number of bits .Compression involves a complementary pair of systems, a compressor (encoder) and a decompressor (decoder). The encoder converts the source data into a compressed form occupying a reduced number of bits, prior to transmission or storage.The decoder converts the compressed form back into a representation of the original video data.

In H.264/AVC this is carried out by applying a transform to the residual samples and quantizing the results. The transform converts the samples into another domain in which they are represented by transform coefficients. The coefficients are quantized to remove insignificant values, leaving a small number of significant coefficients that provide a more compact representation of the residual frame.

A video encoder used in proposed system consists of three main functional units:

- a prediction model
- a spatial model
- an entropy encoder

H.264/AC address several weaknesses in previous video compression standards, H.264 delivers on its goals of supporting:

- Implementations that deliver an average bit rate reduction of 50%, given a fixed video quality compared with any other video standard
- Error robustness so that transmission errors over various networks are tolerated
- Low latency capabilities and better quality for higher latency
- Straightforward syntax specification that simplifies implementations
- Exact match decoding, which defines exactly how numerical calculations are to be made by an encoder and a decoder to avoid errors from accumulating

Encryption

Advanced Encryption Standard (AES)

Advanced Encryption Standard (AES) algorithm not only for security but also for great speed. Encrypts data blocks of 128 bits in 10, 12 and 14 round depending on key size .It can be implemented on various platforms especially in small devices. It is carefully tested for many security applications.

SHA1

SHA1 stands for "Secure Hashing Algorithm". It is a hashing algorithm designed by the United States National Security Agency and published by NIST.It is the improvement upon the original SHA0 and was first published in 1995.SHA1 is currently the most widely used SHA hash function. It is currently used in a wide variety of applications, including TLS, SSL, SSH and PGP.SHA1 outputs a 160-bit digest of any sized file or input. It uses a 512 bit block size and has a maximum message size of 2^{64} -1 bits. Key string which is taken from the user is converted into a hash using SHA-1 algorithm. The first 128 bits of this hash generated is used as our key for AES encryption process.By using SHA-1 and AES/DES algorithm we are going to generate key of 256 bit. For achieving higher security. Above all steps are done in reversed manner at the receiver side for retrieving data

Why AES/DES?

Factors	AES	**DES**	**RSA**
Developed	2000	1977	1978
Key Size	128, 192, 256 bits	56 bits	>1024 bits
Block Size	128 bits	64 bits	Minimum 512 bits
Ciphering & deciphering key	Same	Same	Different
Scalability	Not Scalable	It is scalable algorithm due to varying the key size and Block size	Not Scalable
Algorithm	Symmetric Algorithm	Symmetric Algorithm	Asymmetric Algorithm
Encryption	Faster	Moderate	Slower
Decryption	Faster	Moderate	Slower

Power Consumption	Low	Low	High
Security	Excellent Secured	Not Secure Enough	Least Secure

Why 256 bit key?

KEY	COMBINATION	SECURITY LEVEL
8	$2^8=256$	VERY LOW
16	$2^{16}=65536$	LOW
32	$2^{32}=4294967296$	LOW
64	$2^{64}=1.84X10^{19}$	LOW MEDIUM
128	$2^{128}=3.40X10^{38}$	MEDIUM
256	$2^{256}=1.15X10^{77}$	HIGH

What is H.264/AVC?

H.264/MPEG-4 AVC is a recently completed video compression standard jointly developed by the ITU-T VCEG and the ISO/IEC MPEG standards committees. The standard promises much higher compression than that possible with earlier standards. It allows coding of non-interlaced and interlaced video very efficiently, and even at high bit rates provides more acceptable visual quality than earlier standards. It increase the coding efficiency and coding flexibility.The H.264/ MPEG-4 AVC standard is a new “state-of the- art” video coding standard that addresses a fore mentioned applications

H.264 /AVC Applications

- The H.264 was designed to be flexible video format and has a very broad application range including
- Low bit-rate Internet streaming applications.
- HDTV broadcast and Digital Cinema applications.
- Web software embedding.
- Mobile TV standardization.
- Video conferencing products.
- SDTV and HDTV standardization and deployment.

Why H.264/AVC?

Tools	MPEG-2	MPEG-4 Part 2	H.264/MPEG-4 AVC
I-, P- and B-pictures	Yes	Yes	Yes, and, I-, P- and B-slices
Flexible picture prediction structure and stored B picture	Basic, no stored B-picture	Basic , no stored B-picture	Yes, allowed
Transform	8x8 DCT	8x8 DCT	Approximation of 4_4 DCT (a bit-exact transform)
Intra prediction in blocks of intra MB	Fixed prediction of DC coefficient	Adaptive prediction of DC coefficient, and first row/ column of AC coefficients	Adaptive spatial prediction of 4x4 or 16x16pixel blocks
MC prediction 16x16, 16x8	16x16; interlace only 16x8	16x16; interlace only 16x8	Yes, 16x16, 16x8, 8x16
MC prediction 8x8	No	Yes	Yes
MC Prediction sub8x8	No	No	Yes, 8x4, 4x8, 4x4
MC prediction with 1/4 pel	No, 1/2 pel only	Yes, 1/2 pel and 1/4 pel	Yes, 1/4 pel only
Multi reference prediction	No	No	Yes
Direct prediction mode in B pictures	No	1 Mode only :temporal direct with mv update	2 Modes: temporal direct no mv update, spatial direct

