An Open Access Journal Available Online

Survey of Video Encryption Algorithms

Babatunde A.N.[1], Jimoh, R.G.[2], Abikoye O.C.[3] & Isiaka B. Y.[4]

Department of Computer Science,
College of Information and Communication Technology,
Kwara State University, Malete, Nigeria.
[1]drealak@gmail.com
Department of Computer Science,
Faculty of Communication and Information Sciences,
University of Ilorin, Ilorin
[2]jimoh_rasheed@yahoo.com
Department of Computer Science,
Faculty of Communication and Information Sciences,
University of Ilorin, Ilorin
[3] Kemi_adeoye@yahoo.com
Department of Computer Science,
College of Information and Communication Technology,
Kwara State University, Malete, Nigeria.
[4]yabolaji4@gmail.com

Abstract: Research on security of digital video transmission and storage has been gaining attention from researchers in recent times because of its usage in various applications and transmission of sensitive information through the internet. This is as a result of the swift development in efficient video compression techniques and internet technologies. Encryption which is the widely used technique in securing video communication and storage secures video data in compressed formats. This paper presents a survey of some existing video encryption techniques with an explanation on the concept of video compression. The review which also explored the performance metrics used in the evaluation and comparison of the performance of video encryption algorithms is being believed to give readers a quick summary of some of the available encryption techniques.

Keywords: Encryption, Video Security, Performance Metric, Compression, Decompression.

1. Introduction

The security of video data is becoming more important nowadays because of the rapid development in multimedia video compression and the latest development in internet technologies. These breakthroughs have enabled video data to be used as a medium through which sensitive information can be easily stored and transmitted. Hence, video data needs to be protected from unauthorized access during the cause of transmission and storage. Video encryption is the widely established and secured means of video content protection (Ajay et al., 2013; Yogita, 2013; Darshana & Parvinder, 2012; John & Manimurugan, 2012; Mayank et al., 2012; Jolly & Saxena, 2011).

Traditional ciphers which are based on the theory of number (algebra concept) which are the Advanced Encryption Standard (AES) and Data Encryption Standard (DES). These two methods are most straight forward approaches to total video security. Majority of these encoders are utilized for text and binary data that is due to huge volume of data are not fit for multimedia data. Developing a cryptosystem for video data using these traditional ciphers incur significant overhead and expensiveness in actual time video systems such as video conferencing and digital image surveillance (Zhaopin et al., 2012). Also, considering the fact that consecutive frames bear close resemblance, it is likely that a subtle amount of pixels might change from one frame to another. Hence, there is high data tautology in continuous image data which can be removed to ensure that the big size of the video data is reduced for easy transmission and storage. This is the reason traditional ciphers muff viewable information. (Zhaopin et al., 2012; Furht et al., 2005). Hence, there is need for efficient video compression techniques. Video compression is very important in the efficient transmission and storage of videos. This is because raw video data contains an immense amount of data and a high bit rate which increases the communication and storage requirements.

Video encryption algorithms generally works with videos in a compressed format because of its large volume nature to make its storage and transmission over bandwidth-limited networks feasible (Rajagopal & Shenbagavalli, 2013; Yogita, 2013; Mukut & Pradhan, 2011) An absolute solution for protecting video transmission cannot be provided by a single technology. (Eugene et al., 2001; Jolly & Saxena, 2011). Encryption of video data can however take place before, during or after compression.

2. Compression

2.1 Compression of Video

A video consist of series of discrete digital images exhibited at a fast succession with fixed magnitude. In videos, these images are called frames with each frame liable to resemble close frames. The magnitude at which frames are displayed is measured in (fps). A frame is digital image which is made up of pixel’s rasters. A pixel is a small square with only one property called color. Hence, a frame with W pixels breadth and of H pixels height has a size of frame $W * H$ pixels.

Video compression is an engineering of video signals under constraint without losing its quality by utilizing data redundancy in between successive video frames. (Suganya & Mahesh, 2014). It is the process of encoding video data to contain fewer bits thereby allowing an effective data movement and storage. Compression is a reversible process whose inverse called decompression reproduces the uncompressed video data (decoding). (Djordje, 2009).

In video compression, a small percentage of the original video bits is required by each frame hence assuming a compression algorithm shrinks an input multimedia data by a Compression Factor (CF):

Bit Rate (BR) = Bits per frame * frame rate where Bits per frame=$W * H * Color\ depth$.

$$= W * H * CD * FPS/CF$$

$$= W * H * \left(\frac{CD}{CF}\right) * FPS$$

Where $\frac{CD}{CF}$ is the average bit per pixel (BPP).

Thus,

$BR = W * H * BPP * FPS$ and $VS = (BR * T) / CF$

Bit rate is the amount of magnitude of information a digital video stream contains. Bit rate equates the quality of the video in uncompressed videos. Bit rate is an important feature during transmission. This is so because bit rate must be supported by a strong enough transmission link. Also, since the video size is proportional bit rate and duration.

