International Journal of the Physical Sciences Vol. 6(16), pp. 4053-4063, 18 August, 2011
Available online at http://www.academicjournals.org/IJPS
DOI: 10.5897/IJPS11.372
ISSN 1992-1950 ©2011 Academic Journals

Full Length Research Paper

An experiment of scalable video security solution using H.264/AVC and advanced encryption standard (AES): Selective cryptography

Mohamed Abomhara[1], Othman O. Khalifa[2], A. A. Zaidan[3,4,5]*, B. B. Zaidan[3,4,5], Omar Zakaria[6] and Abdullah Gani[1],

[1]Faculty of Computer Science and Information Technology, University of Malaya, Kuala Lumpur, Malaysia.
[2]Electrical and Computer Engineering Department, International Islamic University Malaysia, Kuala Lumpur, Malaysia.
[3]Faculty of Engineering Multimedia University, Cyberjaya, Selangor Darul Ehsan, Malaysia.
[4]Predictive Intelligence Research Cluster, Sunway University, Petaling Jaya, Selangor, Malaysia.
[5]Institute of Postgraduate Studies, Research and Development Group, Al-Madinah International University, Shah Alam, Malaysia.
[6]Department of Computer Science, Faculty of Defence Science and Technology, National Defence University of Malaysia, Kuala Lumpur, Malaysia.

Accepted 20 April, 2011

This paper presents an efficient and effective framework for the design and development of enhanced selective video encryption scheme for H.264/AVC based on advanced encryption standard (AES). Due to the importance of maintaining the security of information that is publicly displayed, many approaches have been implemented to provide security for information dissemination over the networks. These include encryption, authentication, and digital signatures. For video, the method has been adopted to protect unwanted interception and viewing of any video while in transmission over the networks. In this paper, we design a new selective video encryption based on H.264/AVC and AES. In this proposed scheme, instead of encrypting the entire video stream bit by bit, only the I-frames bitstreams are encrypted. This method took into consideration the good features of selective encryption algorithms with regard to computational complexity, and data compression performance. The proposed scheme was tested in the simulated environment using different video sequences. The experimental results show that the proposed method provides adequate security to video streams. It has no effect on compression ratio and does not reduce the original video compression efficiency. Moreover, it is a suitable technique for secure H.264 bitstreams that require transmission or storage in un-trusted intermediate devices.

Key words: Encryption /decryption, H.264/AVC, video compression, video ciphering, advanced encryption standard (AES).

INTRODUCTION

With the rapid growth of the Internet and multimedia within different security applications in the distributed environments (Raad et al., 2010, Zaidan et al., 2011), it has become easier for digital data owners to transfer multimedia documents all over the world via the Internet (Abomhara et al., 2010a). As a result, multimedia security has become one of the most important aspects of communications with the increasing volume of digital data transmission (Zaidan et al., 2010a, f). In addition, some applications, such as TV broadcast, video on demand, and video-conferencing, require a special, reliable and secure way of storing and/or transmitting digital images and videos, may be used in many applications.In general, multimedia security is provided by one or more methods to protect multimedia contents (Hmood et al., 2010a, b, c). Traditionally, these methods were mainly based on cryptography (Alam et al., 2010; Zaidan et al., 2010b). Cryptography is the art of keeping information secret by transforming it into an unreadable format (encryption) by using special keys (Zaidan et al., 2010c; Zaidan et al.,

*Corresponding author. E-mail: aws.alaa@gmail.com.

2010d), which in turn, render the information readable again for the trusted parties by using the same or other special keys (decryption) (Zaidan et al., 2010e; Kessler, 1998). Modern cryptography, however, is not limited only to maintaining the secrecy of information but also to: ensuring the identity of the communicating parties (authentication); ensuring that information is not tampered by others (integrity); and preventing any of the communicating parties from denying any received or sent information (non-repudiation) (Abomhara et al., 2010b; White, 2003; Harris, 2007).

Security is necessary when communicating multimedia data over any untrusted medium such as the public networks (Ahmed et al., 2010), and in particular, the Internet. In order to protect information from theft, alteration or misuse, cryptography can also be used for user authentication (Hmood et al., 2010d). In modern cryptography, there are three types of cryptographic schemes: Secret key (or symmetric) cryptography, public-key (or asymmetric) cryptography (Alanazi et al., 2010b; Nabi et al., 2010), and hash functions. Symmetric-key cryptography refers to encryption methods in which both the sender and receiver share the same key (Sameer et al., 2011). This was the only type of encryption technique publicly known until 1976. Whitfield and Hellman (1976), proposed the notion of public key cryptography, which was also known as asymmetric key cryptography. It uses two keys, one for encrypting information by the sender, and one for decrypting information by the receiver (Alanazi et al., 2010a). The hash function, also called message digest or one-way encryption, is a transformation that takes an input and returns a fixed-sized string, which is called the hash value (Medani et al., 2011). While symmetric or asymmetric encryption methods provide the means to ensure information confidentiality, hash functions provide a measure of the integrity of a file (Zaidan and Zaidan, 2011). For instance, hash algorithms are typically used to provide a digital signature of a file's contents and to ensure that the file has not been altered by an intruder or virus (White, 2003; Harris, 2007).

In some applications such as commercial TV broadcast and military applications, the information or content has to be securely transmitted and stored. Furthermore, video-conferencing has become a daily practice in financial businesses, as it saves time, effort, and travel expenses for large companies. This communicated video application has to be completely secure against theft, alteration or misuse. For this purpose, security algorithms can be applied to these multimedia applications to ensure their security (Shieh, 2003; Wenjun et al., 2006; Massoudi et al., 2008). Communication security for multimedia can be accomplished by means of standard symmetric key cryptography, as such media can be treated as binary sequence and the whole data can be encrypted using a cryptosystem such as AES or DES (Weng et al., 2006; Naji, et al., 2009). In general, when the multimedia data is static (not a real-time streaming) it can be treated as regular binary data and the conventional encryption techniques is used. In the past, encrypting the entire video data using standard encryption algorithms was referred to as a Naïve approach (Agi and Gong, 1996). This method can provide substantially high security but it incurs huge computational cost. Presently, most of the researches are focused on selective video data encryption, which can reduce computational cost as it encrypts only a part of video data.

