**Methodology proposed by Meyer and Gadgets**

This methodology is proposed for MPEG videos [15]. This method uses traditional encryption methods RSA or DES in CBC mode to encrypt MPEG video stream. It implements 4 level of security.

(i) Encrypting all stream headers.

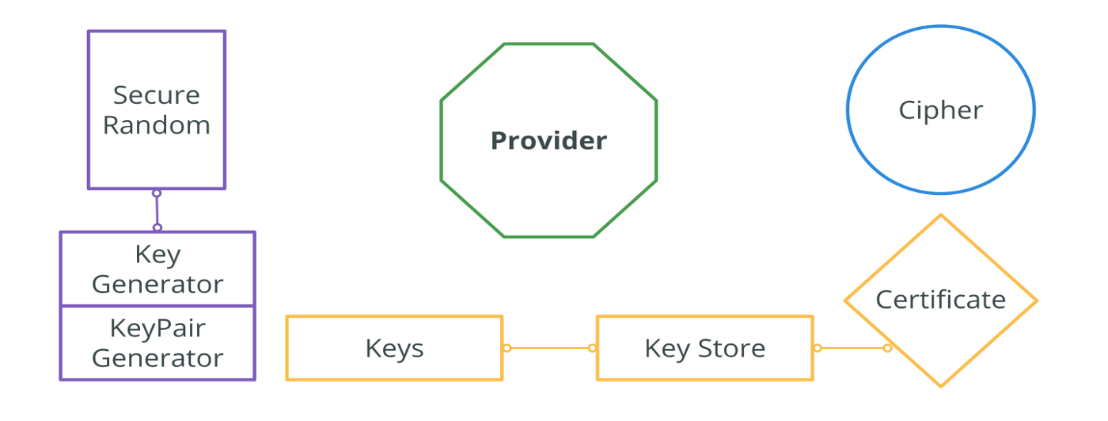
(ii) Encrypting all stream headers and all DC and lower AC coefficients of interceded blocks.

(iii) Encrypting I-frames and all I-blocks in P- and B frames.

(iv) Encrypting all the bit streams.

The number of I blocks in P or B frames can be of the same order as the number of I blocks in I frames. This reduces considerably the efficiency of the selective encryption scheme [16]. Encryption ratio may vary based on which parameters are encrypted. Encrypting only headers have very less encryption ratio. But encrypting all the bitstreams have 100% encryption ratio. Speed of this methodology again varies based on traditional algorithm in use such as DES or RSA and number of parameters that are encrypted.

Many security levels can be obtained. Encrypting only stream headers is not sufficient since this part is easily predictable. But encrypting all the bit streams can provide high security. Detailed cryptanalysis of this methodology is not defined. A special encoder and decoder are required to read unencrypted SECMPEG stream. The encoder proposed is not MPEG compliant.



Figure

**Methodology proposed by Spanos and Maples**

Aegis mechanism is proposed in [17]; it encrypts intraframes, video stream header and the ISO 32 bits end code of the MPEG stream using DES in CBC mode. Experimental results were conducted by the authors showing the importance of selective encryption in high bitrate video transmission to achieve acceptable end-to- end delay.

It is also shown that full encryption creates bottleneck in high bitrate distributed video applications. Agi and Gong [18] showed that this algorithm has low security since encrypting of only I-frames offer limited security because of the inter-correlation of frames; some blocks are intra-coded in P and B frames. Furthermore, Pand B-frames are highly correlated when they correspond to the same I-frame.

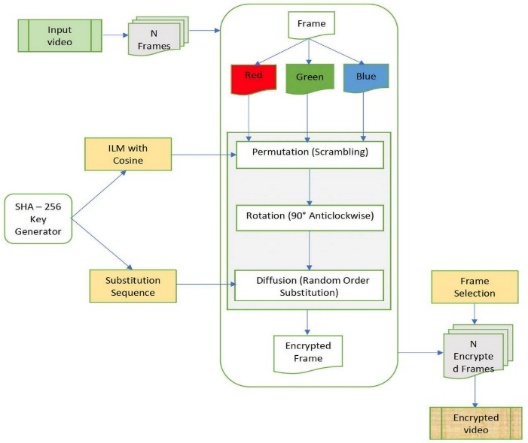
They also underlined that it is unwise to encrypt stream headers since they are predictable and can be broken by plaintext-ciphertext pairs. Alatter and Al-ragib [19], apparently unaware of Agi and Gong work [18], stressed the same security leakage. Encryption is performed after compression, thus no impact is observed on the compression efficiency. The resulting bitstream is not MPEG compliant.