The average Bits Per Pixel (BPP) is a measure of the efficiency of compression, a true color with no compression may have a BPP of 24 bits per pixel.

2.2 Types of Video Compression

There are two types of video compression techniques; Compression can be lossy or lossless.

Lossless compression: In this type of compression, compression doesn’t relinquish any visual content or details carried by initial data. The original data is not distorted. Here, the degree of compression is limited. It permits a recovery of 100% original data recovery. This method is employed when loss of information causes a major damage. (Djordje, 2009). Examples includes the Huffman algorithm, Run length coding etc,

Lossy compression: In a lossy compression, a higher compression rate can be achieved by removing unnecessary information which are not obvious to the viewers and will not change the subjective quality of the decoded video signal. It is employed in data which contain lot of redundancies and insensitive to losses. In Lossy compression some information that cannot be recovered are destroyed, that is original data cannot be recovered in this technique. (Hosseini, 2012). However, the recovered information is useful in some ways. (Sashikala et al., 2013; Djordje, 2009).

2.3 Video Compression Format

A lot of video compression as well as codec algorithms such as the intel RTV/ indeo, IBM photo motion, moving Joint Photographic Experts Group (MJPEG), wavelets, H.261/H263, Moving Picture Experts Group (MPEG) have been reported in literature in the last three (3) decades but our current interest is on MPEG compression.

MPEG (Moving Picture Coding Experts Group) compression whose founding fathers are Leonardo Chairigline (Italian) and Hiroshi Yasuda (Japan) has a basic idea in transforming a stream of discrete samples into a bit stream of token such that it take a less space. A video stream is series of digital pictures. MPEG makes use of the temporal relationship between successive frames for compression of video streams. (Hosseini, 2012). The basic principle behind MPEG video compression is image to image prediction.

MPEG and some video compression algorithms utilized in standards usually contain the following: reduction in resolution, motion estimation, Discrete Cosine Transformation (DCT), entropy coding and quantization. One very important step is the motion estimation.

The motion compensation is the procedure through which the positions between diverse types of frames are obtained. In motion compensation, MPEG video can be defined as series of frames. Frames in this series are coded using three (3) different categories of frames. We have I-frame which is also called the intra-frame, the predicted frame referred to as P-frame and the bi-directional frame referred to as B-frame. The P and B- frames are referred to as inter-coded frames.

The self-contained frames which is also known as I-frame are called the key frames. They have no correspondence to other frames. These are employed as access points in MPEG streams and are coded using a discrete cosine-based approach related to JPEG format. To decode any frame, one needs to search and find the closest previous I-frame. This is done to allow reverse playback, skip ahead or error recovery. (Hosseini, 2012; Sayood, 2003). They produce the lowest compression ratio within the three frames. (Hosseini, 2012; Raymond and furht, 1997; Djordje, 2009).

P-frames which is known as the predicted frames are frames of previous I-frame or P-frame. These are coded using forward predictive coding. The purpose of coding P-frames is to find matching images that are of related forms in the preceding corresponding frame then code just the dissimilarity in the P-frame and the matching being found. For individual main block in the frame, the encoder locates a corresponding block in the former P-frame or I-frame which is considered the best match for it. The corresponding block can potentially be anywhere in the image. Once exact frame is identified, the pixels of the corresponding block are deducted from the referencing pixels in the main block. This give a result of residual value that is near zero. This residual is coded using a similar approach to JPEG algorithm. There is need for a coder to send the motion vector which is achieved using Huffman compression algorithm. If there is no match located, then the block would be coded the same as an I-frame. (Hosseini, 2012). Less space is required in this frame as compared with the I-frame as only the differences are stored. Also, the compression ratio here is appreciably higher than that of I-frames. (Raymond and furht, 1997; Djordje, 2009).

B-frames which are referred to the bi-directional frames are coded using two different directional corresponding frames (forward and backward frame) which can be I-frame or P- frame. In this type of frame, a reusable data is looked for in both directions. This approach is like P-frames but instead of just looking for the former I or P-frame for a match the next I or P- frame is looked for in the method. If a match is identified for the two directions, the average of the two (2) reference frames is used. If only one good match is found, then the one found will be used as the reference. In cases like this the coder must pass information specifying the corresponding that was employed. (Hosseini, 2012; Lelewer and Hirscherg, 1987). B-frame provides the highest amount of compression. (Raymond and furht, 1997; Djordje, 2009).