Owing to a variety of constraints (such as the near real-time speed, etc.), communication security for streaming audio and video media is more difficult to be accomplished. Encryption of video and audio multimedia content is not simply the application of established encryption algorithms, such as DES or AES to the binary sequence, but it involves careful analysis to determine and identify the optimal encryption method when dealing with video data (Cheng and Li, 2000; Furht and Socek, 2003; Ahmed et al., 2007). Recently, encryption techniques provide the basic technology for building secure multimedia system. In order to provide real-time and reliable security for digital images and videos, many different encryption algorithms have been proposed to make networked continuous media secure from potential threats such as hackers and eavesdroppers. Most of these video encryption algorithms were designed for various video coding standards such as MPEG-1, MPEG-2/H.262, and MPEG-4 (Yibo et al., 2007). Unfortunately, these encryption algorithms are not appropriate to ensure security for current multimedia contents. Therefore, current researches are focused on modifying and optimizing the existing cryptosystems for real-time video. It is also oriented towards exploring the format-specific properties of many standard video formats in order to achieve the desired speed and enable secure real-time streaming (Deniz et al., 2007; Fang et al., 2008).

Motivation

Today, the use of multimedia data and contents is very widespread and is becoming a part of our daily life. In the absence of a reliable security system to protect multimedia data, multimedia users on the public networks like the Internet face risk of their sensitive information being compromised. It is necessary, therefore, to provide adequate security for such information so that the service provided is reliable for conducting various types of business transactions. There is a need for end-to-end encryption for multimedia data, because while communication between users can be made secured using encryption, the multimedia transmitted between them through a public network is not encrypted. The results from a number of researches indicate that multimedia data can be encrypted using symmetric key algorithm with MPEG bitstream.

Thus, the use of the symmetric key algorithm with H.264/AVC, is a solution to provide end-to-end security for multimedia data.

Problem statement

With the dramatic increase in use of multimedia applications, the exponential increase in security incidents and constant attempts by hackers to compromise confidentiality and integrity of multimedia contents, underline the need for stronger security. Until now, there is still a lack of appropriate video encryption algorithms. Since the mid 90's, many research efforts have been devoted to design specific video encryption algorithms. However, these proposed encryption algorithms are characterized by considerable imbalance between security and efficiency. Some of them are efficient enough to fulfill the real-time requirements, but have a limited level of security. On the other hand, some are able to meet security demands adequately, but have limited encryption efficiency. Moreover, most of these algorithms are related to certain video compression schemes and implemented together in software. This makes them less compatible with today's video compression schemes (Yibo et al., 2007; Salah, 2003). Therefore, it is very important to design an efficient video encryption algorithm to ensure not only the confidentiality of the multimedia data, but also to avoid the computational complexity.

Research objectives

A good and reliable video streaming system must be able to stream video over a communication medium in a scalable, efficient, and secure manner. The objectives of this research are as follows:

1. To gain a deep understanding of video data security and multimedia technologies;
2. To investigate how encryption and decryption techniques could be implemented for video applications;
3. To integrate the available AES security protocol into the H.264/AVC video compression technology and encrypt the I-Frame of H.264/AVC bitstreams;
4. To simulate and implement an encryption system which embeds encrypted multimedia files (video) to enhance the selective encryption feature of H.264/AVC, and
5. To evaluate the performance of the proposed system and compare the proposed scheme with the relevant existing systems.

Research questions

The research presented in this paper design a new selective video encryption based on H.264/AVC and AES. The research questions for this paper are:

1. How do the propose method provides adequate security to the video streams?
2. Is it effect on compression ratio and reduce the original video compression efficiency?
3. Is it a suitable technique for secure H.264 bitstreams that require transmission or storage in un-trusted intermediate devices?

CURRENT VIDEO ENCRYPTION/ DECRYPTION TECHNOLOGIES

The exchange and communication of multimedia have grown dramatically in recent years. Today, we are even witnessing an increasing demand for remote video communication. The development of encryption systems aims to provide a secure and reliable way for information exchanges. However, the security aspects of video exchanges have yet to be fully addressed. Exisiting video coding standards do not incorporate requirements to have encryption capabilities.

In many cases, the compressed video data is treated like any other types of data and encryption is carried out only after the video encoding process is fully completed, while decryption takes place at the receiver's side before the start of the video decoding process (Bergeron and Catherine, 2005). One of the well-known methods used is the Naïve algorithm, which is the most straight-forward method to encrypt every byte in Moving Picture Experts Group (MPEG) files (Agi and Gong, 1996). This method adds more latency and involves more computations. However, encryption of the whole compressed bitstream is very expensive in terms of both delay and processing time. Researchers have proposed selective encryption where partial encryption is done on selected bits of the video bitstream. This algorithm allows insertion of the encryption mechanism inside the video encoder (e.g. MEPG-2, MPEG-4, and H.264/AVC).The selected bits for encryption are chosen based on the considered video standard and according to each of their encrypted configuration to give a non-desynchronized and fully standard-compliant bitstream (Bergeron and Catherine, 2005). Moreover, video bitstreams are typically huge even after compression, and current data encryption and decryption algorithms are relatively slow. Thus, using these encryption techniques to encrypt the whole video bitstream increases the overall processing time drastically, going beyond 1/30 of a second per frame, leading to higher computational overhead. Currently, researcher is focusing a lot of attention on secure digital media over the network. The field of multimedia security is growing extremely fast. In order to deal with the problem of processing overhead and to meet the security requirements of real-time video applications with high quality video compression, several encryption algorithms to secure video streaming have been proposed (Salah, 2003; Habib and Pong, 2006; Halawa and Elkamchouchi, 2008), as follows:

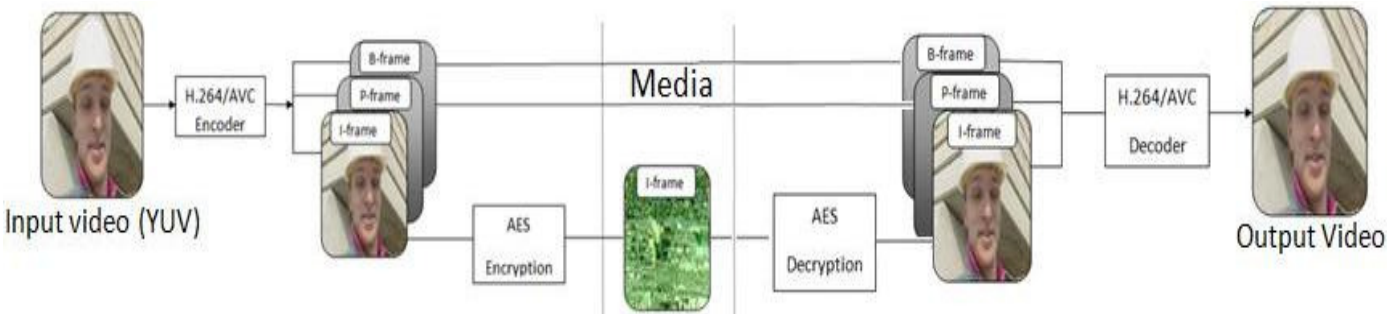

Figure 1. Diagram of the proposed selective encryption method.

