CHAPTER 2
LITERATURE SURVEY

This chapter presents details of well known encryption and compression algorithms in the following categories: (i) independent video encryption algorithms, (ii) joint video compression and encryption algorithms, and (iii) video compression standards.

2.1 INDEPENDENT VIDEO ENCRYPTION ALGORITHMS

As already mentioned in Chapter 1, subsection 1.4.2, both compression and encryption are carried out separately in independent encryption techniques. Any suitable algorithms can be used for compression and encryption (Abomhara 2010). Some of the well known encryption algorithms are discussed in the following subsections.

2.1.1 The Data Encryption Standard (DES)

DES is a famous block cipher encryption algorithm. IBM’s Lucifer was adopted, modified and released as DES standard by National Institute of Standards and Technology (NIST) in 1977 (Valizadeh 2004). DES is commonly used to encipher PIN numbers in bank transactions. DES can generate block ciphers with each block containing 64 bits. A 64-bit key is used for encryption of blocks (Seung 1996).
2.1.2 **Rivest-Shamir Adelman (RSA) Algorithm**

RSA is one of the widely used public key algorithms. It was invented in 1977 by Ron Rivest, Adi Shamir, and Len Adelman. It is based on factorization of integers into their prime (Guido 2003). Consider that sender ‘X’ and receiver ‘Y’ want to communicate with each other. The receiver ‘Y’ chooses two distinct large primes $p$ and $q$ then multiplies them together to form $N = p*q$. It also chooses an encryption exponent $e$, such that the, greatest common divisor of $e$ and [(p-1)*(q-1)] is 1. The receiver then computes decryption key $d$, $d=1/e \mod [(p-1)*(q-1)]$. The pair $(N,e)$ is made as public; $p$ and $q$ are kept as secret. Let $M$ be the plain text block and $C$ be the cipher text block, then

\[ C = M^e \mod n \]  
\[ M = C^d \mod n \]  

Both sender and receiver must know values of ‘$n$’ and ‘$e$’. Receiver should also know the value of ‘$d$’ also. The above mentioned scheme makes a public key encryption of $K_U = \{e, n\}$ and private key encryption of $K_R = \{d, n\}$.

2.1.3 **Advanced Encryption Standard (AES)**

Rijndael cryptosystem (Guido 2003) was adopted by NIST as AES standard in 2001. AES operates on 128-bit blocks, arranged as $4 \times 4$ matrices with 8-bit entries. The algorithm is capable of using a variable block length and key length (Guido 2003). The latest specification of AES allows any combination of key lengths i.e. 128, 192, or 256-bit keys and blocks of length 128, 192, or 256-bit.
2.1.4 Wavelet Packet Transform Algorithm

An encryption method based on wavelet packet transform is proposed in (Dominik 2006). This method encrypts only selected portions of video and therefore consumes less time for ciphertext generation. As it does not encrypt entire data, it is vulnerable to security threats. Wavelet transform before encryption may increase the computational complexity when compared to other algorithms (Dominik 2006).

2.1.5 Elliptic Curve Cryptography Algorithm

The polynomial interpolation based Elliptic Curve Cryptosystem (ECC) is proposed in (Liew 2011). ECC uses 160-bit key which is shorter than keys used in other heavyweight algorithms such as RSA. As the key size is smaller in ECC, it takes less encryption time. Transferring video streams over wireless networks using ECC is prone to privacy and malicious attacks due to smaller key size (Liew 2011).

2.1.6 Twofish Algorithm

Twofish (Bruce 1998) is an open source encryption algorithm which has the key size of 256-bits. Sixteen rounds of XOR operation is performed during encryption which leads to more computational steps. Twofish requires low computational resources but complex decryption processes. Twofish algorithm is prone to known-plaintext and piracy attacks. Hao et al have proposed a lightweight and scalable encryption algorithm for streaming video over wireless networks. The security architecture proposed in (Hao 2007) is based on the lightweight public key scheme called Derivable Public Key (DPK).
2.1.7 Pretty Good Privacy (PGP) Algorithm

Pretty Good Privacy (PGP) is used for secured communication through the Internet (Yongcheng 1996). This is based on Public Key Infrastructure (PKI) and some standard encryption mechanisms. PGP is an open source algorithm and allows anyone to evaluate and recommend modifications. In PGP, keys are of 512, 1024, or 2048-bit lengths. It can transfer text data faster than video data over the Internet.