The particular frame used in a video determines the compression and quality ratio of the video compression. I-frames increases value and dimensions while B-frames reduces better but gives a poor value. The length that exists between 2 I-frames measures the quality of an MPEG-video. Motion vector is the relationship between 2 frames in terms of motion. The motion vector and the arithmetic difference depend on effectiveness of the implemented motion compensation algorithm. Motion compensation operation is computationally intensive which usually not suitable for real-time applications. (Djordje, 2009). It is a process that involves frame segmentation, search threshold, block matching, prediction error coding and vector coding.

Some common examples of MPEG algorithms include MPEG-1, MPEG-2 and MPEG-4.

Moving JPEG (IS92a) uses the Joint Photographic Experts Group (JPEG) to provide compression for each frame of the video and hence providing a randomized access to individual frames. Compression ratio in this standard is very low as the algorithm considers not the advantage of similarities between adjacent frames. (Raymond and Furht, 1997).

MPEG 1 (IS92b) on the other hand supports the compression of image resolutions of about $352 * 288 \text{ pixels at } 30\text{fps}$ into a data stream of 1.5mb/s. It allows fast forward and backward search with synchronization of audio and video.

MPEG-2 (IS93b) is a quality supporting reduction of digital image resolution of just about $704 * 576\ pixels\ at\ 30fps$ and $HDTV\ of\ 1920 * 1152\ at\ 60fps$. It compresses approximately at three (3) times that of moving JPEG. It is compatible with MPEG 1 but allows a better quality with a slightly higher bandwidth of between 2 and 20 Mbits/sec. The development of MPEG-2 had extra emphasis on scalability with the ability of playing different resolutions and frame rates of a video. MPEG-2 was designed because of the inability of MPEG-1 to be used in audio coding and video quality for television broadcasting systems and also its inability to efficiently encode interlaced fields. MPEG-2 aids the recovery from errors in transmission as some error recovery mechanisms were used with the encoder. (Raymond and Furht, 1997).

MPEG-4 was released in late 1998 with a main development over MPEG 2. This was developed for use in environments that are interactive such as multimedia application and video communication (Djordje, 2009). It has a bit rate of between 10kbits/sec to 1Mbits/sec. MPEG-4 has the ability of regrouping the content of a frame into objects which individual can access through the MPEG-4 syntactic description language (MSDL). MPEG-4 can reduce the bit rate independently for certain applications and they are adaptive to specific areas of video application. Its other characteristics include robustness in error-prone environments, improved coding efficiency, improved temporal random access etc. It supports both MPEG-1 and MPEG-2 functionalities although many of the tools in MPEG-4 need enormous computational ability (for encoding and decoding) this makes then not practically applicable for most normal and non-experts or real-time systems.

The usage of MPEG has touched so many real-life applications like cable television, broadcast satellite that is not interrupted, real-time encoding, computer network etc.

2.4 Data Redundancies

Video compression is feasible because video data contains a lot of redundancies. However, it must be noted that there is always a trader-off between quality and data size when compression methods are employed. The higher the ratio of compression, the smaller the size of the video and the lower the video quality.

2.4.1 Types of Data Redundancies

There are basically two (2) categories of redundancy in a video data; the spatial redundancy and temporal redundancy. Spatial redundancy: In a frame of a video data, nearby pixels are often correlated (related) with each other, this correlation is called intra-frame correlation, that is, Spatial redundancy is divided into two types: the statistical and redundancy in subjective type. Redundancy in statistical type simply mentions that the neighbouring values of pixel in digital image are frequently much correlated. Entropy coding such as Huffman coding can be applied to remove this type of redundancy. Redundancy in subjective type on the other hand mentions that human visual system is invariant to particular visual information parts. Hence, these parts may be taken away without resulting to serious subjective standard degradation.

Temporal redundancy: (inter-frame correlation) means adjacent (neighboring) frames are highly correlated, that is, within a sequence of video, successive frames are usually the same. The movement in the scene is usually due to differences between successive frames. Similarity in two successive frames in a sequence, result to a condition in which many of the blocks in the difference frame have no information and this indicates no further need of any transmission.

In other words, to have a well compressed video, the spatial and temporal redundancy must be efficiently reduced. There are basically three (3) factors to be considered during the compression process: the image size, the color depth and the frame size.

Image Size: complete screen resolution is normally 640 x 480 pixels or 800 x 600 pixels for a 14 inch monitor. Just like in frame rate, compressing the image size can greatly reduce file volume. When reducing an image dimensions, a 4:3 aspect ratio should be used. Aspect ratio of a digital image represents the proportional relationship between an image width and its length. It is quite possible to play back a 320 x 240 image sized video at double-size to have a complete-screen movie with practically good results. A small video size would normally run at 192 x 144 pixels.

Color Depth: Normal digital video has 24-bit colour (millions of colours).

Cutting down the colour range to 16 bit (thousands of colours) will reduce file size by one third. Some codecs permit 8-bit color (256 colors) which only might work for animations.

