International Journal of Research in Advent Technology, Vol.3, No.5, May 2015
E-ISSN: 2321-9637

A Review on Video Encryption Techniques

Mr. Mithilesh Kumar Dewangan[1], Mr. Deepak Shrivastava[2]

[1]*M.Tech. Scholar, CSE Department, DIMAT, Raipur*
[2]*Asst.Professor, CSE Department, DIMAT, Raipur*
[1]mithilesh.dewangan@gmail.com
[2]dshrivastava76@gmail.com

Abstract-With the rapid a advancement in multimedia technology, it has become possible to generate and transmit more and more multimedia data in military commercial and medical field. Some of these data includes some sensitive information which is required to be accessed by the intended person only. Therefore, security and privacy of these information is of prime concern today. In the last couple of years several encryption methods have been proposed for secure video transmission. Though lots of algorithms of video encryption have been presented but only few are used in real time. In this paper, a brief description and comparison of different video encryption algorithm has been presented. Encryption speed, stream size and security level are used for comparing the performance of these algorithm.

Keywords- AES (Advance Encryption Standard), DES (Data Encryption Standard), Video Transmission, Video encryption

1. INTRODUCTION

Protecting the information from un-authorised individuals by converting it into a non-recognizable form is known as Cryptography. Scrambling the content of data like text audio, video and image to make it unreadable, unintelligible and invisible is known as data cryptography. Reverse operation of data encryption is called data decryption which, with the help of reverse algorithm regenerate the original data. Egypt is known to have used the cryptography first in the world. Since then cryptography undergoes different stages and development. In II- world war, cryptography played a very vital role and made the allied force upper hand and later on helped the allied force to win a war. During that war, allied forces, with the help of cryptography system deciphered the enigma cipher machine of Germany which they used to encrypt their military secret communication [1].

In modern days, cryptography is no longer limited to military operation but it is used by different organization, people and groups for securing their information from unauthorised person.

In cryptography system, original data which is to be transmitted or stored is called plain text. Plain text is readable by computer and human being. While the encrypted data or scrambled data or disguised data is

Called cipher text. Neither man nor machines are able to read the cipher text until unless it is decrypted.

Over all system which provides encryption and decryption operation is called cryptosystem.

Cryptosystem comprises of an encryption/decryption algorithm, necessary software component and key. Key is long string of bits which is used to encrypt and decrypt the data. Person who knows the key can encrypt and decrypt the information by applying it into a encryption and decryption algorithm [2] [3].

In the 19th century, Kerchhoff proposed the security principle or theory for any encryption system. This theory is the basis of cryptosystem design. Kirchhoff observed and explained that the security of ant cryptosystem does not depend on the encryption algorithm but instead on the key. Once the encryption algorithm is broken, cryptosystem is not able to protect the data or information. Key space decides the security level of the encryption algorithm. Key space is the size of key[3]. Larger size of the key made the attacker to spend more time for exhaustive search and hence make the security level higher. Key is a sequence of a random bits which is used to transform plain text in to cipher text and vice versa. Larger key size ensure the enhanced security. Now a days common key size are 128,192, and 256[3] [4].

Length of the key, secrecy of the key and initialization vector decides the strength of the encryption algorithm. Key in encryption algorithm can be categorized as the symmetric and asymmetric key. If the crypto system is useing same key for encryption and decryption key then it is calle3d symmetric key algorithm. If on the other hand two different keys are used for encryption and decryption

then it is called asymmetric key algorithm. In asymmetric key algorithm, two keys are used which are known as the public and private key.

A. Symmetric key based encryption algorithm

In symmetric key based encryption system, both sender and receiver use same key for encryption process and decryption process. Symmetric key is also called secret key because both sender and receiver has to keep it secret for proper protection of the information [4] [5]. Security strength of the symmetric key based algorithm depends on how well both sender and receiver keep the key secret.

If somehow, intruder manage to get the key then all the information can be decrypted by the intruder easily.