* **Methodology proposed by Shi and Bhargava**.

In [20], the authors proposed video encryption algorithm (VEA) which uses a secret key to randomly change the signs of all DCT coefficients in an MPEG stream. It is fast as it operates on a small portion of original video. It is more efficient than DES algorithm because it only selectively encrypts a small number of bits of the MPEG compressed video and selected bit is only XORed one time with the corresponding bit of the secret key. VEA does not protect from plaintext attack provided the attacker knowns the original video image (plaintext and ciphertext).

In [21], the authors present a new version of VEA reducing computational complexity; it encrypts the sign bits of differential values of DC coefficients of I-frames and sign bits of differential values of motion vectors of Band P-frames. This type of improvement makes the video playback more random and more non viewable. When the sign bits of differential values of motion vectors are changed, the directions of motion vectors change as well.

In addition, the magnitude of motion vectors change, making the whole video very chaotic. Modified VEA encrypt DC coefficients of I frame, and leave AC coefficients of I frames unchanged.



Thus it significantly reduces encryption computations. Because DC coefficients of I frames are differentially encoded, changing a few sign bits of differential values of DC coefficients will affect many DC coefficients during MPEG decoding. MPEG’s differential code of DC coefficients and motion vectors increase the difficulty to break MVEA encrypted videos.

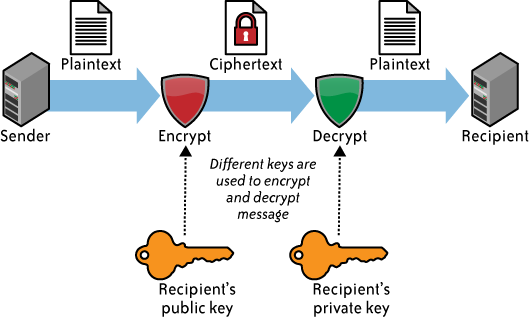
The first version of VEA [21] is only secure if the secret key is used once. Otherwise, knowing one plaintext and the corresponding ciphertext, the secret key can be computed by XORing the DCT sign bits. Both versions of VEA are vulnerable to chosen plaintext attacks; in [21], it is feasible to create a repetitive/periodic pattern and then compute its inverse DCT.

The encryption of the image obtained will allow us to get the key length and even compute the secret key by chosen-plaintext attack.

MHT: The authors propose a method using multiple Huffman coding tables. The input datastream is encoded using multiple Huffman tables. The content of these tables and the order that they are used are kept secret as the key for decryption. In the proposed system, instead of training thousands of Huffman coding tables, it only train and obtained four different Huffman tables.

Then, thousands of different tables can be derived using a technique called Huffman tree mutation. Gillman and Rivest [25] showed that decoding a Huffman coded bit stream without any knowledge about the Huffman coding tables would be very difficult.

However, the basic MHT is vulnerable to known and chosen plaintext attacks as pointed out in .



MSI: The arithmetic QM coder is based on an initial state index; the idea is to select 4 published initial state indices and to use them in a random but secret order. Unlike Huffman coding with a fixed and pre defined Huffman tree, the QM coder dynamically adjusts the underlying statistical model to a sequence of received binary symbols. It is very difficult to decode the bitstream without the knowledge of the state index used to initialize the MQcoder. A little effect on compression efficiency is observed. This is due to multiple initializations of the QM coder due to initial state index changing.

In our thesis we will be mainly concerned with the conﬁdentiality aspect of information

security, speciﬁc to image and video data. Conﬁdentiality to information is provided using

encryption schemes. The original message is referred to as plaintext and the encrypted

message is referred to as ciphertext. The plaintext can be obtained from ciphertext using

the reverse process of encryption known as decryption. Encryption is performed using a

secret key as an input. If the same key is used for both encryption and decryption, the

encryption system is known as symmetric-key encryption or private-key encryption. If

a diﬀerent key is used for encryption and decryption, and the keys used exist in pairs,

such systems are known as asymmetric encryption or public-key encryption. In public key

encryption, the key used for encryption is made public by the receiver, and is referred

to as public key, and the key used for decryption is kept secret by the receiver, so that

only he can decrypt the message. The decryption key is also referred to as private key.

Public key encryption can be also used for purpose of authentication by following the

reverse process of encryption. Public key crypto-systems are more commonly used for

authentication and for sharing a secret key used in private-key encryption system.