CHAPTER 1

INTRODUCTION

1.1 WHY IS ENCRYPTION NECESSARY?

Traditional commerce requires security of data in all aspects of multimedia format and a very necessary requirement of traditional commerce. The applications associated in the real world as of video conferencing applications and VOD applications requires that only the paid users can access the multimedia data presented before the various user stream.

No doubt authentication controlled mechanisms are available in order to manage the accessibility of multimedia formatted data in distributed form. But, on formats of wireless networks, networks of satellite or any other IP network system the data in multimedia format cannot only be made secure by such authentication mechanisms. Treating the complete data in the format of binary form confirms that it is one of the greatest famous techniques to secure underlying data in multimedia format. Further, the complete data is encrypted with the usage of secret key algorithms for encryption such as the Data Encryption Standard Algorithm also called as DES for short, AES, IDEA, etc. Secret key encryptions are very complicated and require heavily computed values. The problems faced are described in two implementations.

In the software, as the algorithms are implemented it shows that it is slow enough in processing the large data amount that are formed applications in the multimedia format. The other one is related to hardware where its applications in hardware format implementations additional costs are added at both the ends of data generators and also the receiving users.

There are two major factors causing challenge to multimedia data encryption. First, typical multimedia data have large size (the size for eg., of any MPEG-1 video format of two hours is in and around 1GB). Secondly, processing of the data in multimedia formats has the need to get processed in the real-time-frame scenario. The video codec-device is put or overlaid with heavy burden when large or huge data is being processed in a very small timespan. Heavy affects are also seen on the requirements related with space and storage and also the network communications are drastically burdened. The application of algorithms of both encryption as well as decryption type aggravates the faults and causes the latency to increase either at the time or even after the phase of encoding.
1.2 Motivation for Research Work

In this thesis, four efficient MPEG video encryption algorithms are preferred for implementation. The four algorithms although have varied strengths of attack and attack protection, it does cause additional overhead no doubt smaller in size in those of the codec of MPEG. These algorithms can be implemented on software. These implementations are not slow and fast by means of speed. The speed of such an implementation fulfils the requirement of the applications available in the format of MPEG in real-time data providing immense importance. The development of hardware-based encryption techniques in video is getting its toll now. In order to decode the bit streams of MPEG on the DVD, hardware may be used as DVD protection is becoming vital. Usage of techniques of encryption in MPEG helps protecting the contents of DVD from basically and possibly two types of the required equipment: DVD decoders for video and equipment having the capability of storing and recording. The video decoders of the DVD format could be encrypted using the aforementioned technique of encrypting the DVD.

1.3 Problem Domain

The existing algorithms cannot be used for perceptual video streaming. Also, the percentage of encryption is low in all algorithms.

Another problem associated with existing algorithms is the time taken for encryption by these algorithms is higher than the threshold for the streaming delay permitted.

1.4 Objective of Research

Here, the four encryption algorithms for video suggested and given by Bhargava, Wang and Shi, processed in MPEG video format will be analysed using the MATLAB tool. The aim of this implementation is to first analyse how the encryption algorithms affect the video and then calculate parameters such as the percentage of encryption in these formats and secondly to determine the delay caused due to encryption of video. Also, the size of the actual video is compared with the encrypted video to check for buffer allocation while transmission. Another part of the implementation involves making use of varied key lengths with these four algorithms and consequently analysing how the encoding time is affected with different key lengths. This might help us in deciding what application requires which type of encoding and encryption and the security level that is necessary to be provided in such applications in
multimedia world. Thus, it is quite clear that there cannot be any perfect encryption algorithm, it always is and will be dependent on the application or the authorized users in the real world scenario.

1.5 Organization of the Thesis

The Thesis organization is shown as follows. Chapter 2 is a brief introduction to MPEG and its working fundamentals. Chapter 3 discusses the earlier work related with video encryption that are being developed and implemented in multimedia security field. Chapter 4 provides with the technical aspects of the four video encryption algorithms that are to be analysed and finally be used in the implementation field. Chapter 5 shows implementation using MATLAB tool and the respective results are also obtained and compared comprehensively. Finally, the conclusion and future scope as well as future aspects of the work are discussed in Chapter 6.
CHAPTER 2

LITERATURE SURVEY

2.1. WHAT IS MPEG?

The MPEG (Moving Pictures Expert Group) had initiated in 1988 named as Working Group 11, Subcommittee 29, of ISO/IEC JTC11 holding the target to define those standards related to compression of audio signals and video signals in digital format. The basis taken by it was the videoconferencing and video-telephony ITU-T2 standard, along with that of the Joint Photographic Experts Group (JPEG). Compression of still images like that of electronic photography had been the defined initial work, task and target for JPEG. The MPEG is said to be a generic standard. It is being designed to support a diverse multimedia application range involving video telephony and video conferencing. A toolkit manner approach is followed by MPEG standard in order to solve the problem of being generic causing havoc due to large number of applications being supported by the same standard that is basic in nature. [1]

Defining an algorithm of coding of the video bit streams for Digital Storage Media, especially CD-ROM is described as the primary motive of MPEG standard. The standard obtained as the resultant one is showed to be comprised of three basic or intuitive parts. This includesthe coverage of the aspects of the systems i.e. (multiplexing and synchronization), video coding and audio coding. [1]

Surprisingly, it is vital and imperative to point out that a restriction is involved in MPEG-1 regarding the video formats. It could be used for non-interlaced video formats and supports for rate of bits streams up to around 1.5 Mbit/s in the format of video. Only specification of the semantics and syntax is done. Theprocess of coding is not specified at all: this is left primarily to the disposition of the coder’s designers. This provides aspect for improvement since refinement of the techniques of coding is done and development of new techniques occur inherently. Before transmission occurs, an operation of video bit-rate reduction also termed as “compression” takes place with the removal of less important or unimportant information from the signal and also by doing reconstruction task of an approximate image. This is done from the data that has remained in the decoder system. In video signals, we identified three types of redundancies that are unique and not similar to each other in any
ways. They are: Spatial and temporal redundancy, entropy redundancy and psycho-visual redundancy.[1]

2.1.1. Picture types

The kind of picture used significantly tells about the prediction mode that is being utilized for coding each of the macro blocks:

2.1.1.1. Intra pictures (or I-pictures)

Coding of this picture type is done without any reference to any other picture types. By spatial redundancy type reduction only and not redundancy caused temporally, the compression that is moderately achieved is gained. Since I-pictures provide the points of accessibility lying in the bit-stream they are quite important. These are the points where without any reference to past pictures decoding can be begun without any distortion.[1]

2.1.1.2. Predictive pictures (or P-pictures)

Coding of this picture type is done with the use in prediction of motion-compensation type with the help of previous I-pictures or P-pictures. Further, it could be utilized in the form of referential value in the upcoming predictions. By helping to reduce spatial as well as temporal redundancy, the P-picture-type allows greater compressibility in comparison to those I-picture types.[1]