2.1.8 Tiny Encryption Algorithm (TEA)

Tiny Encryption Algorithm (TEA) is the fastest encryption algorithm (David 1994). This is based on Feistel function which involves more number of rounds to get better security. TEA performs mixed operations such as XOR, ADD and SHIFT which are used to provide better secrecy. The block size and key size are 64-bit and 128-bit respectively. TEA encrypts data into a machine language format, and is vulnerable to brute-force attacks.

2.1.9 RC 4 and RC 6 Algorithms

Rivest Cipher 4 (RC4) is good for Secured Socket Layer (SSL) security (Anil 2007). The Rivest Cipher 6 (RC6) is a symmetric key based lightweight block encryption technique. RC6 is structurally similar to its previous version RC5, and uses dependent data rotation, XOR operation and modular addition. It employs more number of rounds, wide variety of wavelengths and different key sizes (David 1994), (Hao 2007). RC6 supports keys with 128, 192 and 258 bits which has a block size of 128 bits. In RC6, four working registers and integer multiplication inclusion method are used whereas only two registers are used in RC5. The multiplication process of RC6 provides better security and higher throughput when compared to RC5.
2.1.10 Lightweight Cellular Automata-based Symmetric Key Encryption

Somanath et al have proposed a Lightweight Cellular Automata-based Symmetric Key Encryption (LCASE) technique which generates a 128-bit lightweight block cipher with 128, 192 and 256-bit keys (Somanath 2009). LCASE is mainly used in resource constrained devices which require low processing power and low-end-devices that need less memory storage. LCASE is against differential cryptanalysis and linear cryptanalysis which may be affected by timing attacks.

2.1.11 International Data Encryption Algorithm (IDEA)

IDEA is a symmetric block cipher encryption technique proposed in (Rajashekhar 2010). Initially, IDEA was called as Improved Proposed Encryption Standard (IPES) and performs eight identical transformations for encrypting the data. It has the key size of 128 bits and block size of 64 bits. IDEA uses the same features and framework for both encryption and decryption but uses different keys for encryption and decryption. Two operations namely, key mixing and addition are performed in each round. Key mixing combines four 16-bit input words with sub-key words in parallel by using either modular addition or modular multiplication operation. Subsequently, output generated in previous round is given as input to the next round (Leong 2000). IDEA uses sub-keys which are 0 or 1 for key mixing and XOR operation. These sub-keys are very weak and create problems during XOR operations.

2.1.12 Humming Bird-2 Algorithm

Daniel et al have proposed an authenticating encryption algorithm, Humming Bird-2 (HB-2) for the hardware implementation of lightweight process using low end microcontrollers (Daniel 2011). This consists of 128-
bit secret key and 64-bit initialization vector. It includes properties of both traditional stream ciphers and block ciphers. As authenticated encryption process is involved HB-2 provides confidentiality and integrity. The important drawback of this algorithm is hardware leakage which leads to complex calculations.

2.1.13 PRESENT Algorithm

One of the most compact video encryption algorithms, PRESENT, is proposed in (Andrey 2007). This is 26 times smaller than the standard encryption algorithm AES. Its block size is 64-bit and the key size is either 80-bit or 128-bit. This is used in low-power consumption and high chip efficiency devices. In PRESENT, both hardware efficiency and security have been equally considered for cipher design. Main goal behind the development of PRESENT is that the level of security should offer 64-bit block and 80-bit key. This algorithm is suitable for low-power designs.

2.1.14 Probabilistic Encryption

Main objective of probabilistic encryption is the randomness which gives different constants for same messages and different ciphertexts (Shafi 1984). Security is improved in probabilistic encryption by hiding partial information about the plaintext. During encryption, the plaintext is padded with the random string generating the padded encrypted cipher. Decryption is done by using the reverse process by eliminating padding from the probabilistic encryption.
2.2 JOINT VIDEO COMPRESSION AND ENCRYPTION ALGORITHMS

In joint compression and encryption algorithms, encryption is done along with compression. Encryption takes less time when compression is combined with it (Shaou 2002). Combining compression and encryption provides high speed encryption algorithms as well as improved security.