1. Pure permutation algorithm which simply scrambles the bytes within a frame of an MPEG stream by permutation. It is extremely useful in situations where the hardware decodes the video, but decryption must be done by the software.
2. Zig-Zag permutation approach maps the individual 8×8 block to a 1×64 vector using a random permutation instead of mapping 8×8 blocks to a 1×64 vector in a Zig-Zag order using a random permutation list (secret key).
3. Video encryption algorithm: Bhargava et al. (1996, 1998) introduced four different video encryption algorithms: Algorithm I, Algorithm II (VEA); Algorithm III (MVEA); and Algorithm IV (RVEA).

The joint video team (JVT) finalized the draft of the new coding standard for formal approval submission as H.264/AVC and was approved by ITU-T in March 2003 (Richardson, 2007). Researchers started work to make the H.264/AVC bitstream secure. Most of them tried to optimise the encryption process with respect to the encryption speed, and the display process. Yuanzhi et al. (2006) proposed an encryption scheme which is based on the analysis of the H.264/AVC entropy coding system, and adaptive to digital right management (DRM). (Nithin et al., 2007) presented a novel H.264 selective encryption algorithm that encryptes sign bits of transform coefficient and motion vector to allow secure transcoding with decryption. Yajun et al. (2007) designed a new selective encryption scheme based on H.264.

PROPOSED ENCRYPTION SCHEME

Selective encryption can enable new system functionality such as allowing the preview of content since particular parts of the bitstream are encrypted. For selective encryption to work, it needs to rely on a characteristic of the compression algorithm to concentrate on important data relative to the original signal in a relatively small fraction of the compressed bitstream. These important components of the compressed data become candidates for selective encryption. In the proposed selective encryption, for an I-Frame bitstream of H.264/AVC, the bitstream is encrypted to minimize computational complexity and provide new functionalities. In the meantime, it provides reasonable security of the bitstream. The block diagram of the proposed selective encryption is shown in Figure 1. The input video is first compressed by the H.264/AVC encoder. The output bitstream of the H.264/AVC encoder consists of individual types of data, the video frames (pixels), Intra frame, inter frames, etc.

Aside from protecting video streams, the design of video encryption algorithm should consider real-time requirements and compression ratio. Furthermore, the encrypted bitstream should also prevent error propagation. Based on early selective encryption algorithms, the features of the latest video coding standard H.264 and the requirements of video encryption algorithm design, this study proposes a new scheme in which the H.264/AVC and the AES encryption algorithms are combined. A global overview of the proposed method is shown in Figures 2 and 3. Moreover, in selecting key coefficients of the encryption scheme, the encryption algorithm is also very important, as it will affect the security and compression ratio directly. The encryption algorithm of this proposed system is as follows: The basic idea of the scheme is to encrypt I-frames bitstream of the H.264/AVC encoder using AES in block cipher mode with a key of 128 bits. Figure 2 presents the main encoding/encryption process. After the encryption key K is generated, the main encryption part is processed. The H.264/AVC encoder reads the input video frames (frame by frame). (Notice that by default, the first input frame is considered as I-Frame). Once the target of the frame shown as I-Frame is the encryption, galorithms is called. The main encryption process consists of an XOR operation. The original frame is $XORed$ with secret key, $(X = I - frame's\ bitstream \oplus K)$, where $\oplus$ is XOR operation. The encrypted bitstream is then written to the encoder data file. The inverse operations are the decryption process of decoding the encoded frames back to their original form. Figure 3 represents the main decryption/ decoding process. The input encode

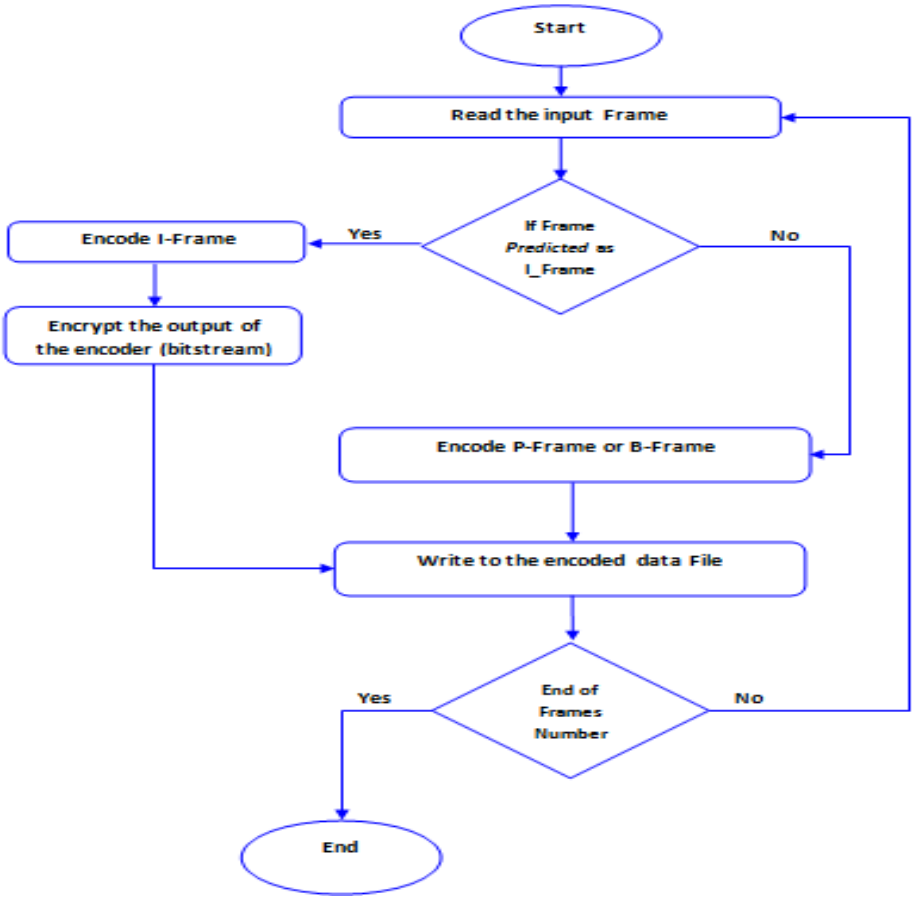

Figure 2. Block diagram of encoder/encryption function.