2.1.1.3. Bi-directionally Predictive pictures (or B-pictures)

These picture types make usage of both the last passed as well as next intra or predictive-frame type having the purpose of compensating the motion. That’s why maximum degree of compression is offered. Above we saw that to allow backward prediction from the next (forward) frame, the rearrangement of those pictures from the original display order to those picture of a transmission (or bit stream) order is made sequentially. This is done so that the transmission of the bidirectional-picture-type could be done henceforth the last gone and upcoming frames that this provides referential for. Introduction of time-delay takes place which is determined by the count of B-pictures that occur in a consecutive manner.[1]
2.1.2. GOP (Group of Pictures)

Group of Pictures or GOP is defined to be the one formed with the occurrence of varied types of picture organized in a sequential manner may be repetitive in nature. [1]

![MPEG-1 Bit Stream Hierarchy](image)

**Figure 2.1:** MPEG-1 Bit Stream Hierarchy

2.2. BASICS OF MPEG VIDEO COMPRESSION ALGORITHMS

Generally, a significant amount of redundancies are found within and between frames in video sequences. Reducing the rate of bits flowing in bothspace and during transversal is the ultimate goal of video sourcecoding. It is done by finding both redundancies i.e. statistical redundancies and subjective redundancies and by using entropy coding techniques, where a "minimum set" of information is encoded. The implementation of methods of compressibility of any video is thoroughly dependent on the quality of redundant data held in the video stream and also the original compression techniques at the time to code. [2]

Depending on requirements of the applications there are two types of coding. They are lossless coding and lossy coding. With retention of original video quality lossless coding aims for reduction in image data or video data for storage as well as for transmission. The quality of the image that is decoded must be identical to the quality of image before it was encoded, whereas the goal of lossy- type techniques in coding being specified is to reach a defined bit-rate as the target, for storage and transmission purpose. [2][3][4]
2.3. THE SOURCE MODEL FOR MPEG VIDEO CODER

Generally speaking, redundancies of statistical origin or type tend to occur in sequences of a video in temporal as well as directions in space form. So, it is thought that the value of specific pixels in image could easily be predicated from the close by pixels in the exact picture. These techniques are called Intra-frame coding techniques. If the same is done from pixels of a nearby frame then the techniques are called as the inter-frame techniques. It is elaborately given that in few situations the scenario changes. As in changing scenes of sequences of a specific video, it is observed that the correlation occurring temporally between pixels in close by pictures is quite smaller in size or also vanishes – then what the pictured scene in video does is that it then starts assembling together the collection of images that are still and not correlated in nature. In this situation, the Intra-frame coding techniques are suitable for correlation of spatial type exploration to gain efficiency in compression of data. If so ever, the correction among pixels found within the close by pictures (or frames) is high. That is in those instances where two pictures (or frames) occurring consecutively have identical or similar content, it is desirable enough to make usage of such a technique that employs prediction temporally also called to be motion-compensated prediction between pictures (or frames). These techniques are known as Inter-frame DPCM coding techniques. High data compression could be achieved with the help of combining adaptively the MPEG video coding methods. This is termed as DPCM/DCT-hybrid video coding.

2.4. SUBSAMPLING AND INTERPOLATION IN MPEG

Near about all the techniques used for coding of video mentioned, make large-scale usage of subject and quick before the process to encode. Reduction in dimension of the input video and before encoding process begins the count of pixels to be coded is the primary concept. The video dimensions could be horizontal or vertical in nature. It is important to note that in few or many multimedia applications subsampling of the videos is being done in the timely way. Too for reduction of the frame’s rating before encoding and decoding is the path of perseverance in the mpg files, avi files, dat files. On the opposite or the decoder’s side, the images that are decoded are functioned with interpolation for displaying purpose. Defined as one of those that are highest rudimentary technique of compressibility, it is vitally stored to hold the comprehensible images in the source path of subsampling. This is because it too
provides usage in those particular features in the eye of a human-being that are physiological in type and nature, thus removing redundancies of subjective type present in the video data. It is observed that sensitivity towards variation in brightness is higher than the sensitivity towards variation in chromaticity of the human eye. Consequently, first division of the pictures into YUV components (one component of luminance and two components of chrominance) is done by the MPEG coding techniques. Then, the components of chrominance are subsampled with relativity to the component of luminance with a Y:U:V ratio that are well-defined and distinct to applications particularly.[2][3][4]

Figure 2.2: Motion Compensated Interpolation
2.5. MOTION COMPENSATED PREDICTION

The most impressive quality about Motion-compensated prediction is that it allows for reduction in those redundancies related with time occurring among the pictures and they are utilized as a technique of prediction, in an extensive manner in standards associated with coding of the video sequences in the format of MPEG-1 and MPEG-2 for temporal DPCM coding. The motion estimation calculated between the pictures (or frames) is the basic idea of motion-compensation. If all the parts in a sequential video scene have spatial displacement in approximation, the requisite movement among frames could be explained by the count of parameters of motion limited in nature. This can also be said to be done by the motion vectors for motion of smallest unit of block’s motion in translation. In this example, a motion compensated prediction pixel from a previously coded frame gives the best prediction of an actual pixel. Usually, both the calculated error of prediction along with motion vectors, are being sent towards decoder in the receiving end. However, single motion information encoded with each of the image pixel already coded is generally neither necessary nor desirable. As a result, separation of images is usually done to convert into blocks of pixels that are not joined in nature then, just a single motion vector’s thorough calculation is done, encoded and transmission finally having these blocks as shown in the figure 2.4 takes place. [2][3][4]
2.6. TRANSFORM DOMAIN CODING

For still image coding and video coding, transform coding has turned as a very popular compression method. De-correlation of Intra-frame or Inter-frame image data with errors and encoding of transform-coefficients are the defined goals of the Transform Coding instead of using the exact actual pixels of the images. In order to achieve this target, the images provided as input are broken into blocks of pixels that are not joined in nature.

A primaryaim related to the transformation coding has been in making quite lot of Transform coefficients negligible in order to possibly be done by making them smaller in size that are enough to do so. This property was measured as the statistics values or the measures of subjects and not as the general values. It is not at all necessary to code for transmission purpose. Moreover, minimization of dependence elements of statistics’ origin among them having target of having reduced quantity in binary required the encoding process for the remaining of them is desirable. Most top-left parts called as lower DCT coefficients has concentration of most significant DCT coefficients and increased distance decays the coefficients’ significance. It can be concluded that for the reconstructing of images the importance of higher DCT coefficients is quite less than that of the lower coefficients i.e. in comparison.