2.2.1 SECMPEG Algorithm

The joint compression and encryption algorithm proposed in (Jurgen 1995), SECMPEG, does selective encryption using conventional encryption algorithms. This has been designed to provide security for high volume video signals such as, ISO standard 11172 or MPEG-1. Before decoding, the video is segmented and converted into block of streams which is represented using four layers and five confidentiality levels (C-levels). Then, Huffman coding is used for compression and DES is used for encryption. In level 0, encryption is not performed. Level 1 and level 2 consist of details about layers 1 to 4. The level 3 contains all I-frames which are intra-coded macro-black blocks. Encryption takes place in level 4. In SECMPEG algorithm, all layers of video stream are not encrypted due to selective encryption.

2.2.2 Zig-Zag Permutation Algorithm

The proposed solution in (Lei 1996) performs compression and encryption with minimum overhead using random permutation and probabilistic encryption. It provides different levels of secrecy for various multimedia applications. The proposed strategy employs Discrete Cosine Transformation (DCT) to map smaller blocks of size 8x8 to bigger blocks of
size 1x64. The output of DCT is uniformly quantized and all quantized coefficients are arranged in zig-zag order. Finally, entropy coding is done for compression. In this technique, compression is done before encryption which leads to less execution time. But the computational complexities involved in both zig-zag order and mapping decreases the speed of video compression. The zig-zag permutation is prone to known-plaintext attack (Lei 1996).

2.2.3 Video Encryption Algorithm (VEA)

The Video Encryption Algorithm (VEA) is introduced by Changgui Shi and Bharat Bhargava for joint compression and encryption of video data (Changgui 1998a). This is an efficient video encryption algorithm which has less computational complexity. Only a streamed video can be encrypted using VEA technique. Before encryption, size of the video data should be reduced using any standard compression method. MPEG-2 or MPEG-4 is used for compression, because VEA and MPEG are mutually dependent on their statistical properties (Changgui 1998a).

2.2.4 MPEG Video Encryption Algorithm (MVEA)

A MPEG Video Encryption Algorithm (MVEA) is proposed in (Changgui 1998) for joint video compression and encryption of video applications. This is an improved version of Video Encryption Algorithm (VEA) (Changgui 1998a) where the XOR operation is used with a secret key whereas in VEA, XOR operation is used without passing any secret key (Changgui 1998a). Sign bit of discrete cosine coefficient in I-frame block is also encrypted. In MVEA, the differential sign value of DC coefficient and motion vectors in P-frames and B-frames are XOR-ed with a secret key. This
method is used in secure video-on-demand, video conferencing and video email applications. The main disadvantage of MVEA is, the huge size of secret key used in encryption (Bharat 2004).

2.2.5 Real-time Video Encryption Algorithm (RVEA)

To overcome known-plaintext attack, Changgui et al have proposed RVEA (Changgui 1999). The difference between VEA, MVEA and RVEA lies in the use of XOR operation. VEA uses only XOR operation and MVEA uses XOR operation with a secret key. In RVEA, the XOR operation is replaced by DES algorithm. RVEA is a selective encryption algorithm which operates on sign bits of both DCT coefficients and motion vectors of MPEG-compressed-video. RVEA can use any secret key cryptographic algorithms to encrypt selected sign bits. Encryption time of RVEA is much less than naive algorithms because it encrypts only 10% of the total bit stream. RVEA can defend known-plaintext attack, but, it may be affected by perceptual attacks.

2.2.6 Set Partitioning Hierarchical Tree

This method is proposed by Shaou et al for transmitting biomedical signals over the Internet (Shaou 2002). It is necessary to compress biomedical files/signals for efficient use of bandwidth while transmitting to long distances over the Internet for urgent treatments. Privacy and security are important issues when compressed biomedical signals or data is delivered over a public channel such as the Internet. In (Howard 2000), a biomedical signal compression method called Set Partitioning in Hierarchical Trees (SPIHT) is proposed for compression which uses the AES algorithm for encryption. In this method, the compressed SPIHT bit streams are identified
based on their importance to signal quality. Then, AES is used to encrypt important parts that can be defined and chosen by the user (Howard 2000). This method encrypts only selected parts of biomedical signal.

