CHAPTER 1

INTRODUCTION TO MULTIMEDIA SECURITY

1.1 PROLOGUE

Recent advancements in computers and communications have brought in a huge market for distributing digital multimedia through the Internet. Multimedia data such as images, audio and video are currently used extensively in applications like video-on-demand, video conferencing and broadcasting. However, this increase in digital documents, multimedia processing tools, and the worldwide Internet connectivity has also created a perfect stage for copyright fraud and uncontrollable distribution of multimedia bringing to the forefront the challenging issue of multimedia content security. Hence, the problem of efficient multimedia data encryption has recently gained more attention in both academia and industry.

Although encrypting the entire multimedia content by traditional cryptographic cipher yields a satisfactory level of security, it has several shortcomings. First, the computational cost associated with encrypting the entire multimedia content is often high due to the large data size. Second, the encryption and decryption operations add further level of complexity to the system. Also, additional hardware or software is needed in order to implement it. This is particularly unfavorable in applications such as mobile communications and embedded systems, where devices such as cellular phones and portable equipments are resource constrained due to size limitation and power consumption considerations. Hence, it is desirable to develop efficient yet secure multimedia encryption techniques. Several selective encryption schemes have been proposed as possible solutions, in which only a specific portion of the multimedia data is selected for encryption. One possible classification of selective encryption algorithm is relative to the application of encryption with respect to compression.
i. **Pre compression**

This type of selective encryption algorithm performs encryption before compression. (Fig.1.1). Such algorithms are inherently format compliant and perform encryption prior to compression causing bandwidth expansion which adversely affects compression efficiency.

![Fig.1.1 Pre compression approach](image)

ii. **Post compression**

Selective encryption algorithms belonging to this category perform compression before encryption (Fig. 1.2). But these algorithms introduce overhead and are inherently non format compliant.

![Fig.1.2 Post compression approach](image)
iii. In compression

A new approach of integrating encryption with compression has recently become the area of research in multimedia encryption. This paradigm called as joint compression and encryption is shown in Fig. 1.3. Hence the two fold objectives of high security and efficient use of transmission and storage resources are thus achieved. By exploiting this feature, effective encryption schemes can be designed that can achieve high security at a relatively low computation cost.

![In compression approach](image)

1.2 CRYPTANALYSIS

Cryptanalysis is the art of deciphering an encrypted message in whole or in part, when the decryption key is not known. Depending on the amount of known information and the amount of control over the system by the adversary or cryptanalyst, there are several basic types of cryptanalytic attacks.
i. **Ciphertext-only attack**

This is an attack where the adversary has only the ciphertext to work with. Without any knowledge of the plaintext, the cryptanalyst analyzes the ciphertext by searching for statistical similarities between different pieces of ciphertext or from sequences that occur more than others. If the ciphertext is purely random without statistical irregularities, the adversary would have to resort to the brute force exhaustive key search attack.

ii. **Brute force attack**

This is a type of ciphertext-only attack, which is based on exhaustive key search. For well-designed cryptosystems, this should be computationally infeasible. Normally 128-bit keys are considered secure against the brute force attack.

iii. **Known-plaintext attack**

In this type of attack, an adversary has some knowledge about the plaintext corresponding to the given ciphertext. This may help determine the key or a part of the key.

iv. **Chosen-plaintext attack**

In this attack, an adversary can choose the plaintext and obtain the corresponding ciphertext. The adversary may later use the knowledge about the plaintext-ciphertext pairs to obtain the secret key or at least a part of it.

For an encryption scheme to be effective, it must be able to withstand these cryptographic attacks by the adversary. Hence deciding the level of security needed for a particular application is a significant task and optimal security level has to be identified. If the multimedia to be protected is not that valuable, it is sufficient to choose relatively
light level of encryption. On the other hand, if the multimedia content is highly valuable or represents government or military secrets, the cryptographic security level must be the highest possible. For many applications such as pay-per-view, the content data rate is typically very high, but the monetary value of the content may not be high at all. Thus, very expensive attacks are not attractive to adversaries, and light encryption such as degradation may be sufficient for distributing the video. In contrast, applications such as videoconferencing or videophone may require much higher level of confidentiality.