There are two major elements in the coding standards of MPEG formats. These techniques could be named as the prediction values of the motion compensation with time aspects and the other one is the coding in the transformed domain. These two features combine and form a collaboration that are really essential during the time of encode. Another feature relevant with the MPEG algorithms is that the processing of these both methods is done on image blocks of smaller in size. [2][3][4]

2.7. OVERVIEW OF MPEG-1

Covering vast multimedia devices starting from interaction-friendlymachines on the CD-ROMs to the requisite reach of thesequential video on networks of communication, compression technique for the video developed by MPEG-1 is a boon. In order to allow the huge applicable portfolios’ range quite wide diverse points of requisite parts as inputcan
besuggested by the user. In fact, according to a recommendation made by MPEG, every MPEG-1 decoder with compatibility feature should pursue the ability for providing assistance to a minimum of parameters of sources of video up on the structure of the television. [3][2][4]

Also, in order to make implementations supporting both these standards plausible, we made to sought in having common points of interference and calculations permissible in all the formats of the required containers of CCITT H.261 standard. How so ever, MPEG-1’s major goal was towards achieving successful gains for applications of CD-ROM in multimedia format only, with requirement of additional functionalities being in support of both the encoder as well as the decoder. The most significant features provided by MPEG-1 includes fast-forward (FF) type search or even fast-reverse (FR) type search throughout the bits in compressed form, video being accessed randomly, video being played in the reversed direction and ability of editing of the bit stream in compressed form. [3]

2.7.1. The MPEG-1 Inter-Frame Coding Scheme

The generic MPEG-1 video compression method is on a Macro block structure’s basis, the motion compensation’s basis and the conditional replenishment’s basis of macro blocks. With illustration in Figure 4(A), coding method of the MPEG-1 starts to encode the very initial picture in a sequential video in I-picture also called as intra-frame coding method. Every consecutive picture has to be in P-pictures coding method or inter-frame prediction -the information that is closest last or past picture I-picture or P-picture having predicted. Thus, the algorithm of MPEG-1 helps in processing the video sequence pictures in a manner which is based on blocks. All and every color picture provided as input picture in a sequential video has been divided to form those macro blocks that do not overlap with each other or any other picture. It is illustrated in the Figure 4(B). Every single macro block holds packs made from data from both the luminance and the co-sited chrominance bands - four luminance blocks i.e. (Y₁, Y₂, Y₃, Y₄) and two chrominance blocks i.e. (U, V), each with size 8 x 8 pixels. Hence the sampling ratio that is being recorded through calculations in middle of the pixels of luminance of Y:U:V and that of the pixels of chrominance is 4:1:1. [3]
Figure 2.5: (A) I-pictures (I) and P-pictures (P) in a sequence of video. Coding of predictive-pictures is done with the usage of motion-compensated-prediction that is dependent on the closest past frame. Every single frame is partitioned into not joined macro blocks.

(B) With each macro block, the data relevant to four blocks of luminance i.e. \( Y_1, Y_2, Y_3 \) and \( Y_4 \) and two blocks of chrominance i.e., U and V are coded. Every single block consists of 8x8 pixels.

Figure 2.6 highlights the block picture where the DPCM/DCT in hybrid forms of MPEG-1 encoders as well as decoders structures. The intra-mode method is applied by I-picture as its encoding is done with no referencing towards any previous picture or upcoming picture. On the encoder’s side, application of the DCT is done in every single block of the 8x8 chrominance and luminance blocks. After the resultant DCT’s output, each of the sixty-four DCT coefficients are provided with quantization all over properly in a uniformed way. The quantizer step size used in quantization of the DCT-coefficients within a macro block is sent to the decoder’s region on the other end. After quantizing it, the DCT coefficient with the smallest value called the DC coefficient is dealt in a varied style from the other coefficients that are remained called the coefficients of AC direction. Figure 2.5 depicts the zig-zag scanning concept. [3]
This functionality provides for an integral quality that the algorithm to code MPEG-1 supports to update the result. This result is obtained by clearly verifying which macro block has changed in comparison to the same data that is available from the last coded frame in the GOP and the sequence of video is thoroughly examined by the encoder for the replenishing purpose. If the prediction modes are completely providing suitability to the encoder then its efficient working is determined which clearly analyses the future picture group held in the macro block.

Also the human eye is more sensitive towards the Y block and less of the catching blocks. These components are gained after converting the color code format image into the holding format image to get better results of vision. The amount of data is large in the network transmission. Hence we require the data to be compressed and reduce the spatial as well as temporal redundancies caused due to the smooth flow of video.
Figure 2.7: Performing "zig-zag" scan within an 8x8 block of those DCT coefficients that are having quantization values. Encoding is done of those quantized DCT-coefficients with values not equal to zero only. The figure also depicts the probable places for DCT-coefficients that are of non-zero value. The aim of this scanning method is the tracing of the DCT-coefficients in accordance with the importance they hold.
FIGURE 2.8 (B)

FIGURE 2.8 (C)
2.7.2. Conditional Replenishment

This functionality provides for an integral quality that the algorithm to code MPEG-1 supports to update the result. This result is obtained by clearly verifying which macro block has changed in comparison to the same data that is available from the last coded frame in the GOP and the sequence of video is thoroughly examined by the encoder for the replenishing purpose. If the prediction modes are completely providing suitability to the encoder then its efficient working is determined which clearly analyses the future picture group held in the macro block. Also, the human eye is more sensitive towards the Y block and less of the CR Cb blocks. These components are gained after converting the RGB format image into the YCbCr format image to get better results of vision. The amount of data is large in the network transmission. Hence we require the data to be compressed and reduce the spatial as well as temporal redundancies caused due to the smooth flow of video. [3]

2.7.3. Functionalities for Storage Media

Important storage media functionalities like randomly accessibility of any video sequence and FF and FR playing of video functionalities are supported with the use of compression...
algorithm of MPEG-1. This was done in order to incorporate the requirements for specific storage media and to further examine the advantages of motion compensation and motion interpolations that are significant. This concept is well depicted in the given figure (Figure 2.9) for a GOP i.e. group of pictures arranged in a video sequence consecutively. As already discussed in Figure 2.5, 3 types of frames are assumed: Coding of Intra-pictures or (I-pictures) is done with no reference to any other picture present at any sequential video. For randomly accessing and FF/FR featured functionalities in the bit-stream, the I-pictures allow access points but very less compressibility is achieved. P-pictures, typically coded with the referential theme of the closest past encoded in any other picture type than the B one does, normally increasing coding efficiency by incorporating motion compensation. P-pictures provide for none of the suitability of the accessibility places or locations for randomly accessibility functionalities or edit ability as they are normally used in referential theme for predicting of next or previous pictures. B-pictures require both to find out the results in a clear cut manner approach. Zeal for the gain of compressibility in larger extent, on the basis of the closest past and future P-pictures or I-pictures motion-compensation can be employed. Also, B-picture itself is nowhere and not ever used as any reference.