bitstreams would be read by the decoder if the frame target is I-frame. The decryption function is called and it uses the same encryption key to decrypt back the encrypted bitstreams. The encoded bitstream (I-Frame) is partially encrypted using an AES block cipher with a 128 bit key size, which is XOR-ed with the cipher key to generate the cipher data, while keeping the rest of the data unencrypted because it is believed that encrypting the I-Frame only is more significant due to the fact that conceptually, P- and B- frames are useless without knowing the corresponding I-frame. In the proposed system, the bits to be encrypted were chosen with respect to the considered video standard to ensure that full compatibility is achieved by selecting the bit (I-Frame bitstream) for which each of the encrypted configurations negligibly modifies the decoding process contexts in a sense where its introduction neither creates de-synchronization nor leads to non-compliant bitstream. As such, an encryption operation leading to a change of symbol table used in the coding process is not negligible, as opposed to an encryption operation that leads to interpreting a given I-frame's bits. In each case, it is important to note that the bits should maintain this capacity in every coded bitstream, and that it cannot be envisaged to consider cases where given configurations of bitstream will allow immediate or delayed resynchronization. Our interest in choosing the way of encryption is performed as the following:

1. Ensures the compatibility with the requirements of the considered video standard.
2. Makes it difficult for cryptanalysis attacks to find an angle to break the encryption key, as it is aimed at making all solutions possible, hence removing the possibilities to rule out some cases based on non-respect of standard syntax.

SELECTIVE ENCRYPTION TESTING AND EVALUATION

Let us consider a single video frame (image) composed of M×N pixels (where M is the width and N the height of the image), where each image is in the YUV colour space. The YUV format is typically sub-sampled and for this work, the 4:2:0 formats have been used. The Peak-Signal-to-Noise-Ratio (PSNR) is used to measure image quality. In the simulation, quarter common intermediate format (QCIF) video sequences with 128 × 144 pixels

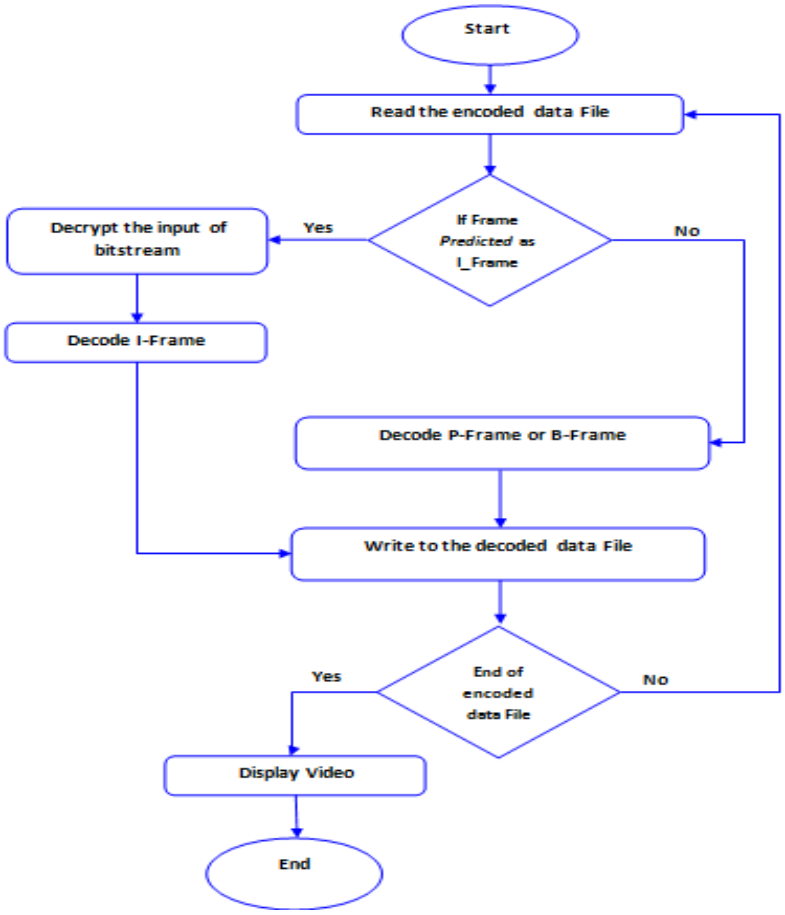

Figure 3. Block diagram of decryption/decoder function.

(Crowd) and 288×252 pixels (Foreman) were used.

Simulations were carried out on the first 297 frames of the 'Foreman' sequence and 31 frames of the 'Crowd' sequence.

Effect of encryption on the video quality

For the effect of encryption on the video, the Peak-Signal-to-Noise Ratio (PSNR) was tested with only decoded/unencrypted I-Frame video and the decoded/decrypted I-Frames video. Figures 4 and 5 show the PNSRs of the decoded video with encrypted I-Frames, as well as the decoded video with decrypted I-Frames.

In the encrypted video, the PNSRs are all lower than those of the decrypted videos, showing difference of at least 25 dB. However, the PNSRs in the encrypted videos are slightly higher at certain points due to the high motion-like movement. Likewise, it was noticed that in the encrypted videos, there is a drastic decrease in the PNSR at every I-frame. When all the I-Frames in the video sequence of the tested video clips had been encrypted, it was noticed that the security level had increased significantly. Figure 6 shows a reconstructed video frame after encrypting an I-Frame bitstream. Assuming that an attacker does not have access to the encryption key in encrypting the I-Frame bitstream, the encrypted bitstream values are arithmetically decoded and the corresponding decoded bits depend on earlier results and corrupt the subsequently required decoding states. Therefore, the reconstructed video is a noise-like pattern. From the results, it can be concluded that encrypting the I-Frame hides the content of each frame in the video clip. However, when these frames were put in motion, it was noticed that the movement could be clearly recognized. In the case of the "Crowd" video clip, the movement of the persons could easily be recognized but the details of the persons were not clear as shown in Figures 7 and 8. The same thing is true for the "Foreman" video clip, where the motion of the men could be recognized while their details, as well as background could not be recognized.