Frame Rate: A raw video runs 30 frames per second. Although, the illusion of motion can still be obtained with speeds as slow as 10 frames per second when there are no speedy moving objects. Cutting the speed to 15 frames per second or less can reduce the size of a file in half (or less than half) without sacrificing quality when there is only a moderate amount of motion. Evaluations should be conducted on the video file to determine which colour depth is important because reducing colour depth can really affect the image.

3. Encryption

3.1 Introduction

Data encryption is an appropriate method of protecting video data from unauthorized access. Various traditional ciphers have been proposed but are more suitable for text and binary data. As video data comprises of enormous volume, it is herculean to use these encoders in video protection.

3.2 Classification of Encryption

Typically, Video encoding techniques can be grouped into four basic types; completely layered technique, permutation based technique, selective encryption technique and perceptual technique. (Ajay et al., 2013; Yogita, 2013; Zhaopin et al., 2012; Jolly and Saxena, 2011).

Completely Layered Encryption: In a completely layered encryption, a cryptosystem is used in the encryption process to encrypt the whole video data after being compressed without considering any region of interest. Encryption is done on the video data frame by frame without considering the objects in video or any other important information. They produce the highest security and they have higher computational Intricacy than the other groups more adequate for securing video storage (Zhaopin et al., 2012; Wong and Bishop, 2005). Due to their high computational demand they are not applicable to real-time video applications (Jolly & Saxena, 2011). Examples of this group can be found in the techniques developed by some researchers (Li et al., 2002; Ganesan et al., 2008).

Selectively Encryption: In a bid to reduce the computational complexity inherited as a result of encrypting the whole video data, algorithms that selectively encrypts a particular video sizes (bytes) within the video frames were designed. These methods selectively encrypts only sensitive or important bytes in the video frames. Although these methods lessen complexity in computation through selection of simply the least set of data encode but the protection and pace level is dependent on how many protected parameters. (Jolly and Saxena, 2011). The works proposed by Spanos and Maples, 1995; Meyer and Gadegast, 1995; Shi and Bhargava, 1998; Wu and Kuo, 2001 etc are examples of algorithms in this group.

Perceptual Encryption: the perceptual encoding needs the audio/video quality of the data be partially devalued such that the encoded data are still partly perceptible after encoding and the audio/ video quality of the data is continuously controlled. Perceptual encryption algorithms are unsuitable for applications which require high security. They are suitable only for entertainment applications like pay per view. (Jolly and Saxena, 2011). The works proposed by Pazarci-Dipcin, 2002; Lian, Wang, Sung and Wang, 2004 etc are examples of algorithms proposed in this category.

Permutation Encryption: The permutation based encryption uses diverse permutation technique s to scramble or protect video contents. The entire video does not necessarily need to be scrambled as a particular set of bytes might be scrambled and a permutation list is applied to serve as a secret key. Permutation based algorithms are generally fast but provides an insufficient level of security. (Jolly and Saxena, 2011). Pure permutation, Zig-zag permutation (Tang, 1996), Huffman code word (1998), correlation preserving (2006) etc are examples of algorithms in this category.

As explained above out of the four (4) classifications, it has been proved and shown that the completely layered video encryption produces the highest level of video security but it is computationally expensive because of its slow nature in processing the very large volume of video data and has in return limited its use in video encryption. (Darshana and Parvinder, 2012; Jolly and Saxena, 2011; Abomhara et al., 2010; Puech et al., 2012).

3.3 Performance Parameter

Many encryption of video techniques have been designed. Irrespective of the classification of any designed encryption technique falls into, the following metrics are being used to evaluate and compare their performance. (Ajay et al., 2013; Darshana and Parvinder, 2012; Zhaopin et al., 2012; Jolly and Saxena, 2011).

Security: In most video employment, several levels of protection for capability of complex processing although most cryptographic applications are completely or partly ascendible meaning different security levels are chosen. To achieve scalability, sizes in key or iterations of different values are allowed. A very high security level is attained with number of iterations or larger key.

The encryption technique security is commonly tested by continuous analysis of key space, experiments, analysis of key sensitivity and invulnerability to attacks.

Continuous experimental result is accomplished through class of comparison that exist in the encrypted data and first (original) multimedia data.

Key space analysis is a procedure that involves the application of number of keys analysis encryption process e.g. a bit of 20 key would give 2^{20} key space.

Sensitivity of key for example in a disordered cipher mentions the original levels of sensitivity and control parameters sensitivity of chaotic map.

A method of encryption should be not affected with cryptanalytic attacks such as identified (known) plaintext attack, chosen plaintext attack, brute force attack etc. (Ajay et al., 2013; Darshana and Parvinder, 2012; Zhaopin et al., 2012; Jolly and Saxena, 2011).