1.3 EVALUATION CRITERIA

Security is the basic requirement of multimedia content encryption. As multimedia encryption is different from text/binary encryption, multimedia requires two kinds of security namely, cryptographic security and perceptual security. Cryptographic security refers to the security against cryptographic attacks, while perceptual security focuses to make the encrypted multimedia contents unintelligible to human perception. Perceptual security is a measure of the perceptual distortion of the cipher video with respect to the plain video. Hence an efficient encryption scheme has to provide perceptual security. For this, the encryption scheme should be designed to meet the following objective evaluation criteria:

i. **Peak Signal to Noise Ratio (PSNR).**

In order to measure the quality of the video data at the output of the decoder, Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR) are often used. The PSNR in terms of decibels (dB) between two frames having 8 bits per pixel is given by eqn. 1.1.

\[
\text{PSNR} = 10 \log_{10} \left( \frac{255^2}{\text{MSE}} \right) \tag{1.1}
\]
where MSE is defined as

$$\text{MSE} = \frac{1}{|A|} SSD$$  \hspace{1cm} (1.2)

and SSD is the sum of the squared differences between the reconstructed (\(s_{\text{ll}}\)) and the original (\(s\)) macro block pixels given by eqn.(1.3) and \(A\) represents the reference macroblock

$$SSD = \sum_{(x,y) \in A} |s[x,y,t]-s[x,y,t]|^2$$  \hspace{1cm} (1.3)

\[\text{ii. Low encryption time}\]

It is imperative that the encryption algorithms should be efficient such that they do not delay the transmission or access operations. Hence the encryption time should not exceed an acceptably small portion of the total computation time of compression.

\[\text{iii. Low overhead bits / No impairment to compression ratio}\]

The ultimate goal of multimedia compression is to reduce the bit stream length to the minimum possible extent. This fundamental goal should not be violated by the multimedia encryption scheme and achieving a high security at the expense of sacrificing the compression ratio is not desired. Thus the total number of bits added due to encryption has to be minimal.

\[\text{iv. Key Sensitivity}\]

Key sensitivity is defined as the change in ciphertext caused by the change in the key. In a good cipher, slight difference in the keys should cause great changes in the ciphertext.
1.4 OBJECTIVE OF THE THESIS

The foremost objective of this thesis is to develop efficient encryption schemes for MPEG-2 and H.264/AVC video to suit varied applications. The thesis aims

i. To focus on modifying and optimizing existing cryptosystems for MPEG-2 and H.264 video in order to provide enhanced security with lower encryption time.

ii. To develop algorithms which integrate encryption and compression with minimum overhead bits.

iii. To propose algorithms which provide optimum security based on the requirement of the applications and to analyze the performance of the proposed algorithms to meet the multifold objectives.

1.5 VIDEO CODING STANDARDS

With the widespread adoption of technologies such as Digital television, Internet streaming video and DVD-Video, video compression has become an essential component of broadcast and entertainment media. In the last decade, video compression technologies have evolved in the series of MPEG-1, MPEG-2, MPEG-4 and H.264.

1.5.1 MPEG-2

MPEG-2 forms the heart of broadcast-quality digital television for both Standard-Definition and High-Definition Television (SDTV and HDTV). MPEG-2 video was designed to encompass MPEG-1 and also to provide high quality with interlaced video sources at bit-rates in the range of 4-30 Mbit/s. MPEG-2 video was developed as an official joint project of both the ISO/IEC and ITU-T organizations and specifies the
syntax and semantics of the video bitstream which include parameters such as bit rate, picture size, resolution etc. MPEG-2 uses the basic coding structure that is still predominant today as shown in Fig 1.4a and 1.4b. These codecs are popularly referred to as hybrid codecs, since they use a combination of predictive and transform domain techniques.

![Block Diagram of MPEG-2 video (a) encoder (b) decoder](image)

**Fig 1.4** Block Diagram of MPEG-2 video (a) encoder (b) decoder
Encoding of video information is achieved by two main techniques; spatial and temporal compression. Spatial compression involves determining redundant information within a picture, and discarding frequencies that are not visible to the human eye. Temporal compression is achieved by encoding the difference between successive pictures. The movement between two successive pictures is determined by motion estimation prediction. The information obtained from this process is then used by motion compensated prediction to define the parts of the picture that can be discarded. A given picture is constructed from the prediction from a previous picture, and may be used to predict the next picture. There is also the need to have pictures which are not used in any reference for random access. Therefore MPEG-2 defines three picture types:

**I** (Intraframe) pictures. These are encoded without reference to another picture to allow for random access.

**P** (Predictive) pictures are encoded using motion compensated prediction on the previous picture. They may themselves be used in subsequent predictions.

**B** (Bi-directional) pictures are encoded using motion compensated prediction on the previous and next pictures, which must be either a B or P picture. B pictures are not used in subsequent predictions.