![Diagram of MPEG-1 GOP](image)

**Figure 2.9:** I-pictures (I), P-pictures (P) and B-pictures (B) in an MPEG-1 video sequence.[3]

To suit diverse applications requirements, the types of frames in a sequential video could be arranged by the user with a flexibility degree of greater extent. Allowing for the largest
amount of randomly accessing the video, FF/FR features of a video and edit-ability, a sequential video coded using I-frames only (I IIII ...) is known to achieve lower degree of compression. Moderate compression amount could be achieved with a video sequence coded with a regular I-frame update and no B-frames (i.e. I P PPPPP I P PPP ...) but only a certain amount of randomly accessing and FF/FR featured functionalities is available to this. Embodiment of all these three frame types, may gain higher degree of compression and adequate randomly accessibility feature and FF/FR featured functionalities but also adds the delay in coding appreciably. No doubt, this late occurrence in time may prove to be intolerable in the applications of video-telephony or videoconferencing applications.[3]

2.7.4. MPEG-1 Rate Control

With the integral characteristic assisted by algorithms related with encoding of MPEG-1 is the possibility to attune the bitrate to the requirements of specified applications by quantizer stepsize (sz) adjustment for quantizing the DCT coefficients.

The cause of this control of rate is because, in general, the consecutive data in video pictures is variable. With the aim to avoid reconstruction errors the encoders and decoders of MPEG believe in implementation of the buffers having exactly the same size.

In theory, by using a large enough video buffers, overflow of buffers can always be avoided.

But, for reducing the time or complexities of the encoder system, a possibility to make choice of buffers is made in such a way that it is integrated virtually. That means there is no actual buffer but only a virtual one is restored In order to get the thorough rating of the system. This will no doubt increase the quality of the mechanism of controlling the rate immensely.[3]

2.7.5. Coding of Interlaced Video Sources

The format of standard video input for MPEG-1 is not in the form of interlaced format. However, it is difficult to believe that coding of interlaced color television with both 525 and 625 lines at 29.97 and 25 frames per second respectively is an imperative application for the MPEG-1 standard. Fundamentally, encoding of only a single subsampled field of horizontal behavior of each and every interlaced video input frame is done. This is called the subsampled top field. At the receiver’s end, the prediction of even field is made from the odd field that is in decoded form and also interpolated form for the purpose of display. [5][3]
Figure 2.10: Motion Compensation in Real Life example

<table>
<thead>
<tr>
<th>PARAMETERS</th>
<th>MPEG-1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standardized</td>
<td>1992</td>
</tr>
<tr>
<td>Main Application</td>
<td>Digital video on CD-ROM</td>
</tr>
<tr>
<td>Spatial Resolution</td>
<td>CIF Format(1/4 TV)</td>
</tr>
<tr>
<td></td>
<td>approx. 288 x360 pixels</td>
</tr>
<tr>
<td>Temporal Resolution</td>
<td>25-30 frames/sec</td>
</tr>
<tr>
<td>Bit Rate</td>
<td>1.5 Mbit/s</td>
</tr>
<tr>
<td>Quality</td>
<td>Comparable to VHS</td>
</tr>
<tr>
<td>Compression ratio over PCM</td>
<td>approx. 20-30</td>
</tr>
</tbody>
</table>
CHAPTER 3

RELATED WORKS WITH VIDEO ENCRYPTION

Data is considered as stream of bits and DES is used for encrypting the data in most of the multimedia data scrambling systems. However, the sow implementation of the DES does not meet the requirements of the video playbacks of MPEG. The solution for its particular drawback is the selective encryption of the portions of the MPEG video.

3.1. SELECTIVE VIDEO ENCRYPTION METHODS

3.1.1. Encrypting MPEG Video Headers

One method for encrypting the MPEG video defines for the encryption of header of the video in MPEG format that is being included in it, GOP headers, slice headers, macro-block headers, figure 2.1. But this method is not effective because of the following reasons:

The very first cause is obvious because all the information that is standardized in nature are contained in the header part which is easier for the attacker to guess this information.

The second reason is that the frames in the MPEG applications are synchronized and ordered; so that the starting of each frame is known.

The third reason is that at the time of transmission on the noisy channel, the bits in the header may propagate errors and this error in one encrypted block can be infused in the whole block of bits. Hence, the synchronization of the video may be lost.

3.1.2. Encrypting I-Frames Only

The other method for selective encryption is to do the encrypting task part in only the I-frames. It is believed that without the reference to the consequent I frames, the P and B frames are of no use. Although, in reality, few Predicted and Bidirectional frames consists or holds in it the I blocks of coded form, so because of this a large amount of the MPEG video is viewable even when no Intra type frames are available. Hence, encrypting just the I frames does not give a secure option for encoding.
3.1.3. Encrypting Headers Plus DC or AC Coefficients

Various other types of encryption techniques used for encrypting the MPEG video are the following:

- All headers along with the DCs and the lower ACs terms can be encrypted
- Using two algorithms for encryption; i.e., encrypting the first half with the DES/IDEA and encrypting the other half with the “one-time-pad” generated from that frame.

In the systems that support such type of encryption techniques, the compression of MPEG video is done first and then the video is encrypted. While the decompression operation is done first and then the video is decrypted. Hence, these types of systems increase the processing of the decoding process of the video and also increase the latency in the real-time video delivery.

3.1.4. Tang’s Algorithm

In the Tang’s algorithm, Tang found out a method to combine together the methods of encryption and compression in MPEG format using a single action only. This method has replaced the Zigzag order with the random permutation list for mapping the DCT coefficient to just a single vector of matrix 1 x 64 vector. The computational complexity to map in accordance with the list of values to permute randomly is done. And the given zigzag order is exact as before hence processing (for encrypting and decrypting) is very less for both the compressed video and decompressed video procedures but the Tang’s method the arte of compressing video streams which is the serious drawback of this algorithm. The reason behind the reduced compression rate is that the probability distribution of the DCT confidents is distorted by the random permutation and the table of Huffman code words is in usage with more than enough amount.

3.1.5. VEA ByQiao and Nahrstedt

Another algorithm proposed in the field of encryption of video is the VEA. Its working is based on two points that are important. These two points includes: properties related with the statistics of the standardization of MPEG video and the requisite standardization of symmetric...
key algorithm as suggested by QiaoAndNahrstedt. This algorithm helps in reducing and making the encryption done data small. The basic formula of Video encryption Algorithm is that it divides the entire stream of video bits into smaller parts i.e. (c1, c2, c3, c4,..., c2n-1, c2n) and these small-small parts are further partitioned into two data divisions. First list is of parts having odd values (c1,c3,c5,...,c2n-1) and the second list is of even values (c2,c4,c6,...,c2n). After this deviation process, key to encrypt the even list is being applied. The E(c2, c4, c6, ..., c2n) is the function for even segment, where we have E as a function to encrypt. Finally, the cipher text retrieved is collaborated with that of the algorithm for encryption and then XOR’s output against the chunk list of odd value data. Since the key will change every time for each frame in VEA algorithm, hence it is save from known plaintext attack.