### 2.2.7 Frequency Domain Scrambling Approach

Wenjun et al have proposed a frequency domain scrambling approach in (Wenjun 2003), which performs encryption after employing Discrete Cosine Transform (DCT). The input video signal is converted into frequency domain at the encoder side and coefficients are divided into equal segments. These are subject to selective scrambling which consist of operations such as selective bit scrambling, random sign change, block rotation, block shuffling and coefficient shuffling with a sub-band segment. A key is used to control the scrambling.

### 2.2.8 Pure Permutation Algorithm

In this algorithm, compression occurs before encryption because of real-time processing, and it is decoded by the hardware (Adam 2004). The pure permutation algorithm is obtained by scrambling bytes in a frame of a video stream. Separate software is used for decryption. This algorithm is prone to known-plaintext attack. It provides limited security. If frames are known, the secret permutation list can be determined easily by comparing with the cipher text. Hence, all frames can be decrypted easily. According to Shannon's Theorem, even if hackers know one I-frame of video stream, it decrypts the whole video.
2.2.9 MHT Scheme

In (Chung 2005), Multiple Huffman Table (MHT) converts entropy coders into encryption ciphers. In this scheme, a Huffman table is used and the ordering is kept as a secret using a key. The pre-stored multiple Huffman tables are used to quantize the DCT coefficient. Therefore, it is impossible to decode the bit stream without knowing tables and the key. The computational overhead of MHT is less. It is vulnerable to chosen-plaintext attack and random bit attack (Jiantao 2007).

2.2.10 Singular Value Decomposition and Parallelized Wavelet Filter Bank

Min-Sung et al have proposed a method in which, compression and encryption are done by using two transform stages (Min 2005). They are Singular Value Decomposition (SVD) and Parallelized Wavelet Filter Bank (PWFB). The proposed method uses orthogonal matrices, generated by SVD which spreads frequency content of the signal into the available spectrum when applied on the original vector. The attacker can easily guess the approximate frequency spectrum of the wavelet decomposition.

2.2.11 Puzzle Algorithm

The Puzzle algorithm (Fuwen 2005), (Fuwen 2005a) is inspired by the children’s game puzzle. There are two main steps involved in this algorithm. The first step is puzzling the compressed video of each frame by partitioning it into ‘n’ blocks of length ‘l’ and disordering these blocks by random permutation list ‘p’. In the second step, the temporary cipher text $T$ ($t_1$, $t_2$, and $t_q$) is obscured using an encryption method with low computational overhead.
2.2.12 Selective Encryption Algorithm

Selective encryption technique has been proposed to reduce the amount of processing overhead and to meet the security for real time video applications (Xiliang 2003), (Yuefa 2012). It uses layering structures to encrypt different levels of selective parts in MPEG video, i.e. encryption of all headers, such as I-frame, I-blocks in P-frames and B-frames. The main objective of selective encryption is to encrypt only the I-frame as there is no use of P-frame, and B-frame without I-frame. Aegis (George 1995) is another version of new secure MPEG video mechanism introduced by Maples and Spanos which encrypts only the I-frame of all MPEG groups of frames in a video stream (George 1996), (Iskender 1996). Aegis uses DES for encryption. Main drawback of Aegis is the large key size during encryption. Therefore, it is not suitable for applications such as military videos, business video conferencing and pay TV broadcast in which security is the main constraint (Ishfaq 2005).

2.2.13 DCT Based Bitwise XOR Encryption

An algorithm for the practical lossless compression and encryption of gray scale video has been proposed in (Daniel 2007). This is based on temporal correlations in the video. It uses distributed source-coding technique for compressing the encrypted video data. The video has been encrypted by applying bitwise exclusive-OR (XOR) between key bits and the source. Then DCT and localized predictors are used on the encrypted bit frames.

2.2.14 Randomized Entropy Coding/Rotation in Partitioned Bitstream

A joint compression and encryption technique is proposed in (Dahua 2007). It contains two modules namely, Randomized Entropy Coding
(REC) and Rotation in Partitioned Bitstream (RPB). The first module Randomized Entropy Coding (REC) is used for video compression which can multiply entropy coding by employing Multiple Huffman Table (MHT). The second module Rotation in Partitioned Bitstream (RPB) is used for encrypting the compressed video stream. The RPB module partitions the bit stream after performing randomized entropy coding operation on video stream and then performs rotation on each partition. This operation helps in defending known-plaintext and chosen-plaintext attacks. This method is used for encrypting large real time video applications, because the size of video data has been reduced using REC module before encryption. The computational cost of this combined algorithm is very high and the encryption speed is less when compared to other existing algorithms such as AES, RSA and PGP.