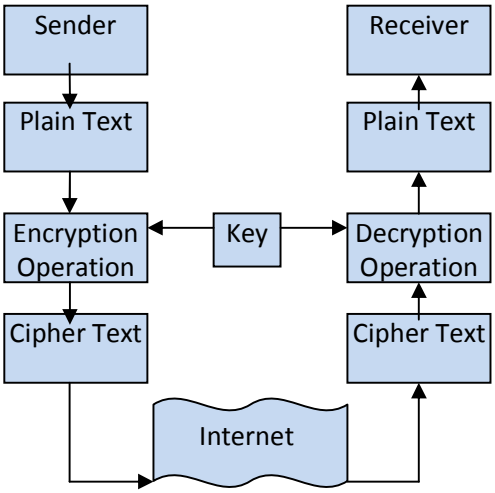

Figure1 Symmetric Key Based Algorithm

This makes the symmetric key based encryption system very complicated and these system need to be updated and shared when required. Symmetric key can ensure the confidentiality but does not ensure the authentication. In symmetric key algorithm, it is not possible to know that who actually sent the information as the symmetric key are used by the many person. Even after these drawbacks, symmetric key system is used in many application because of its fast operation and high security with large size of key. Data encryption standard(DES), triple Des and Advance Encryption standard(AES) are some example of symmetric key based encryption algorithm.

Since DES work a block of 64 bits at a time with a input key of size 64 bits, therefore it is called block cipher. Since in this method every 8 bit in the key is parity bit therefore effective size of the key in this algorithm is 56 instead of 64 bits [6] [7].

Advance encryption standard (AES) is also block cipher. This system work on 128 bit block at a time arranged as the 4 X 4 matrix with 8 bit entries. In this algorithm the block length and the key length are variable. Latest AES standard allow the key length of 128, 192 or 256 bits with block length also 128, 192 and 256.

B. Asymmetric Key based Encryption Algorithm

Asymmetric key based encryption algorithm is also called a public key algorithm. Martin Hellman, professor of Stanford university and his student Whitfield first presented the concept of public key cryptography system in 1976 [8]. They explained the two key based crypto system for securely communicating in the non-secure communication channel without sharing a secret key among each other. This eliminates the problem of secret key distribution using two different instead of single key.

In this type of system, two keys are used. One key is known as the public key and it is known to all. Second is known as the private key and known only by the owner.

There is mathematical relation between public and private key. If one key is used to encrypt the information then other key is required to decrypt the information. Though both public and private keys are mathematically related but it doesn't mean that a person who knows the public key is able to figure out the private key [4] [5].

For authentication, sender encrypt the data with his private key and all the person who possess the corresponding public are able to decrypt the information.

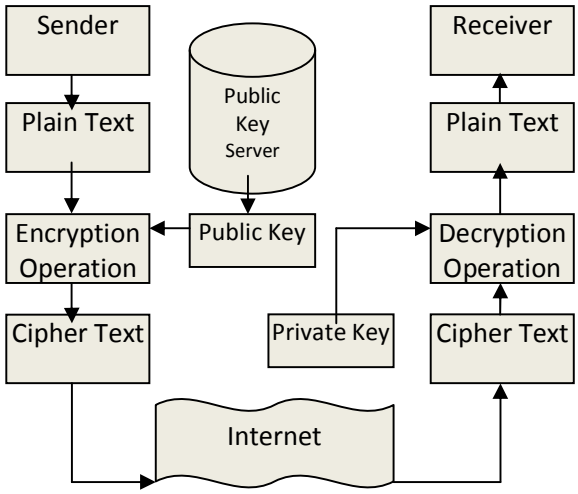

Figure2 Asymmetric Key Based Algorithm

This gives a confidence to the receiver that the information is encrypted by the private key owner only. Encrypting the information with private key is called *open message format* as this does not ensure the confidentiality of the information. Anybody who possess the public key are able to decrypt the information.

RSA (Rivest-Shamir Adelman) is the most popular asymmetric key based encryption algorithm.