3.2. CONCLUSION

Tremendous amount of work is being done in selective encryption methods. This is because it is always easier to encrypt only few requisite parts instead of applying encryption to the whole video data stream or bit streams. Also the data in video is very large and if we encrypt the whole data it is not wise moreover, it consumes a lot of time and energy as well. Researchers deeply studied various selective encryption methods for image data and video bit streams. Finally they concluded that work which has been done using these algorithms is promising and abundant still there are a lot of improvements can be done in this works. The lack of an integral key management system is one of the sensed shortcomings.[9]
CHAPTER 4

TECHNICAL REVIEW

4.1. ALGORITHM-I

Bharagava, Shi, and Wang were the founders of the four varied video encryption algorithms named Algorithm-I, Algorithm-II (VEA), Algorithm-III (MVEA), and Algorithm-IV (RVEA).

First algorithm makes use of the permutation of Huffman code words in I-frames. This algorithm assimilates encryption as well as compression in a single procedure. The permutation p is the secret part of the algorithm. This secret part is extensively used in permuting the standardized MPEG Huffman code word list. Hence, in order to save the ratio of compression, only those code words having exact bit count should be permuted. This can be done only by selecting the permutation p to such that it does so. Daniel Socek showed that this algorithm has higher vulnerability towards both known-plaintext attack, and cipher-text-only attack. The attacker could possibly sense and cause reconstruction of the permutation p that is kept secret, only if some of the video frames are known in advance. This can be done by analysing and creating a comparison between the frames that are known and the frames that are having encryption done on it.

However, the first algorithm is also vulnerable to cipher text-only attack, but there is low frequency error attack on Algorithm-I cipher text. Basically, since permutation p is of the special form i.e., it only shuffles the code words with the same length. Most security appears from shuffling 16-bit code words in the AC coefficient entropy table. However, since there are very limited numbers of code words with length of less than 16 bits, it is very easy to reconstruct all of the DC coefficients and most frequent AC coefficients (since these will be encoded with less than 16-bit code words). Hence in other words, the only tough part would be to outline how the 16-bit code words are shuffled by the permutation p. But the video that is just in reconstruction phase video might resemble the same quality as the real one because figuring out shuffling criteria is extremely rare to occur.[16][17]
Figure 4.1: Algorithm-I Huffman permuted coder

4.2. ALGORITHM II (VEA)

We know that the most integral information about the MPEG video is carried along by I-frames. Thus, encrypting only the necessary sign bits of the DC coefficients of the blocks of I frames is done by simply XOR-ing them with an m-bit binary key, $k=k_1k_2...k_m$ that is secretly buildin this algorithm. Randomly changing of the sign-bit of the DC coefficients of an MPEG video stream which happens to belong to the same GOP of $w_1w_2...w_n$ combined in a function is the intrinsic effect seen after applying the aforementioned technique to encrypt.

When 0 is the found value of the key bit $k_i$ (mod m), a wi bit will remain unchanged. The same value will be in a state of flipping if the found out value of the key bit $k_i$ (mod m) is calculated as 1. Ultimately, reusability of the secret key would be done by the upcoming GOP. This helps in resynchronizing of the values. The resynchronization capability for bit streams of video is required in the case of transmission errors. They are rewinding, and the opposite. The level of secure transmission of this scheme is dependent vitally on the usingkey’s length. The writers provide for the knowledge that a binary-key long enough should be used. But, key with quite large size might prove impractical as well as infeasible. But, using a key with small size, the breakage of any system might take place and could be easily turned down.
When stream of video and the size of the key is same and also is specific and only one and is being used at most one-time then that is in correspondence to Vernam cipher that is also known with the name of one-time pad. This cipher provides complete security. But, it is not possible practically done for applications of the mass media like services of Video on Demand and other like applications. Although, when the size of the key is quite small, the complete technique is simplified to known as Vigenere-like cipher.

A lot many attacks are being developed for this well-researched ancient cipher. Additionally, Vigenere is highly sustainable to the plain-text attack. Anybody can just literally read the secret key. Writers suggest the usage of the pseudo-random generator that creates a stream of pseudo-random bits that is ought to be the key k of any selected size. The problems related to this method are the problem to be secure, to be random, and the speed of this P-RNG (Pseudo-Random Number Generator). In addition, the other issue regarding this generator is how to synchronize the P-RNG and the transmission of the secret key must be secure. [16][17][7]

4.3. ALGORITHM-III (MVEA)

A lot of advancement has been incorporated into the Algorithm-II (VEA). The sign bits of the differential values of DC coefficient as well as motion vectors in P-frames and B-frames be encrypted using XORs using the confidential key, in-place of encrypting just the sign bits of DC coefficient in I-frame block. Such kind of enhancement makes a video playback further much random as well as much more non-viewable.

The position of the motion vector gets altered as soon as the sign bits of the differential values of the motion vector are altered. Along with this there is also a observable alteration in the magnitude of the motion vector which makes or leads to creation of the entire video being a lot chaotic or hectic. It has also been found during studies that the encryption of sign bits of motion vectors causes to the encryption of sign bits of DCT coefficient in B- as well as P-frames useless or to say redundant.

Further, the Algorithm-III (MVEA) was made in order of encrypting only the sign bits of DC coefficients in the I-pictures of sequence of video in MPEG standard, although it leaves the coefficients of AC not encrypted. Doing this makes an increment in risks factors of secure transmission but with significance it deteriorates the overhead of computation. Namely, because the DC coefficient and the sum of all AC coefficients within the block are related, an
attacker might make usage of the non-encrypted AC coefficients to make out the unknown DC coefficients that are already in encrypted form. For this treason, any of the application the authors recommend encrypting all DCT coefficients in the I-frames for applications that need higher level of security. However this type of improvement makes the video playback more random and more obscure (nonvisual). With similar conduct of VEA, this algorithm, i.e. MVEA is dependent on the size related with the secret key.[7][16][17]

The Algorithm III is an improvement to the Algorithm II explained in the aforementioned paragraph.

The Algorithm-III (MVEA) heavily relies on the m-bit secret key, k just the same is done in the the Algorithm-II (VEA). Moreover, the task of resynchronizing the bits of key is done just in the starting of any GOP. Unluckily, the basic issues related with secure transmission relevant to VEA are again also applicable to MVEA.[7]

4.4. ALGORITHM-IV (RVEA)

The concept of Algorithm-IV (RVEA) was recommended by Bhargava, and el. The difference between Algorithm-IV (RVEA) and that to Algorithm-III (MVEA) is that Algorithm-IV (RVEA) makes use of a traditional symmetric key cryptography for encrypting the sign bits of DCT coefficient and the sign bits of motion vectors. The process of encryption is speeded up by the algorithm by only encrypting definite or specific sign bits in MPEG stream. Henceforth we can very well say that this particular algorithm is far superior in comparison to the previous mentioned three algorithms that is to say Algorithm-I, Algorithm-II (VEA), and Algorithm-III (MVEA) in parlance of security. In the Algorithm-IV (RVEA), the sign bits of DCT coefficients and motion vectors are merely pulled out from the MPEG video sequence, and encrypted by means of a fast conventional cryptosystem such as AES, and after this it is then reinstated back to its original position in the encrypted form. The outcome of this is alike to VEA/MVEA whereby the sign bits are made to either reverse or left as it is without making any changes. The number of bits for encryption is restricted to at most 64 by the authors, for each MPEG stream macro block, with the vital and ultimate intention of plummeting and bounding the time taken for computation. Subsequent, we define exactly as to how these sign bits are carefully chosen for encryption.[7][16][17]