For each macroblock, which consists of one 16×16 luminance block and two 8×8 chrominance blocks, a syntax element indicating the macroblock coding mode is transmitted. While all the macroblocks of I pictures are coded in INTRA mode, macroblocks of P-pictures can be coded in INTRA or INTER mode. In B-pictures, the prediction signal for the motion-compensated INTER mode can be formed by forward, backward, or bidirectionally interpolated prediction. The motion compensation is generally based on 16×16 blocks and the motion vectors are predicted from a single previously encoded motion vector in the same slice.
In the MPEG-2 encoder, texture coding is done using Discrete Cosine Transform (DCT) on blocks of 8×8 samples, and uniform scalar quantization is applied that can be adjusted using quantization values from 2 to 62. The entropy coding is performed using zigzag scanning and two-dimensional run-level Variable Length Coding (VLC). There are two available VLC tables for transmitting the transform coefficient levels, of which one must be used for predictive-coded macroblocks and either can be used for INTRA macroblocks as selected by the encoder on the picture level.

1.5.2 H.264 /AVC

Recent trends in Digital video technology, has enabled newer applications with a broadening range of requirements regarding basic video characteristics such as spatiotemporal resolution, chroma format and sample accuracy. H.264 is the latest video coding standard of the ITU-T Video Coding Experts Group (VCEG) and the ISO/IEC Moving Pictures Experts Group (MPEG) and has currently become the most widely accepted video coding standard.

Though prior video coding standards such as MPEG-2 / H.262 and H.263 have been used in several digital video applications, new technology domains such as mobile TV, High Definition TV broadcasting, professional video recording and digital cinema have started proliferating in which these previously standardized video coding technology are hardly able to keep pace. Another reason for the advent of this coding standard is that traditional application areas of digital video are requiring more cost-efficient solutions in terms of bit rate and end-to-end reproduction quality. H.264 also has the flexibility to support a wide variety of applications with very different bit rate requirements.

In the face of these challenges, H.264/MPEG4 Advanced Video Coding (AVC) standard, has demonstrated significantly improved coding efficiency, substantially enhanced error robustness, increased flexibility and scope of applicability relative to its predecessors thus opening new markets and opportunities for the industry. Another set of extensions for Scalable Video Coding (SVC) is currently being designed aiming at a
functionality that allows the reconstruction of video signals with lower spatiotemporal resolution or lower quality from parts of the coded video representation.

The video coding layer of H.264/MPEG4-AVC is similar to that of other video coding standards such as MPEG-2 video. It uses a hybrid of block-based temporal and spatial prediction in conjunction with block-based transform coding. Fig. 1.5 shows the block diagram of a H.264 video encoder.

![Block diagram of a H.264 video encoder](image)

**Fig. 1.5** Basic coding structure of H.264/AVC for a macroblock

A coded video sequence in H.264/MPEG-4-AVC consists of a sequence of coded pictures. A coded picture can represent either an entire frame or a single field, as in the case of MPEG-2 video. The encoding of a picture begins with splitting the picture into blocks of samples. The first picture of a sequence is typically coded in *Intra* mode i.e., without using any other pictures as prediction references. Each sample of a block in such an Intra picture is predicted using spatially neighboring samples of previously coded
blocks. The encoding process chooses which neighboring samples are to be used for Intra prediction and how these samples are to be combined to form a good prediction, and sends an indication of its selection to the decoder.

For all remaining pictures of a sequence **Inter** coding is utilized. Inter coding employs inter picture temporal prediction (motion compensation) using other previously decoded pictures. The encoding process for temporal prediction involves choosing motion data that identifies the reference pictures and spatial displacement vectors that are applied to predict the samples of each block. The **residual** of the prediction (either Intra or Inter), which is the difference between the original input samples and the predicted samples for the block, is transformed. The transform coefficients are then scaled and approximated using scalar quantization. The quantized transform coefficients are entropy coded and transmitted together with the entropy-coded prediction information for either Intra- or Inter-frame prediction.

**Entropy coding:** H.264/AVC supports two methods of entropy coding. The default entropy coding method uses a single codeword set for all syntax elements except the residual data. The vectors of scanned transform coefficient levels are transmitted using a more sophisticated method called Context-Adaptive Variable Length Coding (CAVLC). This scheme basically uses the concept of run-length coding as it is found in MPEG-2, H.263, and MPEG-4; however, Variable Length Coding (VLC) tables for various syntax elements are switched depending on the values of previously transmitted syntax elements. Since the VLC tables are well designed to match the corresponding conditional statistics, the entropy coding performance is improved in comparison to schemes using a single VLC table.