Transmission Error Tolerance: The real time passage of multimedia data frequently happens in noisy environments, this is right in the case of wireless networks where the delivered data is liable to bit errors. It is highly desirable that technique of encryption be unaffected and invariant to errors in transmission. The robustness of a video transmitted over a network can be tested by correctly decrypting data encrypted not considering whether some bytes or a frame are degraded or lost during the process of transmission. A fault tolerant is a scheme of encryption that does not affect format of file and its small modification in a pixel does not spread to others. This can also be done by analyzing the relationship in the frames decrypted quality and bit-error number that occurred in the frames that are encrypted (Ajay et al., 2013; Darshana and Parvinder, 2012; Zhaopin et al., 2012; Jolly and Saxena, 2011).

Encryption Ratio: Encryption ratio can be defined as proportion between encrypted video size and the complete data size. Encryption ratio has to be minimized as much as possible to reduce computational complexity. (Ajay et al., 2013; Darshana and Parvinder, 2012; Zhaopin et al., 2012; Jolly and Saxena, 2011).

Compression Efficiency: Compression is performed on video data because of their large size to minimize storage space and bandwidth usage. The encryption method can be achieved earlier, in the course or after compression. Whichever time process of encryption is carried out, the encrypted video size must be made as small as possible. (Ajay et al., 2013; Darshana and Parvinder, 2012; Zhaopin et al., 2012; Jolly and Saxena, 2011).

Degradation: Video distortion can be measured by visual degradation. Visual degradation may be low or high. For example, video sensitive applications such as video conferencing in business gatherings require a great visual degradation while for an entertainment application a low degradation may be needed. (Ajay et al., 2013; Darshana and Parvinder, 2012; Zhaopin et al., 2012; Jolly and Saxena, 2011).

Computational Efficiency: This is defined by its space and complexity in time of encryption algorithm. Complexity in space of an encoding algorithm is the memory required by the program to run while complexity in time is encryption or decryption time. There is however need for a small encryption size and decryption technique with also fast algorithms to meet real-time requirements for applications in video. (Ajay et al., 2013; Darshana and Parvinder, 2012; Zhaopin et al., 2012; Jolly and Saxena, 2011).

Lossless Visual Quality: This is an extremely desirable feature for applications in entertainment. Algorithms in encryption should be able to give the same visual quality as initial video when decrypted properly. (Ajay et al., 2013; Darshana and Parvinder, 2012; Zhaopin et al., 2012; Jolly and Saxena, 2011).

Format Compliance: As a result of the enormity of data in multimedia and irrelevant data, the encoding of data are usually performed before transmission which produces data streams with some format information. This format information will be used by the decrypter to regain a successful multimedia data. It is wished that the multimedia format is kept by the encoding algorithm, that is, the bit stream encrypted should be conformable with the compressor. (Ajay et al., 2013;

Darshana and Parvinder, 2012; Zhaopin et al., 2012; Jolly and Saxena, 2011).

3.4 Video Encryption Algorithm

This section reviews some encryption techniques that has being in literature in the last two (2) decades.

Ajay et al., 2013 proposed an encryption algorithm where a video cutter is used to separate the video into frames. These video frames are in video format as they contain audio data. A shuffling block shuffles these video frames which are then moved on to frame stitching block. A new video is formed by frames which are now in random position. In this technique, the audio stream cannot be decrypted unless one has the knowledge of the shuffling methodology. A random key generated by a function in java is used by the shuffling algorithm, this function is called shuffling key which is encrypted end to end with the video applying AES that is carried together with the video to the destination decryption block.

This algorithm will suffers from brute force attack. There is however need to increase the security strength of the algorithm. To achieve this, AES is used to encrypt the code words extracted from MVDs, DCs and ACs. Computational time is saved by extracting and encrypting only important or sensitive code or words. Code words are after encryption mixed-up with the blocks on every frame remaining the same but with a changed location. The video is however sent to the client who runs the algorithm in AES over the code words to decrypt and also to get a standard video. The decryption block also decodes the random key and apply it to restructure frames to its initial location. The proposed algorithm has a very good computational speed and a high level of security.

Mayank et al., 2012 proposed an encryption scheme which is based on the encryption of I-video frames by using an effective and generalized scheme based on computation in matrix. This system applies the concept of video frame and XOR operation. They made use of knowledge of matrix computation for generating the encrypted I-frame. All video frames were collected then were taken one after the other and a key frame selected as the key image for the encoding and decoding process. A secured channel is used to send key image. The remaining frames were encrypted by their designed algorithm and after the encryption algorithm has been applied on all frames, they were combined to form an encrypted video. This scheme is efficient and secured against a cryptographic but it can only be applied to a certain class of video sequence and video codes. (Yogita, 2013).