System implementation

Hardware and software details

- **JAVA 1.7**
- **Two Personal computers**
- **Networking Devices**
- **Network cable**
- **HUB**
- **Router**
- **Any operating system (Linux/windows)**

Advantages of H/W and S/W used

- As weare using java as programming language, ultimately we are getting platformindependence facility.
- H.**264**/AVC algorithm does the both the things Scrambling and compression.
- AES/DESoffers greater flexibility in terms of compression options and transmissionsupport for Image and text**.**
- Noneed to use separate system or image / Text / Video.We are providing facilityin one single system.

- Bandwidthrequire lesser than current system.
- Costreduces as we are combining three systems

Results and discussion

If We apply proposed system for transmitting video, image and text files and if we compare it's result with existing system we get following results.

TEXT NAME	COMPRESSION		SPEED		SECURITY	
	EXISTING SYSTEM	PROPOSED SYSTEM	EXISTING SYSTEM	PROPOSED SYSTEM	EXISTING SYSTEM	PROPOSED SYSTEM
TEXT	50% Approx	LESS THAN 50%	LOW	HIGH	LOW	HIGH
IMAGE	50% Approx	LESS THAN 50%	LOW	HIGH	LOW	HIGH
VIDEO	50% Approx	LESS THAN 50%	LOW	HIGH	LOW	HIGH

Conclusion:

We can concluded that all the existing algorithms does not help effectively for privacy protection of electronic data, So our system focus on this problem and give effective solution by combining exiting algorithm and methods in different way, for transmission of Image, video, and text. we don't have to use different systems, the same proposed system can be used for same. One more advantage of proposed system is, at receiver end as well as sender end we can use same system. Because of such combination the systems provides a simplicity to user and give proper protection to media transfer at end

Along with the security factor. Proposed system will very efficiently address the parameters like compression ratio, speed of data transfer, time required

References:

[1]IainE. Richardson,*TheH.264 Advanced Video Compression Standard*,Second Edition by, Wiley Publications, Vcodex Limited, UK.

[2]"JVTH.264/AVC Reference Software.",http://iphome.hhi.de/suehring/tml.

[3]F.Dufaux and T. Ebrahimi, "H.264/AVC Video Scrambling for Privacy Protection",*in*

Proc. IEEE InternationalConference on Image Processing,SanDiego, CA, Oct. 2008.

[4]A.W.Senior, S. Pankanti, A. Hampapur, L. Brown, Y.-L. Tian, and A. Ekin, "Blinkering Surveillance: Enabling Video Privacy through Computer Vision" IBMTechnical Report RC22886,2003.

[5]F.Dufaux and T. Ebrahimi, "Scrambling for Video Surveillance with Privacy",*in IEEE Proc. Workshop on PrivacyResearch In Vision*,New York, NY, June 2006.

[6]Saranya.P,Varalakshmi.L.M, "H.264 based Selective Video Encryption for MobileApplications,"*International Journal of Computer Applications*,Volume 17– No.4, pp. 0975 – 8887 March 2011.

[7]Ci-LinLi, Chih-Yang Lin, and Tzung-Her Chen,"Efficient Compression-Jointed QualityControllable Scrambling Method for H.264/SVC,"*InternationalJournal of Network Security*,Vol.16, No.6, PP.541-548, Nov. 2014

[8]YongshengWang, Maire O'Neill, FatihKurugollu,"THE IMPROVED SIGN BIT ENCRYPTION OFMOTION VECTORS FOR H.264/AVC,"*20thEuropean signal processing conference*,Bucharest, Romania, August 27-31,2012.

[9]W.K. Cham, R.J. Clarke, Simple high efficiency transform for image coding, in: Proceedings of the International Picture Coding Symposium, Davis, CA, 1983, pp. 66–67

[10]Z. Shahid, R. Eifrig, A. Luthra, K. Panusopone, Coding of an arbitrary shaped interlaced video in MPEG-4, in: Proceedings of the IEEE International Conference on Accoustics, Speech and Signal Processing (ICASSP'99), 2009 pp. 3121–3124

[11]A. Alatter, A.G. MacInnis, SEI message for the film mode hint in JVT codec, JVT-E078, Joint Video Team of ISO/IEC MPEG and ITU-T VCEG, Geneva, October 1999

[12]Zafar Shahid, Transform Coding of Images, Academic Press, New York, 2011

[13]W. Zeng, G. Sullivan, Field repetition and timing indications, JVT-E122, Joint Video Team of ISO/IEC MPEG and ITU-T VCEG, Geneva, October 2003

[14]A. Hallapuro, M. Karczewicz, H. Malvar, Low complexity transform and quantization—Part I: basic implementation, JVT-B38, Joint Video Team of ISO/IEC MPEG and ITUT VCEG, January 2002