2.2.15 Optimized Multiple Huffman Tables

Studies on security of video encryption scheme based on secret Huffman tables, cryptanalysis shows certain drawbacks in MHT technique (Shaimaa 2010). To overcome this, a new scheme, Optimized Multiple Huffman Tables (OMHT) was proposed for efficient secure video transmission in (Shaimaa 2010). The OMHT technique depends on using statistical-model-based compression which generates different tables from same type of images or videos to be encrypted. This led to increased compression efficiency and security. The effectiveness and robustness of this scheme was verified by measuring its security strength and comparing the computational cost against other techniques (Ahsan 2011). High compression ratio and encryption degree are achieved in one single step which simplifies the system design and makes it flexible.
2.2.16 Multilayer Key Stream Based Encryption

A lightweight multilayer key stream based video encoding using joint encryption and compression is proposed in (Suman 2011). The multilayer key is extracted from the video stream which acts as a key generator. Two different key streams are used to encrypt the video data. Every video has an associated video key $V_k$, chosen by the content creator/provider which could be content adaptive. Every frame in the Group of Pictures (GOP) has a global key called the temporal key $T_k$. The first temporal key is generated from $V_k$. The temporal key is used to encrypt the frame which is in the temporal domain. Subsequent temporal keys are generated by using hashing, SHA-256. The joint process encodes a slice first, then encrypts it with a RC4 stream cipher, and performs post slice-encoding. The post process bits are not encrypted, as they may be required when the decoder analyzes Network Abstraction Layer Units (NALU). If the decoder cannot analyze the NALU correctly, it is difficult to extract the payload and decrypt. A new key is generated only when a new slice begins encoding and all keys are never generated simultaneously. This improves security by avoiding the presence of a complete key stream set in the memory at any time. This has been facilitated by efficient handling of packet loss in real-time transmission. The key may be affected by known-plaintext attack, because it is derived from selected frames of video data.

2.2.17 Arithmetic Coding (AC)

In 1952, David A. Huffman has proposed an entropy encoding algorithm called Huffman Coding for lossless data compression (David 1952). It uses a variable length code table for encoding symbols or characters in a file. Codes are derived based on the estimated probability of occurrence of each possible value of the source symbol. It is also called as prefix-free code.
because any of the bit-string representing one particular symbol will not be the prefix of another bit-string representing some other symbol. Huffman coding is employed in static applications such as FAX, electronic books, ZIP files, JPEG, MPEG (Hassan 2010). In 1994, Paul and Jeffrey (Paul 1994) have proposed an efficient implementation of arithmetic coding which provides an effective mechanism for removing redundancy in the encoded data. Main advantages of arithmetic coding are its optimality and inherent separation of coding and modeling. Pure arithmetic coding is optimal for a stochastic data source whose probabilities are exactly known, but it relies on relatively slow arithmetic operations such as multiplication and division (Nithin 2008).

A preliminary analysis on the use of arithmetic coding as encryption scheme is in (John 1999). In arithmetic coding, an entire source sequence is mapped to a single code stream. Therefore, a single error in an arithmetic code stream can cause lot of trouble at the decoder. The Key-based Secured Arithmetic Coding (KSAC) is proposed by Jiangtao et al in 2006, in which key is used to split the interval before encoding new symbol, thus allowing compression and encryption simultaneously (Jiangtao 2002), (Jiangtao 2006). Later, in the same year, a new encryption algorithm was proposed by Daniel Socek et al in which the encryption preserves spatial correlation (Daniel 2007). In 2007, research was conducted by Dahua Xie and Jay Kuo on encrypting multimedia data using joint randomized entropy coding and rotation in partition bit stream, which incurs very less computational and implementation cost (Dahua 2007).