Saranya & Varalakshimi, 2011 proposed a selective video encryption with the purpose of selecting an adequate data in advance the compression for encryption which in return gives a greater efficiency at a reduced cost. They proposed a distinct scheme with RC4 stream ciphers which is used to generate a pseudorandom stream of bits in which the encryption is combined with the plaintext using bit-wise exclusive-or with the decryption executed in the same manner. (Rajagopal & Shenbagavalli, 2013)

Shaima and Khalid, 2011 came up with an in-compression algorithm for encryption applying Optimized Multiple

Huffman Table (OMFT). This technique encodes and encrypts video sequence. It encodes video sequence frame or encrypts the original frame and then reduce and encrypt the motion vector between successive frames. The OMHT encryption technique and the OMHT process takes two (2) parallel paths. No extra time is required to include encryption to the compressed bit stream as both in traditional and selective encryption technique. A statistical model based compression is used to generate different tables from a training set of videos. An increased compression efficiency and security is attained. (Rajagopal & Shenbagavalli, 2013)

Yan and Main, 2009 designed a video encryption system by applying scrambling to the Discrete Cosine Transform (DCT) coefficient in a 16 x 16 macro-block. They used a complete scrambling algorithm to disorder DCT coefficients in the macro-block, a subsection scrambling algorithm to divide the DCT coefficients and scrambles them in different segments according to security and compression ratio. In this video cryptosystem, the encrypted DCT coefficients scrambling algorithm only breaks the order of coefficients or macro-blocks and doesn’t encrypt video data hence it has a low security. Also, because the technique requires only scrambling and not encryption, DCT coefficients scrambling algorithm has high runtime. (Rajagopal and Shenbagavalli, 2013).

Yang and Sun, 2008 developed a chaos-based video encryption method in a DCT (Discrete Cosine Transform) domain. In this CVED, only I-frames are selected as encryption objects, a double coupling logistic map is used to scramble the DCT coefficients of I-frames and then encrypt the DCT coefficients of the scrambled I-frames by using another logistic map. The technique is applicable in real-time applications as only encrypting the coefficients of I-frames consumes little time. The study introduced Five (5) keys in the complete process and thus the key space is large enough to resist brute force attack. This technique is not secured enough as there are some B and P-frames which are unprotected that are encoded without referring to I-frames. (Zhaopin et al., 2012).

Ganesan et al., 2008 designed a public key encryption (PKVE) of videos based on chaotic maps. In this technique, if the number of frames are so many, the phrase scrambling method proposed by Nishchal et al., 2013 will be used which will be followed by the encryption of video using the chebyshev maps (Bergamo et al., 2005). The entire video frame can as well be encrypted using Arnold transform (Prasad, 2010). This technique is secured over known chosen-plaintext intrusion and with high key sensitivity. It is very effective in real time application for 64x64 and 128x128 pixel size videos. (Zhaopin et al., 2012).

Li et al., 2002 proposed a chaotic video encryption (CVES) for real time digital video based on multiple digital chaotic systems. In this technique, each plain block is first XORed by a chaotic signal and then replaced by a pseudo-random S-box based on multiple chaotic maps. This encryption technique is invariant to intrusion and known chosen-plaintext attacks. It has a reduced computational complexity and therefore can be easily utilized for hardware and software. (Zhaopin et al. 2012).

Chiaraluce et al., 2002 described an encryption algorithm for H.263 videos where the cipher operations were seamlessly combined with the H.263 encoding method, that is, RLC and packaging. In this encryption technique, the significant bit in the DC coefficient of DCT, the AC coefficient of I-MB (Intra macro blocks), the sign bit of the AC coefficients of the P-MB (predicted macro-blocks) and the sign bit of the motion vectors are encrypted applying three (3) properly arranged different chaotic functions namely the Skew tent mop, saw-tooth likewise map and logistic map. It has a key space of 2^{512} which is greatly sufficient over brute-force attack. It modifies key every 30 frame and thus secure against known chosen plaintext attacks, it however increases the time of processing. (Zhaopin et al. 2012)

Wu and Kuo, 2001 proposed 2 selective algorithms in encryption for MPEG video called the Multiple Huffman Tables (MHT) and MSI (Multiple State Indices) encryption algorithms. The first algorithm was based on encryption during entropy coding. At the entropy coding stage, symbols in the video stream are transformed to binary sequences in accordance to predefined Huffman table to integrate encryption with entropy coding. The basic MHT encryption work as; at first 2^k Huffman tables created and numbered 0 to 2^k -1 then random vector P of n numbers produced where each number is a K bit number in the range 0 to 2^k -1. The basic building block of this algorithm is that it converts entropy coders into encryption ciphers. (Darshana and Parvinder, 2012; Jolly and Saxena, 2011; Eisenbarth, 2007).