4.4.1. Bit Selection Order in RVEA
Every MPEG video slice is comprised of a single or several macro blocks. The macro block resembles to a 16x16 pixel square, which is made up of four 8x8 pixel luminance blocks indicated by Y1,Y2,Y3,Y4, and a couple of 8x8 chrominance blocks Cb and Cr. Every single of these six 8x8 blocks can be represented as a sequence i.e. ba1a2...an, where n can be to a maximum of 64 since b is the code for DC coefficient and ai is the code for a non-zero AC coefficient. That means, for every such 8x8 block, the order or sequence can be represented as βa1a2...an, which is corresponding to the sign bits of the identical DCT coefficients b, a1,a2,...and an. [7][16]17

The sequence of the choosing of the sign bits for every macro block is represented by figure 4.2 and since the DC and the higher order AC coefficients are incorporating a quite more information than the low order AC coefficients, hence it is the apparent motive behind the choosing of the sequence.

The aim of diminishing and binding the computation time is accomplished by RVEA by limiting the maximum quantity of bits selected. The decryption procedure of RVEA is the same as it is in the encryption procedures.
A very astounding transformation in the decoded frame can be achieved by altering the sign bits of DC coefficients of I frame and as DC coefficients of I frames are encoded in a different manner, so altering with the sign bit of a differential value will cause an impact on all the succeeding DC coefficients in the course of MPEG decoding.[7][16][17]

### 4.4.2 Security in RVEA

The difficulty in salvaging RVEA encrypted video has been escalated by the differential encoding of DC coefficients and motion vectors in MPEG compression. If an initial supposition of a DC coefficient is made incorrectly, then it becomes very difficult to make a supposition regarding the following DC values in a correct manner.

In principle, the problem faced in salvaging up of an RVEA encrypted Mpeg video is as
similar as to the toughness in salvaging the underlining secret key cryptography algorithm. As of now there is no known feasible method for finding out or ascertaining the secret key in DES or IDEA, even if the plaintext and cipher-text is available. It is worth to be noted that the price of plaintext attack to RVEA is amplified by the MPEG decoding procedure which also comprises of the costly IDCT computations.

It is also not feasible as to Cipher-text attack to be made on RVEA encrypted MPEG video. Cipher-text attack on RVEA can only be carried out by the trial and error method whereby all likely amalgamations of the sign bits of assign bits of a frame are tried and its is observed to see if any of the amalgamations of the sign bits is in the position to produce a understandable video frame.

An attack of correlation is made very tough by virtue of the de-correlative characteristic of AC coefficients of DCT. An automatic cipher-text attack i.e. dissemination of secret key or the generation of superior pictures in absence of human participation is difficult even with help of the most potent computer systems as the computers are not aware of the fact as to that if a supposed picture is understandable to humans. A few blurred pictures can be captured or some objects be found out in a few frames by a chipper-text attack having the interference of human being, by frolicking with picture puzzles of flipping sign bits. The process is time consuming and shall consume a lot of time for the attacker to achieve a blurred image. Any person who finds the image thought-provoking and of interest will prefer to purchase the video rather than attacking the ciphered video as the price of purchasing the program is indeed much economical. RVEA just categorically encrypts a fraction of the entire video. It much time-saving process than encrypting the entire video with DES/IDEA. It has been observed that in an ideal MPEG video, fewer than 10 per cent of the entire video bit stream is constituted of sign bits. Henceforth, RVEA saves about 90 per cent of the encryption duration as compared to algorithms encrypting the entire video. RVEA encrypts to a maximum of 64 bits or 8 bytes for every macro block. [7][16][17]

Thus, encryption calculations are substantially lowered by it. E.g., in a 320 × 240 video frame, there is a presence of 20 × 15 macro blocks in every frame.
In order to carry out processing of 30 frames per second, RVEA requires encrypting the data at a rate of $20 \times 15 \times 30 \times 8$ bytes per second, which is around 72 Kb/sec.

As we must here understand that the application of RVEA encryption to a unit of videoslice means that the progression of decryption can initiate only when the entire slice is existing; and a definite quantity of time delay can be found due to the decryption process succeeded by sign correction. In spite of these, RVEA is quite quicker in comparison of other methods that encrypt the entire video frame due to the basic reason that the duration spent in encryption calculation is quite higher than the communication gap. [7][16][17]

**4.4.3. QoS Guarantee in RVEA**

In order to ensure QoS also called Quality of Service for real-time video applications, what is essential is that the duration taken for encryption or decryption must be restricted by a constant and the process of encryption and decryption must not consume a lot of time, or else the video session shall get affected with jitters. The same is specifically true to the MPEG video applications since MPEG video frame sizes differ in duration, which can be seen in Figure 4.3.

The encryption duration taken by the algorithms that encrypt the entire frame varies...
depending on the frame size. More time is taken for encryption in case of bigger frame size which in turn causes further time delay. The effect of this can be seen either in the form of either a poor video playback or an additional load may be added to the video frame synchronization. However the encryption speed of RVEA is not altered by virtue of burstiness of data. Irrespective of the fact as to how big a frame size is or of what type it is (I, P, or B) (see Figure 4.4), RVEA encrypts to a maximum of 64 bits or 8 bytes of data for every macro block. This is the most important and desired characteristic of video decoding.

Figure 4.4 RVEA encryption time for each frame is bounded.
To conclude, only a portion of the entire MPEG video which is generally around 10 per cent, is encrypted by RVEA, by the means of conventional secure cryptographic systems like DES, IDEA, AES to name a few. Hence it can be rightly said that the Algorithm IV (RVEA) is an much advanced and convenient process in comparison of the other mentioned algorithms in terms of security. Moreover it makes a preservation of about 90 per cent of the duration taken for computation as compared to conventional approach. [7]

Figure 4.5: Misleaded macro block in RVEA
Table 4.1: Video Encryption Algorithms Comparison