A thorough study of Secure Arithmetic Coding (SAC) under an adaptive chosen-ciphertext attack is done in (Jiangtao 2009). It is observed that SAC is not suitable for applications where the attacker has access to the decoder (Mahnaz 2010). It also presents an improved version of SAC to
enhance the security and performance. Simultaneous arithmetic coding and encryption scheme utilizing chaotic maps has been proposed in (Kwok 2010). It performs better than traditional arithmetic coding schemes because both position and direction of line segments in the piecewise linear chaotic map are controlled using a secret key. Security aspects of Randomized Arithmetic Coding (RAC) are analyzed and it is observed that RAC is not secured in the presence of an eavesdropper and definitely not secured against chosen-plaintext or chosen-ciphertext attacks (Raj 2011). Randomized Matrix Arithmetic Coding (RMAC) is proposed in (Kavitha 2011) to overcome chosen-cipher text attack. In this scheme, a randomized matrix is generated using random key based on user profile.

### 2.2.18 Chaotic Encryption

The chaos theory was established in 1970 from various research areas, such as physics, mathematics, biology and chemistry. Chaos and encryption technique have tight relationship because chaos mixing property and sensitivity to initial conditions can be connected with confusion and diffusion property in ciphers (Ray 1996), (Ljupco 1998). (Matthews 1984) have discussed about chaotic cryptography, and a novel stream cipher based on one-dimensional chaotic map. Later, many digital chaotic ciphers and analog chaotic secure communication approaches have been proposed in the literature (Stephen 1994), (Jiri 1998), (Alvarez 1999), (Lei 2010), (Zhi 2011), (Amit 2012), (Oi 2012), (Qinchen 2008).

The chaotic map algorithm is used to perform compression and encryption simultaneously (Kwok 2008). This can be applied for lossless data and lossy image compression. In (Amit 2010), a new combined arithmetic coding and chaotic mapping method for image encryption is proposed. It performs both compression and encryption simultaneously (Baptista 1998),
This is prone to cryptographic attacks because use of wrong skew parameter value gives imperfect reconstruction and incomplete random output. A similar value is determined which helps to guess first few symbols of the binary string. This is also prone to plaintext attack. The performance of Chaotic Based Antiemetic Coding (CBAC) is better when encryption is done with Arithmetic Coding (AC). In CBAC, encryption is done on compressed video domain which takes less time (Amit 2010). In (Jianyong 2011), a modified chaos scheme based on the model of sampling without replacement has been presented. In this technique, significant number of chaotic map iterations wasted for visiting irrelevant symbols is reduced. Compression capability is improved and is close to that of conventional entropy coding.

An efficient technique to encrypt and compress a text file is proposed in (Houcemeddine 2010). It overcomes the drawback of MHT. There is only one basic tree for every message and this tree can be mutated according to the input (plaintext), the secret key \((x_0, p, m_0)\) and two parameters \((\alpha, \beta)\). The mutation process depends directly on the plaintext and secret keys, so plaintext attack and ciphertext attack do not have any impact on this algorithm.

### 2.3 VIDEO COMPRESSION STANDARDS

Several techniques are proposed for video compression. Some of the video compression techniques used for text and image compression show better performance when compared to compressed video data. This is due to large sizes of video files. After compression, the compressed data should
maintain its resolution and quality (Andrew 2003). Well known compression techniques are accepted by International Telecommunication Union (ITU) and International Standard Organization (ISO). Some of the popularly used video compression techniques are discussed in subsequent sections.

### 2.3.1 H.120

The first digital video encoding technique H.120 was introduced in 1984 which was published by International Telegraph and Telephone Consultative Committee (CCITT). In 1988, H.120 was modified with contributions from organizations such as ITU Telecommunication Standardization Sector (ITU-T) and Telecommunication Standardization Bureau (TSB) (Kliaratishvili 1994).

### 2.3.2 H.261

ITU Telecommunication Standardization Sector (ITU-T) introduced the first H.26x family video coding standard, H.261 in 1988. H.261 is designed for transmitting video data with data rate in multiples of 64-Kbit/sec over Integrated Services Digital Network (ISDN) lines. But later, this operates at video bit rates between 40-Kbit/sec and 2-Mbit/sec. This standard supports only Common Intermediate Format (CIF) (352x288 Luma with 176x144 Chroma) and Quarter Common Intermediate Format (QCIF) (176x144 Luma with 88x72 Chroma) video frame sizes (Gene 2003). In 1993, new version of H.261 is introduced for processing still picture graphics with 704x576 Luma and 352x288 Chroma resolutions which has backward-compatibility. This was the first standard in which the macroblock concept is introduced (Alessandro 1999). The basic processing unit of H.261 standard is called macroblock. Each macroblock consists of a 16x16 array
of luma samples and two corresponding 8x8 arrays of chroma samples, using 4:2:0 sampling and a YCbCr color space. The H.261 standard is helpful in decoding the stored video data (Mee 1998). However, H.261 cannot be used for real time video encoding.