Not well satisfied with their work, they proposed an enhanced version of the MHT in 2005. A directional hash function was used to initiate a key hopper by first assigning some seed value S which is used and then produce the output values by applying a hash function on the seed value and further values generated from seed value like (S+1, S+2 etc). However, various cryptanalysis studies have shown that the basic and improved MHT techniques are at risk to selected plaintext and identified plaintext attacks. (Darshana and Parvinder, 2012; Jakimoski et al., 2008; Zhou et al., 2007). Also, encrypted videos using MHT scheme is completely incomprehensible and as such cannot be used for perceptual encryption. (Darshana and Parvinder, 2012).

Cheng and Li (2000) extended their limited encryption schemes to digital still images to continuous images (video). The scheme uses a quad tree compression method and wavelength compression algorithm based on zero trees for the video stream I-frame, motion compensation and residual error coding. The scheme works for video stream based on set partitioning in hierarchical trees image compression algorithm. The proposed encryption system encrypts the I-frames, the motion vectors and residual error code of video stream. (Darshana and Parvinder, 2012).

Alattar et al (1999) proposed three (3) methods for selective video encryption of MPEG-I video sequence, based on DES cryptosystem. In the first cryptosystem, every nth I-macro-block was encrypted. In the second method, headers of all the predicted macro-blocks and nth macro-block data were encrypted. The third method encrypts nth macro-block as well as the header of every nth predicate macro-block. This scheme works during compression. (Darshana & Parvinder, 2012).

Shi and Bhawgava (1998) developed a video encryption algorithm (VEA) where an undisclosed key was employed to randomly alter the sign bits of the DCT coefficients of I-frame using the simple XOR operation. The maximum 64 bits of DCT sign values selected and XOR operation is accomplished with the key and due to the fact that only 64 bits of information is being encrypted for each frame the algorithm is very fast. This algorithm produces a very high-visual degradation because the DCT coefficients are being encrypted. The algorithm security is vulnerable to known plaintext attack and known cipher text attack. (Mukut & Pradhan, 2011).

They however improved their work by proposing an algorithm called the MPEG video encryption algorithm (MVEA). In this algorithm, the sign bits of the DCT coefficients of Y, C_b, C_r block of I frames and the sign bits of the motion vector in B and P frames were encrypted with one secret key. Inclusion of the motion vector in encryption is very efficient as it significantly degrades the picture quality. Also, the security of this algorithm relies on the length of the key. Like their earlier algorithm, the algorithm suffers from known plaintext and ciphertext attacks. (Mukai and Pradhan, 2011; Singh and Manimegalai, 2012).

Qiao and Nahostedt (1997) proposed an algorithm for video encryption. This algorithm is based on the statistical properties of MPEG video standard and symmetric key algorithm standard to reduce the amount of data that is encrypted. This algorithm divides the video stream input into chunks (a_1, a_2, a_3, …., a_{2n-1}, a2n). The chunks are then divided into two data segments; the odd list (a_1 ,a_3 , …, a_{2n-1}) and even list (a_2,a_4, …a_{2n}). After this, key for encryption is applied to the even list E (a_2, a_4, …a_{2n}) where E denotes an encryption function. The final cipher text is a concatenation of output of encryption algorithm XORed with the odd list streams which makes the technique invulnerable to known-plaintext attack because the key is changed for each frame. (Darshana and Parvindar, 2012; Yogita, 2013)

6. Conclusion

This paper presents a review on the basic concept of video compression and also an extensive survey of Video encryption and its Algorithms. Although, an essential and various quality of encryption of video techniques have been proposed in this study, most of the techniques are vulnerable to cryptanalysis attacks. The total encryption algorithms provide the most secured form of video security but it is computationally expensive and not applicable in real-time applications. Algorithms based on permutation are very fast but they do not provide meaningful degree of video security. Selective based encryption techniques reduce complexity in computation posed by the naïve video encryption algorithms. They select only few dataset to encrypt videos. The security and speed level is dependent on the part of the video data encrypted. Perceptual encryption algorithms are suitable for applications where the potential video users may need to see a lower quality version of the video before buying them. They are unsuitable for systems that require strong security platform. It is however impossible for a single algorithm to satisfy all performance metric requirements. Thus, selecting an encryption algorithm depends on requirements of the application in use. It can be concluded that it is a challenge for researchers to design an encryption algorithm which maintains tradeoff among all performance parameters.

References

Abomhara, M., Zakaria, O., & Khalifa, O. (2010). An overview of video encryption techniques. In ternational Journal of computer theory and engineering. 2 (1).

Ajay, K., Sourabh, K., Ketki, H., & Aniket, M. (2013). Proposed video encryption algorithm vs other existing algorithms: A comparative study. International Journal of Computer Applications. 65 (1).

Alattar, A.M., Al-Regib, G.I., & Al-Semari, S.A. (1999). Improved selective encryption techniques for secure transmission on MPEG video bit streams. Proceedings of International Conference on Image Processing.