SECURITY OF THE PROPOSED SCHEME

There are two aspects to the security of an entire video

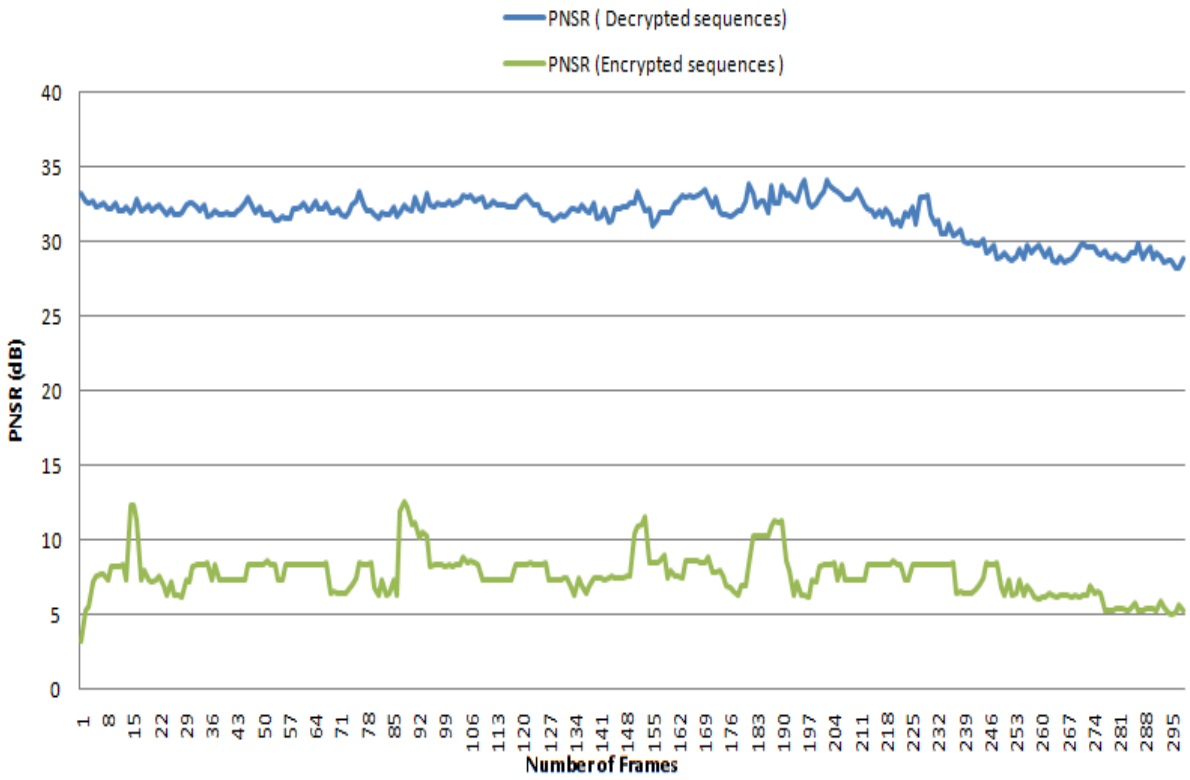

Figure 4. PSNR of 297 frames taken from the 'Foreman'sequence.

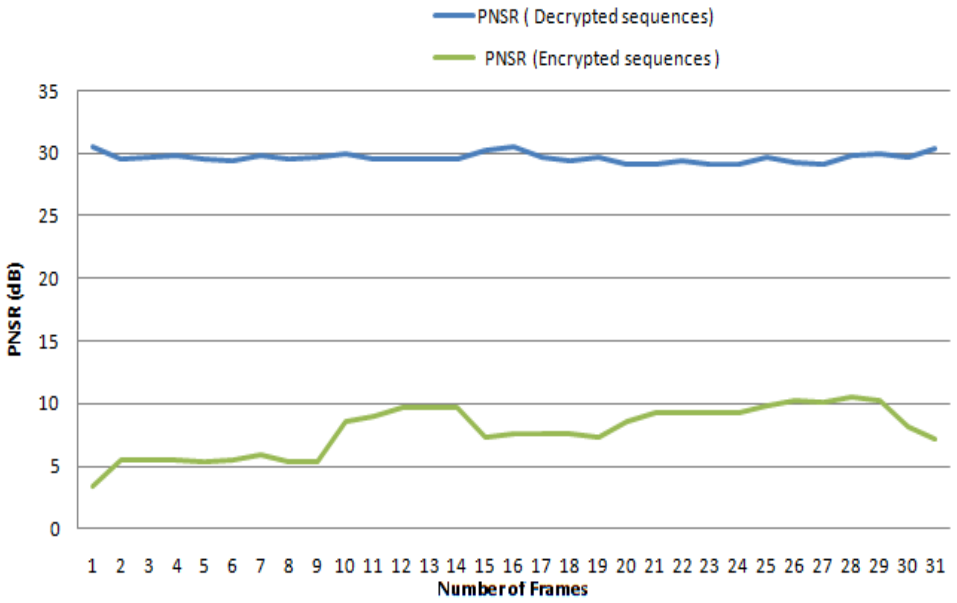

Figure 5. PSNR of 31 frames taken from the 'Crowd' sequence.

encryption approach: (a) Security of the cipher in use itself; (b) The importance and suitability of the data subjected to encryption. The security is rated as low, medium, and high. It may have the additional property of being scalable, depending on the amount of data encrypted. With respect to the two aspects of security, two entirely different types of attacks on image and video encryption are possible. In the case of partial or selective