2.3.3 H.263

ITU-T Video Coding Experts Group (VCEG) has developed a low-bit rate compression format, H.263 in 1996 for videoconferencing application which is in the H.26x family of ITU-T domain. This standard is used in many real-time applications including sites such as YouTube, Google Video and MySpace (Ahmad 2010). Many websites use this standard for their video encoding (Ujwala 2010). Real Video Codec (RVC) was based on H.263 till Real Video 8 was launched. H.263 is also used in Packet-switched Streaming Services (PSS), Multimedia Messaging Service (MMS) and Internet Multimedia Subsystem (IMS) (Kodituwakku 2010).

2.3.4 H.264

H.264 was introduced in 2002 to mitigate disadvantages of MPEG and to improve the compression performance in broadcasting. The H.264 standard is widely used in satellite and cable TV since it is more convenient than other compression standards (Thomas 2010). It is currently used for video recording, video telephony, video streaming and HDTV streaming over the Internet. When compared to MPEG-2, it provides better video quality with half data rate which is more useful for real-time video data transfer with high speed during video conferencing (Enrico 2006), (Suman 2011). References such as (Heiko 2007), (Iain 2003) and (Thomas 2003) may be referred for additional details on H.264.
2.3.5 MPEG-1

The Motion Pictures Expert Group-1 (MPEG-1) compression standard is designed for compressing low quality video, such as Video Home System (VHS). This can be used for making CDs, in cable TV and digital audio broadcasting (Jurgen 1995). MPEG-1 is a lossy compression standard. Many products and technologies are introduced based on MPEG-1 (Tino 1996), (Gene 1996).

2.3.6 MPEG-2

The MPEG-2 standard comes in three main parts, such as systems, video, and audio. MPEG-2 extends functions provided by MPEG-1 to enable efficient encoding of video and associated audio at a wide range of resolutions and bit rates. Part-1 of MPEG-2 standard specifies two types of multiplexed bitstreams (Kwok 2008). They are program stream and transport stream. The program stream is analogous to systems part in MPEG-1. It is designed for flexible processing of multiplexed stream and for environments with low error probabilities. The transport stream is constructed in a different way and includes a number of features that are designed to support video communications or storage in environments with significantly higher error probabilities (Chi 2011).

2.3.7 Audio Video Interleave

Audio Video Interleave (AVI) format is introduced as a built-in feature of the Windows Operating System in 1992. Digital file format is used to store the audio and video data. AVI is derived from Resource Interchange File Format (RIFF), which divides a file's data into several blocks (Navas 2011).
2.3.8 **Dirac**

The open source video compression format known as Dirac was introduced by British Broadcasting Corporation Research (BBCR) in 2008, with the help of Schrodinger and Dirac research foundation (Sinzobakwira 2010). This is a high quality video compression standard used in High Definition Television (HDTV) and compete with existing technologies such as H.264 and Video Coding-1 (VC-1). It supports 1920x1080 resolution (Chi 2011), (Patrick 2009), (Vishesh 2011) and more data rate like MPEG-4 Part 2 and MPEG-2 Part 2. The motion compensation and interframe coding features are included in later versions of Dirac. In 2008, BBC transmitted High Definition Television (HDTV) videos of Beijing Olympics using Dirac standard.

2.4 **SUMMARY**

Brief description of various independent compression and encryption, joint compression and encryption algorithms is presented in this chapter. All these algorithms have pros and cons with respect to efficiency, computational cost, complexities, computational overhead, process time and compression ratio. In the case of joint compression and encryption algorithms, compression and encryption are embedded as a single process and are fast. They provide better compression ratio and less process time. In the case of compression independent encryption techniques, compression is carried out separately. Computational overhead increases the cost. Efforts are being diverted by researchers all over the world to overcome and mitigate the drawbacks in existing algorithms and also for providing better security. Subsequent three chapters discuss details of three proposed joint compression and encryption algorithms that give better CPU and memory utilization.