<table>
<thead>
<tr>
<th>FREQUENCY DOMAIN</th>
<th>Algorithm Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Meyer &amp; Gadegast, 1995 [18]</td>
<td>DES, RSA, Headers, parts of I-blocks, all I-blocks, I-frames of the MPEG stream</td>
</tr>
<tr>
<td>Spanos &amp; Maples, 1995 [19,20]</td>
<td>DES, I-frames, sequence headers and ISO end code of the MPEG stream</td>
</tr>
<tr>
<td>Qiao &amp; Nahavandi, 1997 [22]</td>
<td>xor, permutation, IDEA, Every other bit of the MPEG bit stream</td>
</tr>
<tr>
<td>Shi &amp; Bhargava, 1998 [23]</td>
<td>xor, Sign bit of DCT coefficients</td>
</tr>
<tr>
<td>Alattar, A-Regib and Al-Senari, 1999 [9]</td>
<td>DES, Every nth I-macroblock, headers of all the predicted macroblocks, header of every nth predicted macroblock</td>
</tr>
<tr>
<td>Cheng &amp; Li, 2000 [25]</td>
<td>No algorithm is specified, Pixel and set related significance information in the two highest pyramid levels of SPIHT in the residual error</td>
</tr>
<tr>
<td>Wen, Sevrea, Zeng, Luttrell &amp; Jin, 2002 [28]</td>
<td>DES, AES, The information-carrying fields, either fixed length code (FLC) codewords, or variable length code (VLC) codewords</td>
</tr>
<tr>
<td>Wu &amp; Mao, 2002 [35]</td>
<td>Any modem, Bitstream after entropy coding, quantized values before run length coding (RLC) or RLC symbols, intra bit-plane shuffling in MPEG-4 FGS</td>
</tr>
<tr>
<td>Wu &amp; Mao, 2002 [35]</td>
<td>Any modem cipher, random shuffling on bit-planes in MPEG-4 FGS</td>
</tr>
<tr>
<td>Spatial Cheng &amp; Li, 2000</td>
<td>No algorithm specified, Quadtree structure of motion vectors and quadtree structure of residual domain errors</td>
</tr>
<tr>
<td>Entropy coder: Wu &amp; Kuo, 2000 [26], Wu &amp; Kuo, 2001 [27]</td>
<td>Multiple codec tables, multiple state indices in the QM, Huffman Encryption of data by multiple Huffman coding tables and multiple state indices in the QM coder</td>
</tr>
</tbody>
</table>
CHAPTER 5
IMPLEMENTATION METHODOLOGY

5.1. EXPERIMENT 1: ANALYSIS TO CALCULATE THE ENCODING TIME USING VEA, MVEA and RVEA WITH CHANGING KEY LENGTH.

5.1.1 Execution of Experiment 1

Figure 5.1: Regular MPEG video

Figure 5.2: Encrypted sign-bits of motion-vectors
Figure 5.3: Algorithm II (VEA) – Sign-bits of DCT coefficients encrypted with fixed 64-bit key

Figure 5.4: Algorithm III (MVEA) - Encrypted sign bits of DCT coefficients and Motion Vectors with fixed 64-bit key

Figure 5.5: Algorithm II (VEA) – Sign-bits of DCT coefficients encrypted with fixed 127-bit key
Figure 5.6: Algorithm III (MVEA) – Sign-bits of DCT coefficients and Motion Vectors encrypted with fixed 127-bit key

Figure 5.7: Algorithm IV (RVEA) - Sign-bits of DCT-coefficients and motion-vectors encrypted with fixed 256-bit AES

5.1.2) Result

- This experiment caused a low motion video sequence to be encrypted with varied key lengths along with fast MPEG video encryption algorithms to test the encoding time.

- Hence the encryption time increased thus establishing a result that it could be used in those applications where security is more important than the encoding time overhead or vice versa with lesser key length the applications may use it for less encoding time and thus lesser complexity.
Table 5.1 Encoding time with varied key length

<table>
<thead>
<tr>
<th>ENCRYPTION ALGORITHM</th>
<th>SEQUENCE</th>
<th>ENCODING TIME</th>
</tr>
</thead>
<tbody>
<tr>
<td>No encryption algorithm</td>
<td>Low-motion</td>
<td>111 seconds</td>
</tr>
<tr>
<td>Algorithm-11 (VEA) with fixed 64-bit key</td>
<td>Low-motion</td>
<td>112 seconds</td>
</tr>
<tr>
<td>Algorithm-111 (MVEA) with fixed 64-bit key</td>
<td>Low-motion</td>
<td>112 seconds</td>
</tr>
<tr>
<td>Algorithm-11 (VEA) with fixed 127-bit key</td>
<td>Low-motion</td>
<td>126 seconds</td>
</tr>
<tr>
<td>Algorithm 111 (MVEA) with fixed 127-bit key</td>
<td>Low-motion</td>
<td>127 seconds</td>
</tr>
<tr>
<td>Algorithm 1V (RVEA) with 256-bit AFS</td>
<td>Low-motion</td>
<td>155 seconds</td>
</tr>
<tr>
<td>VEA with 256-bit AES</td>
<td>Low-motion</td>
<td>168 seconds</td>
</tr>
</tbody>
</table>

5.1.3) Conclusion

The encoding time increases with increase in key length as shown in Table III. Hence, selection of key must be made carefully in order to ensure secure transmission of video. The selection of key is a vital part in encryption because a key too long or short, both affects the working of the algorithm. Also, adversaries may compute values to generate obvious keys hence, key must be carefully selected as well as managed.
5.2) Experiment-2: Analysis of Algorithm-I, VEA, and MVEA algorithms proposed by Shi, Wang and Bhargava on MPEG video format using MATLAB

5.2.1) PURPOSE

The experiment is done with the purpose of testing the encrypted resultant video and then calculates the percentage of encryption, delay in playing video due to encryption and size of encrypted video.

5.2.2) Set-Up

We used MATLAB tool to perform this experiment.

5.2.3) Execution of Experiment-2

The input data is the "move.mpg" MPEG-1 video clip. It is first converted into frames and stored in a working directory.

![Video converted into frames](image)

*Figure 5.8: Video converted into frames (6 sample frames out of 29 frames)*

<table>
<thead>
<tr>
<th>Video Format</th>
<th>Original Video Size (S)</th>
<th>No. of frames prior encryption (N)</th>
<th>Original video playing time (T)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mpeg</td>
<td>640 KB</td>
<td>29 frames</td>
<td>1 second</td>
</tr>
</tbody>
</table>
Figure 5.9: Original video frame

5.2.3.1) Implementing ALGORITHM-I

- I-frame of the original mpeg video is depicted in the Figure 5.9. Huffman coding is implemented at I-frames.

- Using MATLAB function permutation of Huffman code words is taken along with symbol and probability calculation in I-frames.

- The code words having the exact amount of bits must only be permuted with p permutation

The figure 5.10 is the encrypted frame and is comprehensible.

Figure 5.10: Encrypted I-Frames with Algorithm-I

5.2.3.2) Implementing ALGORITHM-II (VEA)
RGB to gray scale conversion is done to apply encryption of scaling at the first step.

Simply sign-bits of the DC-coefficients in the I-frame blocks are X-OR with m-bit binary key to get encrypted DC-coefficients.

Encrypting all DC coefficients with VEA including DCs of Y block in loop causes resynchronization. A single frame of the output that is obtained as the result is shown in Figure 5.11. The video image is obscured, and is not comprehensible.

Figure 5.11: Encrypting DC-coefficients using VEA

5.2.3.2) Implementing ALGORITHM-III (MVEA)

The sign bits of the differential values of DC coefficient and motion vectors in P-frames and B-frames are encrypted by XORs them with the secret key making the video more random and non-viewable.