The efficiency of entropy coding can be improved further if the Context-Adaptive Binary Arithmetic Coding (CABAC) is used. On one hand, the usage of Arithmetic coding allows the assignment of a non-integer number of bits to each symbol of an alphabet and on the other hand, the usage of adaptive codes permits adaptation to non-stationary symbol statistics. Another important property of CABAC is its context
modeling. The statistics of already coded syntax elements are used to estimate conditional probabilities of coding symbols. Inter-symbol redundancies are exploited by switching several estimated probability models according to already coded symbols in the neighborhood of the symbol to encode.

In the decoding process, the same prediction values for the prediction of subsequent blocks in the current picture or subsequent coded pictures are computed. The decoder inverts the entropy coding process, performs the prediction process as indicated by the encoder using the prediction type information and motion data. It also inverse-scales and inverse-transforms the quantized transform coefficients to form the approximated residual and adds this to the prediction. The result of the addition is then input to a deblurring filter, which provides the decoded video as its output. The H.264/AVC design includes the deblurring filter for removing block edge artifacts which is applied inside the motion prediction loop. The strength of filtering is adaptively controlled by the values of several syntax elements.

Profiles: The H.264/AVC standard specifies a number of Profiles, each specifying a subset of the coding tools available in the H.264 standard. A Profile places limits on the algorithmic capabilities required of an H.264 decoder. Hence a decoder conforming to the Main Profile of H.264 only needs to support the tools contained within the Main Profile; a High Profile decoder needs to support further coding tools; and so on. Each Profile is intended to be useful to a class of applications. For example, the Baseline Profile may be useful for low-delay, ‘conversational’ applications such as video conferencing, with relatively low computational requirements. The Main Profile may be suitable for basic television/entertainment applications such as Standard Definition TV services. The High Profiles add tools to the Main Profile which can improve compression efficiency especially for higher spatial resolution services, e.g. High Definition TV.
1.6 RESEARCH CONTRIBUTIONS

The thesis proposes and analyses the performance of various security enhancement algorithms for MPEG-2 and H.264/AVC video depending on the requirement of the applications such as video storage, video transmission, real-time interaction and wireless/mobile communication.

- **MPEG-2 Encryption Schemes**

  MPEG-2 video compression is the de facto standard for entertainment video. MPEG-2 standard specifies the syntax and semantics of an enclosed video bit stream such as bit rates, picture sizes and resolutions, and how it is decoded to reconstruct the picture. MPEG-2 has a flexibility of formats and profiles and defines a range of picture sizes to suit different applications. It has so successfully established itself that it is likely to remain as the dominant standard in many applications. This thesis proposes several enhanced encryption schemes suitable to MPEG-2 video applications.

  - **Multiple Huffman Table Scheme**

    Huffman coding is the most widely used entropy coder in image/video compression systems. A scheme known as the Multiple Huffman Table scheme [32-37] was recently proposed to achieve encryption along with compression. Though this scheme has several advantages it does not overcome the chosen plaintext attack. An enhancement of this Huffman scheme is proposed in this work which essentially overcomes this attack and improves the security. The proposed encryption approach consists of two modules. The first module is the Randomized Huffman Table module, the output of which is fed to the second XOR module to enhance the performance. Security analysis shows that the proposed scheme can withstand the chosen plaintext attack. The
efficiency and security of the proposed scheme makes it an ideal choice for real time secure multimedia applications.

- **Randomized Arithmetic coding scheme**

  Arithmetic coding provides an effective mechanism for removing redundancy in the encoding of data. Although arithmetic coding offers extremely high coding efficiency, it provides little or no security as traditionally implemented [38-45]. A modified Randomized Arithmetic coding is proposed in this thesis, which achieves encryption by inserting randomization in the compression process using a secret key. The proposed approach consists of two cascaded modules. The first one is called Randomized Arithmetic Coding (RAC) while the second one is the XOR module. The joint RAC/XOR encryption paradigm incurs extremely low computational and implementation costs. Security analysis shows that the proposed scheme is robust against cryptanalytic attacks and makes it an ideal choice for high quality secure video applications.