Chiaraluce, F., Ciccarelli, L., Gambi, E., Pierleoni, P., & Reginelli, M. (2002). A new chaotic algorithm for video encryption. Institute of Electrical and Electronics Engineer Transactions on Consumer Electronics. 48 (4). (833-844).

Darshana, H., & Parinder, S. (2012). A comprehensive survey of video encryption algorithms. International Journal of Computer Applications. 59 (1).

Djordje, M. (2009). Video Compression. University 0f Edinburgh. Retrieved via www.google.com.

Eugene, T., Gregory, W. C., Paul, S., & Edward, J. D. An overview of security issues in streaming video. Retrieved via www.google.com.

Furht, B., Muharemagic, E., & Socek, D. (2005). Multimedia encryption and watermarking. Springer-Verlag, New York.

Ganesan, K., Singh, I., & Narian, M. (2008) Public key cryptography of images and videos in real time using chebyshev maps. Proceedings of the 2008 Fifth International Conference on Computer Graphics, Imaging and Visualization, Institute of Electrical and Electronics Engineer Computer Society, Washington DC, USA. (211-216).

Hosseini, M. (2012). A survey of data compression algorithms and their applications. Network Systems Laboratory, School of Computing Science, Simon Fraser University, BC, Canada.

John, J., & Mamimurugan, S. (2012). A survey on various encryption techniques. International Journal of Soft Computing and Engineering (IJSCE). 2 (1).

Jolly, S., & Vikas, S. (2012). Video encryption: A Survey. International Journal of Computer Science Issues. 8 (2).

Mayank, A. C., Ravindra, P., & Navin, R. (2012). A novel approach of digital video encryption. International Journal of Computer Applications. 49 (4).

Meyer, J., & Gadegast, F. Security mechanism for multimedia data with the example MPEG-1video, project description of SECMPEG.

Mukut, R., & Pradhan, C., (2011). Secured selective encryption algorithm for MPEG-2 video. Journal of Institute of Electrical and Electronics Engineers.

Lelewer, D., & Hirschberg, D. (1987). Data compression. ACM Computing Surveys.

Li, S., Zheng, X., Mou, X., & Cai, Y. (2002). A chaotic encryption scheme for real time digital video. Proceedings of SPIE, SPIE press, San Jose, CA. 149-160.

Rajagopal, S., & Shenbagavalli, A. (2012). A survey of video encryption algorithm implemented in various stages of compression. International Journal of Engineering & Technology (IJERT). 2 (2)

Raymond, W., & Furht, B. (1997). Real-time video compression techniques and algorithms. Kluwer Academic Publishers.

Sashikala, M. Y., Arunodhayan, S.S., & Nachappa, M.N. (2013). A survey of compression techniques. International Journal of Recent Technology and Engineering (IJRTE). 2 (1)

Sayood, K. (2003). Lossless compression handbook. Academic press, 2003.

Shi, C., & Bhargava, B. (1998). A fast MPEG video encryption. Proceedings of the 6th ACM International Conference on Multimedia, New York, USA. (81-88).

Spanos, G.A., & Maples, T.B. (1995). Performance study of a selective encryption scheme for the security of networked, real-time video. In the Proceedings of the 4th International Conference on Computer and Networks (ICCCN '95). (2-10).

Suganya, G., & Mahesh, K. (2014). A survey of various techniques of video compression. International Journal of Engineering Trends and Technology (IJERT). 7(1).

Puech, W., Erkin, Z., Barni, M., Rane, S., & Lagendijk, R. L. (2012). Emerging cryptographic challenges in image and video processing. Journal of Institute of Electrical and Electronics Engineers.

Qiao, L., & Nahrstedt, K. A new algorithm for MPEG video encryption. In the Proceedings of the First International Conference on Imaging Science, Systems and Technology (CISST'97).

Wong, A., & Bishop, W. (2005). An efficient parallel multi-key encryption of compressed video streams. Department of Electrical and Computer Engineering, University of Waterloo.

Wu, C.P., Kuo, C.C. (2005). Design of integrated multimedia compression and encryption systems. Institute of Electrical and Electronics Engineer Transaction of Multimedia. 7(5). (828-839).

Yan, L., & Main, C. (2009). H.264-Based multiple security levels net video encryption scheme. Institute of Electrical and Electronics Engineers International Conference on Electronic Computer Technology.

Yang, S., & Sun, S. (2008). A video encryption method based on chaotic maps in DCT domain. Progress in Natural Science. 18 (10). (1299-1304)

Yogita, N. (2013). A survey of video encryption techniques. International Journal of Emerging Technology and Advanced Engineering.3 (4).

Zhaopin, S., Guofu, Z., & Jianguo, J. (2012). Multimedia security, a survey of chaos based encryption technology multimedia. School of Computer and Information, Hefei University of Technology, China.