Figure 5.12 shows one of the MVEA motion vectors of type P frames and B frames. The picture is in pixel form.

Figure 5.13 illustrates one of the encrypted frames with MVEA. Every picture frame in the tests conducted using MVEA is obscured. Not a single one is readily viewable.
5.2.4 Results:

Table 5.3 Results Obtained After the analysis of experiment-2

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Encrypted Video Size(s)</th>
<th>No. of frames after encryption (n)</th>
<th>Time to play the encrypted video (t) (in sec)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Algorithm-I</td>
<td>27,000 KB</td>
<td>29 frames</td>
<td>3 seconds</td>
</tr>
<tr>
<td>VEA</td>
<td>1073 KB</td>
<td>29 frames</td>
<td>2 seconds</td>
</tr>
<tr>
<td>MVEA</td>
<td>27,000 KB</td>
<td>29 frames</td>
<td>3 seconds</td>
</tr>
</tbody>
</table>
- Encryption percentage can be calculated by subtracting the encrypted video size(s) with actual video size(S) and multiplying with 100 i.e. (s-S)/S * 100 %. Percentage of encryption has no unit as the units are cancelled while dividing with the same parameter.
- Delay is calculated by subtracting the encrypted video playing time (t) with the actual video playing time (T) i.e. (t-T) seconds.
- No. of frames is counted after encryption in order to check if there is any change in frame lengths. But no frame difference was observed in the experiment.
- Various advantages such as security performance is achieved and mentioned along with a few disadvantages associated with the algorithms due to key length management.
- The advantages help us to know whether this algorithm is suitable for the multimedia requirement in the day-to-day scenario. Applications such as video conferencing require speed as well as audio and video streams to be clear so as to fulfil the purpose of transmission hence here computation time for the algorithm 's encryption must be less and accurate
- Whereas the requirement in TV channel subscription where only the authenticated users are supposed to view the channel must be provided with the decrypted video and the non-authenticated ones must be either shown encrypted ones or not at all. The decryption is done with a key that is possible by providing a card number to the authenticated users through sms or email, etc.
- As the users enter the code, there channels are made visible to them. Hence the purpose is commercial and also security is well implemented even if the overhead is high.
- The final video can be any of the container formats but since we are working on MPEG it is converted back into the mpeg format from the other mentioned format in order to manage for integrity. This integrity is helpful in managing the fortified concepts of visual.
Table 5.4 Calculated Values of Parameters associated with mpeg video encryption

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Percentage of encryption</th>
<th>Delay due to encryption</th>
<th>Frames difference</th>
<th>Advantages</th>
<th>Drawbacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Algorithm- I</td>
<td>20.63%</td>
<td>0.2 seconds</td>
<td>0</td>
<td>Reconstructed video is the same</td>
<td>Cipher-text</td>
</tr>
<tr>
<td>VEA</td>
<td>60%</td>
<td>1 second</td>
<td>0</td>
<td>Resynchronization possible, Vernam cipher</td>
<td>Relies on secret key, Vernam cipher</td>
</tr>
<tr>
<td>MVEA</td>
<td>90%</td>
<td>2 seconds</td>
<td>0</td>
<td>Reduces computational overhead</td>
<td>Relies on secret key, security risk</td>
</tr>
</tbody>
</table>

Figure 5.14: Frames Obtained after encryption in motion vectors using MVEA.

- Finally these frames are looped together in a sequence to form the new encrypted video. The name of the encrypted video is termed as newvideo.mpg. This new video shows us tremendous changes in knowing how the vectors of motion are changed and how are they managed in terms of finding the proper flow of the encrypted video stream. The encrypted
video images or frames were clipped together to provide for this flow in managing the video to be seen.

- The final video can be any of the container format such as avi, dat, etc but since we are working on MPEG it is converted back into the mpeg format from the other mentioned format in order to manage for integrity. This integrity is helpful in managing the fortified concepts of visuality.

5.2.6) Conclusion

We know that in any encryption method or methodologies there is far more significance of the coefficients of DC than those of the AC coefficients. From the experiment, it was found that there is more significance of motion vectors than the various other DCT coefficients. At times when all the Y-blocks’ DC coefficients are encrypted, the level of satisfaction was good in terms of the results given by encryption. Around 1.81% of the time for computations is the relative time that is being spent on encryption i.e. lesser amount of time. So, as we implement VEA in software it is quite faster at least to provide security to the video applications of MPEG format. There is always some disadvantage associated with any method but how advantageous it is to the multimedia sector could be found out through the analysis done. Also key management is an important concern in these algorithms which might affect the encryption parameters.
6.1) CONCLUSION

Here, we have analyzed four MPEG video encryption algorithms. Experiments conducted showed the study with comparison of some algorithms encrypting selectively also highlighting the four video encryption algorithms proposed by Shi, Wang and Bhargava. This analysis could be served as a better criterion for choosing the suitable encryption techniques or algorithms of video in one way or the other.

The exploration of requirements associated with confidentiality through the selectively perceiving the encryption in various selective parts of the payload from any given stream of video. Quite good results were obtained by us when we saw in regard of the "scrambling" contents. The overhead that was required in the time of processing was around 1.8% in the second algorithm whereas the same data obtained with the application of RVEA for encryption at the time of compressing the bit streams was around 2.5%.

The analysis made will help greatly in multimedia applications as well as for security wherever required. The requirement in multimedia varies from one application to another such as video conferencing has different requirements than those of the pay-per-view users. This analysis thus, helps deciding the usage and necessity of any algorithm that might be of utmost relevance to one or the other multimedia applications.

6.2) FUTURE SCOPE

The algorithms that were used for the overall approach and experiment can achieve satisfactory results with less computation. Also, implementing them on the platform of software showed that they are quite fast in nature and performance in order to reach the requirement related to real time of MPEG decoding. It is believed that these algorithms could extensively be used on the path to provide security on video-on-demand applications and pay-per-view programs. It is possible to extend the ideas of these four algorithms to non-MPEG compression scheme such as H.263 for video-conferencing application.
Before selecting any algorithm to be used for encryption in multimedia application systems, a thorough analysis of the application must be done to know what level of security could be satisfying for it to work in a secure manner. Hence, a careful selection of an algorithm needs to be done after knowing the required security levels to be used. Choice of an algorithm will be affecting the speed of the coder-decoder-codec. Thus, it is vitally needed to do before any method is selected for encryption.

Perceptual encryption needs to be implemented for video-conferencing video telephony. Encryption at broadcast levels needs to be in place in the coming future where it would be possible to change the security level of applied algorithm at different users systems. This will not only save the users time and money but will also help the encoder to keep track of all kinds of requirements as well as the users perusal of any such service on the path of transmission. Though a lot of research is done and is still being done on multimedia security it is undoubtedly a vast topic to research and reinvent algorithms and crypto systems that would help the world entirely in the field of communication and technology.
REFERENCES