- **Chaotic encryption**

  Selective encryption of MPEG-2 video stream exploits the relationship between encryption and compression to reduce the encryption requirements, saving in complexity and facilitating new system functionality. Several works based on chaotic theory have been implemented [76-88]. In the proposed work, a video encryption scheme based on the widely used substitution–diffusion architecture which utilizes the chaotic 2D standard map and 1D logistic map is proposed. Hence, the advantages of both, selective encryption and chaos have been combined in this work with no impact on compression efficiency. A cryptanalytic approach is performed for validating the security

- **Secret Sharing based on DCT and DWT**

  In highly sensitive videos such as military applications, confidential video broadcasting etc. where every part of the video is important it is required that Intra and
Inter frames need to be encrypted [89-92]. This work proposes encryption algorithms suitable for real time applications based on the method of Secret Sharing using both Discrete Cosine Transform and Discrete Wavelet Transform with the objective of reducing the time taken for encryption, while maintaining security. Accordion representation is a new video compression approach which tends to exploit the temporal redundancy in the video frames and improves compression efficiency with minimum processing complexity. The proposal consists of avoiding the computationally demanding motion compensation process where temporal redundancy is converted into spatial redundancy. Integration of the two modules, namely encryption based on secret sharing along with Accordion representation is done to obtain an enhanced video security algorithm. This reduces the time taken for encryption, making it suitable for real time applications.

- **H.264/AVC Encryption Schemes**

  Video transmission in wireless environments is a challenging task calling for high-compression efficiency as well as a network-friendly design. Both have been major goals of the H.264/AVC standardization effort addressing “conversational” such as video telephony and “non conversational” such as storage, broadcast or streaming applications. The video coding layer of the H.264/AVC provides significant improvement in compression performance. The network-friendly design goal of H.264/AVC is achieved through the Network Abstraction Layer that has been developed to transport the coded video data over any existing or future networks. This makes H.264/AVC coding an attractive option for all wireless applications including multimedia messaging services, packet-switched streaming services and conversational applications [97-112].

  - **Intra prediction mode Encryption**

    H.264/AVC supports a wide range of prediction options – intra prediction using data within the current frame, inter prediction using motion compensated prediction from
previously coded frames, multiple prediction block sizes, multiple reference frames etc. By selecting the best prediction options for an individual macroblock, an encoder can minimize the residual size to produce a highly compressed bit stream. H.264 employs intra prediction technique to remove spatial redundancies within intra frame. Since video sequences can be easily distorted by modification of the prediction mode, the intra prediction mode is chosen as the main target for easy video scrambling and this encryption scheme is applied over wireless sensor networks [122-125]. Multimedia Wireless Sensor Networks (MWSNs) are sensor networks composed of multimedia sensors which are capable of capturing and transmitting multimedia information and face cryptographic attacks [144-149]. A secure and selective encryption framework has been proposed in this thesis so as to optimize network lifetime and video distortion for the energy constrained wireless sensor network.

- **Intra frame encryption**

Wireless links are error-prone and unreliable and packet video transmission over 3G networks experience packet loss due to fading and interference. This causes substantial quality degradation to the transmitted video which is avoided by appropriate error resilience features [117-118,131-142]. In this proposal, Intra frame of H.264/AVC is encrypted to minimize computational complexity while providing reasonable security, as the important components of the compressed data become candidates for selective encryption. The remaining data is unencrypted due to the fact that conceptually P and B frames are useless without knowing the corresponding I frame and this encryption scheme is applied over 3G networks.

- **Motion vector Encryption**

Motion Vector Differences contain dynamic information and are the important data in H.264 encoding and decoding process and several MVD encryption schemes have been proposed [94-97,114-117]. A selective encryption scheme to encrypt the motion
vectors of the video has been presented in this thesis which aims at providing enhanced security using dynamic keys and permutation code algorithm. The prime concern is that, the added security does not introduce distortion and the scheme adopts permutation code algorithm to encrypt motion vector residuals and DCT coefficients. The video is transformed using DCT and the transformed coefficients are quantized. The dynamic keys are utilized for forming the permutation table.

- **Entropy coding encryption**

  H.264/AVC supports two types of entropy coding modules. Context-adaptive variable length coding (CAVLC) supported in H.264/AVC baseline profile and Context-adaptive binary arithmetic coding (CABAC) supported in H.264/AVC main profile. In CAVLC, Non Zeroes (NZ) are coded by three syntax elements, namely, coeff token, signs of trailing ones, and remaining nonzero levels [99-101]. Zeros are coded by two syntax elements, namely, total number of zeros and runs of zeros. Coeff token is used to code total number of NZs and trailing ones. The remaining NZs are coded using seven VLC look-up tables. In the proposed work, to keep the bitstream compliant, these remaining NZs alone are chosen for encryption as the other syntax elements are used for prediction and cannot be encrypted. CABAC uses the Binary Arithmetic Coding which means that only binary decisions (1 or 0) are encoded. A non-binary-valued symbol (e.g. a transform coefficient or motion vector) is “binarized” or converted into a binary code prior to arithmetic coding. This binarization module is selected for encryption using AES in the proposed work. Simulation results indicate that the proposed selective encryption schemes overcome the drawbacks of the existing schemes [119-121], meet the requirements of an integrated compression encryption system and are fully compliant to H.264/AVC decoder, with no change in bitrate.