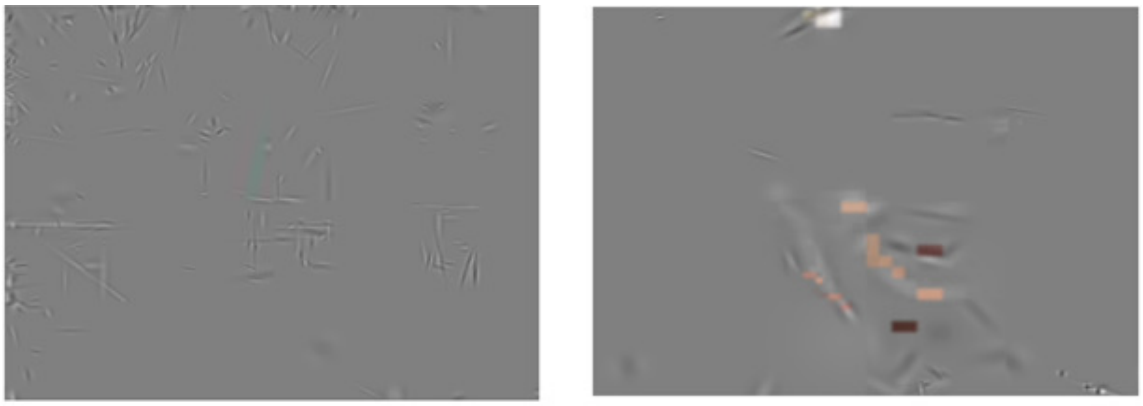

Figure 6. Visual examples of the selective encryption when the I-frames are encrypted.

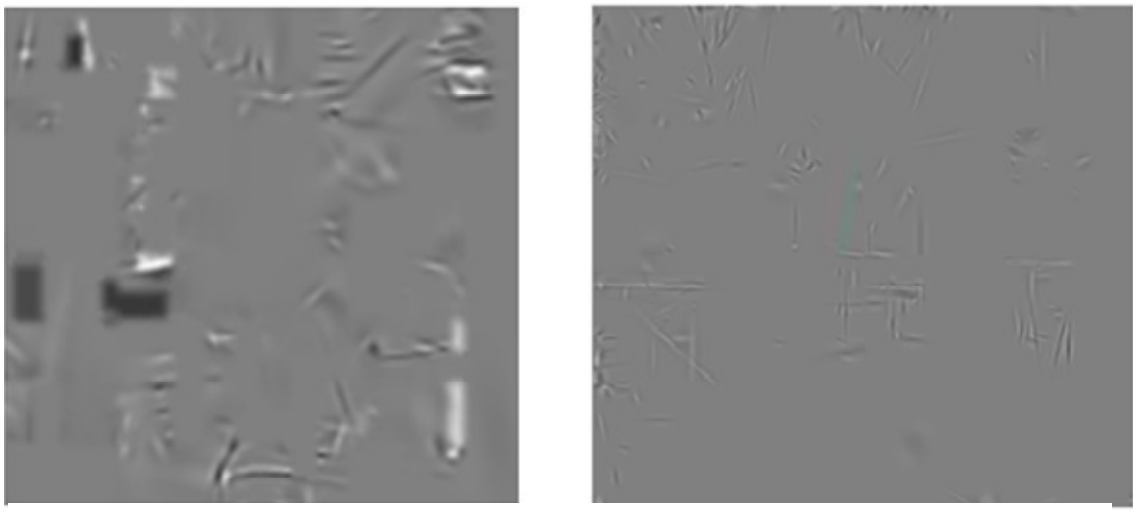

Figure 7. Visual examples of the selective encryption when decoding and the I-Frames are encrypted.

encryption, it is possible to reconstruct the visual content without taking into consideration the encrypted parts. Depending on the importance of the encrypted data for visual viewing, the result may range from entirely incomprehensible to just poor or reduced quality. In any case, when making direct reconstruction, the high frequency noise originating from the encrypted portions of the data is propagated into the reconstructed frame.

Security of the encryption scheme

An encryption scheme is implemented so that an eavesdropper will learn nothing at all about the plaintext if the encoded bitstream is statistically independent of the source messages. There are two basic approaches concerning the security of a cryptosystem: computational security, and unconditional security. Computational security concerns the computational effort to break a cryptosystem. We can define a cryptosystem to be computationally secure if the best algorithm for breaking it requires at least N operations, where N is a specified very large number. The problem is that there is no known practical cryptosystem that has proven to be secure under this definition. In practice, a cryptosystem can be considered computationally secure if the best known method of breaking the system requires an unreasonably large amount of computing time. A cryptosystem is defined to be unconditionally secure if it cannot be broken, even with infinite computational resources

Decoding and I-frames are encrypted
PSNR = 11.36 dB

Decoding and I-frames are encrypted
PSNR = 7.39 dB

Figure 8. Visual examples of the selective encryption when encrypted.

(Johnson et al., 2004). The cipher in this system is generally considered to be very secure. AES is a very powerful standard cipher (Wang et al., 2007) as no practical attack on AES has ever been published or reported. It can also prevent a timing analysis attack, and effectively resist known plaintext attacks. Meanwhile, it is almost impossible to completely get plaintext of a quarter common intermediate format (QCIF) (288×252) frame even if the plaintexts are the same because at present, there is no practical method to achieve the same ciphertext. In our security analysis, we replaced the cipher key with many other keys and we tried to decode and decrypt the encoded sequence with those keys. Our simulation results show, however, that the reconstructed video is a noise-like pattern, as shown in Figure 7. With a key size of 128 bits, it is perfectly secure against ciphertext-only cryptanalysis. This means that an attacker cannot compute the plaintext from the ciphertext without knowledge of the key, even via a brute-force search of the space of all keys. Trying all possible keys does not help at all because all possible plaintexts are equally likely to be decryptions of the ciphertext. This result is true regardless of how few bits the key has or how much one knows about the structure of the plaintext.

Security of the encrypted I-Frame

Decoding a partially encrypted video image by treating the encrypted data as being unencrypted leads to images been severely degraded by noise-type patterns. Using these images to judge the security of the system leads to misinterpretations since a hostile attacker can be much better. In particular, an attacker could simply ignore the encrypted parts, which can be easily identified by statistical means, or replace them by typical non-noise data (Uhl and Pommer, 2005). Figures 8 and 9 clearly show that there can still be information left in the unencrypted parts (which represent the motion data) of the data after selective encryption has been applied because in the case of direct reconstruction, this is hidden by the high frequency noise pattern. A defect of many investigations of visual data encryption is the lack of qualifying the quality of the visual data that can be obtained by attacks against encryption. The reason is the poor correlation of PSNR and other simple quality measures and perceived quality, especially for low quality images. For the simplest attack, the visual examples may even be related to meaningful numerical values (Thomas et al., 2007). Assuming the cipher in use is unbreakable, we conducted the first attack by directly reconstructing the selectively encrypted video data. The encrypted parts introduced noise-type distortions. Hence, we replaced the encrypted frames by artificial data mimicking typical images. The encrypted I-Frames were replaced by some other frames and subsequently, reconstruction was performed as usual, treating the encrypted and replaced parts as non-encrypted.

Figure 9 shows image reconstructions as obtained by the replacement attack. Direct reconstruction of an image after replacing some of the encrypted I-frames suggests this setting is safe with PNSR quality. The replacement attack reveals that structural information is still present in the reconstructed image with about 13 to 15 dB. However, the visual information becomes severely estranged. The visual appearance in some frames where it is put in motion has been significantly improved by the replacement attack. In any case, even if a replacement

Figure 9. Visual examples for the efficiency of the replacement attack.

attack is mounted, encrypting I-frames bitstream leads to perfectly satisfying results. However, the complexity of this attack increases significantly if the number of I-Frames which are encrypted is too many, and also the reliability of the result is drastically reduced. Thus, it seems that a relatively high amount of I-Frames needs to be encrypted to realize reasonable security.

Conclusion

We conclude that the proposed encryption scheme in this paper is a secure selective algorithm for use with H.264 and leads to an unintelligible bitstream.

The implementation of a video encryption scheme based on the H.264/AVC encoder and the ASE encryption technique has shown that the encryption of I-Frames has been effective and reveals no useful information in the reconstructed video. Hence, the proposed method has some advantages over conventional full data encryption methods, with regard to complexity. It has no effect on compression ratio. Overall, it is suitable for a secure transmission of videos. The video encryption scheme was tested in a simulated environment to evaluate its performance. The result shows that I-Frame encryption may be more suitable for applications, where the quality of the transcoded sequence is paramount, such as in digital video broadcasting (DVB). For real-time systems that demand high-speed processing, the complexity of I-frames encryption may prove to be too high due to the large volume of data to be encrypted.

ACKNOWLEDGEMENTS

We would like to express our appreciation to all those who have helped us in understanding the importance of knowledge and showed us the best ways to obtain it.

REFERENCES

Abomhara M, Khalifa OO, Zakaria O, Zaidan, AA, Zaidan BB, Rame A (2010a). Video Compression Techniques: An Overview “, J. Applied Sci., 10(16): 1834-1840.

Abomhara M, Khalifa OO, Zakaria O, Zaidan AA, Zaidan BB, Alanazi HO (2010b). "Suitability of Using Symmetric Key to Secure Multimedia Data: An Overview." J. Applied Sci., 10(15): 1656-1661.

Agi I, Gong L (1996). An empirical study of MPEG video transmissions. Proceedings of the Internet Society Symposium on Network Dist. Syst. Security. (SNDSS ’96), pp. 137-144.

Ahmed H, Kalash H, Allah F (2007). Encryption Efficiency Analysis and Security Evaluation of RC6 Block Cipher for Digital Images. Int. J. Comp. Inform. Syst. Sci. Eng., pp. 33-39.

Ahmed MA, Kiah MLM, Zaidan BB, Zaidan, AA (2010). "A Novel Embedding Method to Increase Capacity and Robustness of Low-bit Encoding Audio Steganography Technique Using Noise Gate Software Logic Algorithm.", J. Appl. Sci., 10(1): 59-64.

Alanazi HO, Jalab HA, Alam GM, Zaidan BB, Zaidan AA (2010a). Securing Electronic Medical Records Transmissions over Unsecured Communications: An Overview for Better Medical Governance. J. Med. Plants Res., 4(19): 2059-2074.

Alanazi HO, Kiah MLM, Zaidan BB, Zaidan AA, Alam GM (2010b), "Secure Topology for Electronic Medical Record Transmissions", Int. J. Pharmacol., 6(6): 954-958.

Alam GM, Kiah, MLM, Zaidan, BB, Zaidan, AA, Alanazi, HO (2010). "Using the features of mosaic image and AES cryptosystem to implement an extremely high rate and high secure data hidden: Analytical study", Sci. Res. Essays, 5(21): 3254-3260.

Sameer BHA, Kiah MLM, Zaidan AA, Zaidan BB, Alam GM (2011). Securing Peer-to-Peer Mobile Communications Using Public Key Cryptography: New Security Strategy. Int. J. Phys. Sci., 6(4):930-938.

Bergeron C, Catherine LB (2005). Complaint Selective encryption for H.264/AVC video streams. Workshop on Multimedia Signal Processing, IEEE 7th, Shanghai, China. pp. 1-4.

Cheng H, Li X (2000). Partial encryption of compressed images and videos. IEEE Trans. signal processing. pp. 2439-2451.

Deniz T, Cem T, Nurşen S (2007). Selective encryption of compressed video files. International Scientific Conference. pp. 1-4.

Fang S, Kehui S, Yongqi C (2008). An Efficient MPEG Video Encryption Scheme based on Chaotic Cipher. 2008 Congress on Image Signal Proc., 12-16.

Furht B, Socek D (2003). A Survey of Multimedia Security. Retrieved Feb 10, 2009, from http://socek.net/pubs/furht_iec2004.pdf

Habib Mir MH, Pong MT (2006). Encryption of MPEG Video Streams. 2006 IEEE Region 10 Conference TENCON 2006. 10(12): 1-4.

Halawa A, Elkamchouchi HM (2008). A Novel MPEG Video Encryption Scheme for Protecting MPEG Coded Video in Collaborative Domains. 25th National Radio Sci. Conf., (NRSC 2008). pp. 1-10.

Harris S (2007). CISSP® All-in-One Exam Guide. McGraw-Hill.

Hmood Ali K, Zaidan BB, Zaidan AA, Hamid AJ (2010a). An Overview on Hiding Information Technique in Images", J. Appl. Sci., 10(18): 2094-2100.

Hmood Ali K, Hamid AJ, Kasirun ZM, Zaidan AA, Zaidan BB (2010b). "Hiding Data in Video File: An Overview", J. Appl. Sci., 10(15): 1644-1649.

Hmood Ali K, Hamid AJ, Kasirun ZM, Zaidan BB, Zaidan AA (2010c). On the Capacity and Security of Steganography Approaches: An Overview ", J. Appl. Sci., 10(16): 1825-1833.