- **Scalable video coding encryption**

  Scalable video coding (SVC) is a highly suitable video transmission system designed to deal with the heterogeneity of the modern communication networks. SVC
supports efficient coding of video in such a way that multiple versions of the video signal can be decoded at a range of bitrates, spatial resolutions and/or temporal resolutions or frame rates[150-157]. Several encryption schemes for SVC have been proposed in the literature[158-162] which suffer from one or more drawbacks. A layered selective encryption scheme for Scalable Video Coding (SVC) is proposed in this work. The structure of SVC consists of a Base layer and one or two enhancement layers. For Base layer, motion vector and entropy encryption is performed, while enhancement layers are encrypted based on the type of scalability and the most prominent data of that type. The proposed scheme is found to be computationally efficient as it encrypts domains selectively according to each layer and is format compliant by utilizing the H.264/SVC structure.

1.7 ORGANIZATION OF THE THESIS

Chapter 1 gives an introduction to multimedia security. Multimedia data requires either full encryption or selective encryption depending on the application requirements. For example, military and law enforcement applications demand tight encryption while commercial applications such as pay TV require security at a lower level. Cryptanalysis is further discussed in detail.

Chapter 2 presents an exhaustive literature survey on the security requirements for MPEG-2 and H.264/AVC video. An extensive study on the existing cryptographic schemes is carried out to identify the challenges and problems in the existing schemes used in varied applications.

Chapter 3 explains the proposed lightweight MPEG-2 based encryption schemes. Encryption schemes based on modification to the basic Huffman coding and Arithmetic coding are discussed. Normally a single Huffman table is used in the standard for encoding whereas in the proposed work multiple Huffman tables are constructed for encryption and in Arithmetic coding randomization is introduced for encryption.
Chapter 4 presents encryption schemes for highly confidential applications of MPEG-2 video. Chaos based encryption is one such proposal. Chaotic systems have attracted the attention of cryptographers due to their fundamental features such as ergodicity, mixing property and sensitivity to initial conditions /system parameters. A video encryption scheme based on the widely used substitution–diffusion architecture which utilizes the chaotic 2D standard map and 1D logistic map is discussed. The chapter also presents two proposals, one based on secret sharing of DCT coefficients and the other based on secret sharing of DWT coefficients along with encryption of motion vectors. The other proposal consists of Accordion conversion of Inter frames and scrambling which effectively reduces the computational time.

Chapter 5 deals with H.264 based light weight video encryption schemes. Intra prediction mode encryption is one such example and is applied over wireless sensor networks and the issues on joint optimization of video quality, content protection and energy efficiency have been fully addressed. Similarly Intra frame encryption has been tested over 3G networks, as video transmission for mobile terminals has become a major application and is a key factor to their success.

Chapter 6 presents two enhanced selective encryption schemes for H.264 video. A selective encryption scheme to encrypt the H.264 video using dynamic keys and permutation code algorithm is presented. This scheme adopts permutation code algorithm to encrypt motion vector residuals and DCT coefficients. The chapter also addresses in detail a selective encryption scheme performed with compression in the entropy coding modules. The syntax element which is chosen for encryption in CAVLC module is the magnitude of remaining Non Zeros known as Level information and is encrypted using AES. Selective encryption is performed on binstrings which are input to Binary Arithmetic coding in CABAC entropy coding module. The proposed scheme utilizes negligible computational power at constant bitrate, and is suited for real-time multimedia streaming over heterogeneous networks.
Chapter 7 describes an efficient selective encryption scheme for H.264/Scalable Video Coding (SVC) which makes use of the characteristics of SVC and fully meets the encryption requirements of SVC. The proposed scheme performs encryption in three domains: Intra-Prediction mode (IPM), residual data and motion vector difference values. The chapter discusses the simulation results which indicate that the SVC streams are secured effectively.

Chapter 8 concludes the thesis with the major findings of the study. A summary of the research contribution and scope for further work has been presented.