Hmood AK, Jalab HA, Kasirun ZM, Zaidan AA, Zaidan BB (2010d) .On the accuracy of hiding information metrics: Counterfeit protection for education and important certificates", Int. J. Phys. Sci., 5(7): 1054-1062.

Johnson M, Ishwar P, Prabhakaran V, Schonberg D, Ramchandran K (2004). On compressing encrypted data. IEEE Trans. on signal proc., 2(52):2992- 2006.

Kessler GC (1998). An Overview of Cryptography. Retrieved 20 Des, 2008, from http://www.garykessler.net/library/crypto.html#intro.

Massoudi A, Lefebvre F, Vleeschouwer CD, Macq B, Quisquater JJ (2008). Overview on Selective Encryption of Image and Video, Challenges and Perspectives. EURASIP J. Inform. Security, pp. 1-18.

Medani A, Gani A, Zakaria O, Zaidan AA, Zaidan BB (2011 In press). Review of Mobile SMS Security Issues and Techniques Towards the Solution. Sci. Res. Essays. 6(6): 1147-1165.

Nabi MSA, Kiah MLM, Zaidan BB, Zaidan AA, Alam GM (2010). Suitability of SOAP Protocol in Securing Transmissions of EMR Database. Int. J. Pharmacol., 6(6): 959-964.

Naji AW, Zaidan AA, Zaidan BB (2009). Challenges of Hidden Data in the Unused Area Two within Executable Files. J. Comput. Sci., 5(11) 890-897.

Nithin M, Damien L, David RB, David R (2007). A Novel Secure H.264 Transcoder using Selective Encryption. IEEE Int. Conf. Image Pro., 2007, (ICIP' 2007). pp. 85-88.

Raad M, Yeasin NM, Alam GM, Zaidan BB, Zaidan AA (2010). Impact of spam advertisement through email: A study to assess the influence of the anti-spam on the email marketing. Afr. J. Bus. Manage., 4(11): 2362-2367.

Richardson I (2007). White Paper: An Overview of H.264 Advanced Video Coding. Retrieved NOV 11, 2008, from http://www.vcodex.com/files/H.264_overview.pdf

Salah A (2003). A Light-Weight Encrypting For Real Time Video Transmission. Retrieved Nov 2008, 22, from http://www.cdm.depaul.edu/legacy/checksite.aspx?oldUrl=http://www.cdm.depaul.edu/research/Documents/TechnicalReports/2004/TR04-002.pdf

Shieh JRJ (2003). On the security of multimedia video information. IEEE 37th Annual 2003 International Carnahan Conference on Security Technolo., pp. 51- 56.

Thomas M, Nithin Damien L, Bull DR, David R (2007). A Novel Secure H.264 Transcoder using Selective Encryption. IEEE Int. Conf. Image Proc., ICIP, pp. 85-88.

Uhl A, Pommer A (2005). Image and Video Encryption. From digital rights managements to secured personal comm., 233, Spring Street. NY10013.

Wang Y, Mian C, Feng T (2007). Design of a New Selective Video Encryption Scheme Based on H.264. International Conf. on Comp. Intell. Security, pp. 1-5.

Wenjun Z, Junqiang L, Xinhua Z (2006). Security for multimedia adaptation: architectures and solutions. IEEE Multimedia. pp. 68-76.

Weng L, Wouters K, Preneel B (2006). Extending the selective MPEG encryption algorithm PVEA. IEEE Intelligent information hiding and multimedia signal proc., (IIH-MSP'06). pp. 12-16.

White B (2003). Cisco Security+ Certification: Exam Guide. McGraw-Hill.

Yajun, W, Mian, C, Feng, T (2007). Design of a New Selective Video Encryption Scheme Based on H.264. 2007 Int. Conf. on Comp. Intellig. Security. pp. 1-5.

Yibo F, Jidong W, Takeshi I, Yukiyasu T, Satoshi G (2007). A New Video Encryption Scheme for H.264/AVC. pp. 246-255.

Yibo F, Jidong W, Takeshi I, Yukiyasu T, Satoshi G (2007). A New Video Encryption Scheme for H.264/AVC. pp. 246-255.

Yuanzhi Z, Tiejun H, Wen G, Longshe H (2006). H.264 Video Encryption Scheme Adaptive to DRM. IEEE Trans. Consumer Elect., pp. 1289 -1297.

Zaidan AA, Ahmed NN, Karim HA, Alam GM, Zaidan BB (2011). "Spam Influence on the Business and Economy: Theoretical and Experimental Study for Textual Anti-spam Filtering Using Mature Document Processing and Naïve Bayesian Classifier", Afr. J. Bus. Manage., 5(2):596-607.

Zaidan AA, Zaidan BB, Alanazi HO, Gani A, Zakaria O, Alam GM (2010a). Novel approach for high (secure and rate) data hidden within triplex space for executable file, Sci. Res. Essays. 5(15):1965-1977.

Zaidan AA, Zaidan BB, Taqa AY, Mustafa KMS, Alam GM, Jalab HA (2010b). "Novel Multi-Cover Steganography Using Remote Sensing Image and General Recursion Neural Cryptosystem", Int. J. Phys. Sci., 5(21): 3254-3260.

Zaidan AA, Zaidan BB, Al-Fraja AK, Jalab HA (2010c). Investigate the capability of applying hidden data in text file: An overview. J. Appl. Sci., 10: 1916-1922.

Zaidan AA, Zaidan BB, Al-Frajat AK, Jalab HA (2010d). An overview: Theoretical and mathematical perspectives for advance encryption standard/rijndael. J. Appl. Sci., 10: 2161-2167.

Zaidan, BB, Zaidan AA, Al-Frajat AK, Jalab HA (2010e). On the differences between hiding information and cryptography techniques: An overview. J. Appl. Sci., 10(15): 1650-1655.

Zaidan BB, Zaidan AA, Taqa A, Alam GM, Kiah MLM, Jalab HA (2010f). "StegoMos: A Secure Novel Approach of High Rate Data Hidden Using Mosaic Image and ANN-BMP Cryptosystem", Int. J. Phys. Sci., 5(11): 1796-1806.

Zaidan BB, Zaidan AA, Kiah MLM (2011 Inpress). Impact of Data Privacy and Confidentiality on Developing Telemedicine Applications: Review, Participates Opinion and Expert Concerns", Int. J. Pharmacol., 7(3): 382-387.