2. RELATED WORK

With the introduction of video transmission through internet and wireless medium, there is need to protect these video by applying suitable video encryption methods. Unlike the digital images, digital videos are of large size so they are generally transmitted in compressed format. MPEG[9] or H.264/AVC[10] are two most popular video compression standard. Since most of the videos are in compressed domain therefore most of the video encryption methods are in compressed domain. In the past few years, video encryption field witness various different video encryption standards. Optimizing the encryption process with respect to encryption speed and display were the main focus in this field. Some of the noteworthy contribution in video encryption is discussed in the next paragraph.

a. Naïve Encryption algorithm.

In this encryption algorithm, every bytes of MPEG(Motion Picture Expert Group) video is encrypted using standard DES or AES encryption method. In naïve algorithm, MPEG bit stream is treated just as text data and it does not use any special structure of MPEG [11][12][13]. Due to its slow processing speed this method is not suitable for big size video. This makes this method unacceptable for real time implementation.

b. Permutation based encryption algorithm.

Basic principle of permutation based encryption algorithm is to scramble the byte within a frame of MPEG video by permutation. It is very useful in a situation where hardware is used to decode the video stream but decryption is done in software only.

It was Adam J. Slagell [14] who first discovered that the permutation algorithm is vulnerable to some known plain-text attack.
Therefore it is very important to handle this situation very carefully because just by comparing the cipher text with the known frames, easily exposed the secret permutation list. Once the permutation list is exposed, it will become easier to decrypt the video frames. It should also be noted that knowing only the I frames is sufficient to decrypt the permutation list.

c. Zig-Zag based permutation algorithm

In this approach[15], 8x8 block is first mapped in to a 1x64 vector with the help of random permutation list(secret key). Main steps of zig-zag based permutation method is as given below-

i. Generation of list of 64 permutations.

ii. Apply splitting procedure.

Now suppose, DC coefficients are denoted by 8 bit binary numbers as given

$$D_7\ D_6\ D_5\ D_4\ D_3\ D_2\ D_1\ D_0$$

Then it is divided into two numbers. Number represented by $D_7\ D_6\ D_5\ D_4$ is positioned to DC coefficients and number represented by $D_3\ D_2\ D_1\ D_0$ is positioned to AC coefficient.

Procedure of division or splitting is based on the following observations-

i. Value of DC coefficients are much higher than the AC coefficients.

ii. After division or splitting, extra space is needed for storing one of the spilitted numbers which hence increase the size of MPEG video. Last AC coefficient value in the block can be set to zero without degrading the quality of the video.

Since the computational complexity of zig-zag order mapping according to the permutation list is same as the alone zig-zag order complexity.

Encryption and decryption process using this method produce very little overhead of the compression and decompression process. But video compression rate gets reduced due to the facts that the random permutation disturb the probability distribution of Discrete Cosine Transform coefficients(DCT coefficients).This reduced the optimization accomplished by the Huffman table.
In 1998 L.Qiao and Nahrsted proposed two types of attack on zig zag based permutation algorithm one is the cipher only attack and the second is plain text attack.
Zig-zag based permutation algorithm can be br4oken by the ciphertext only attack. Statistical properties of the dCT coefficients are the basis of this attack. In DCT, all the non zero coefficients are gathered in the upper left corner of the I-block. Statistical analysis performed by the duo in this regard by counting the number of non zero AC coefficients and the DC coefficients. Following observation they noted-

i. DC coefficients have the highest number of non zero occurrences.
ii. Frequency of AC1 and AC2 occupy the position within top 6.
iii. Frequency of AC3 and AC5 occupy the position within 10 .

Zig Zag permutation algorithm is also vulnerable to plain text attack. If person knows certain frames of the video in advance then it can easily figure out the secret key by mere comparison of plain text with corresponding encryption frames.
Later on one of the solution of this problem is proposed which is known as binary coin flipping sequence method. In this method two different permutation list are used.

In this method, a coin is flipped for each 8x8 block, if the result is tail then permutation list(key1) is chosen to apply for the block while if the result is head then permutation list 2 is chosen to apply for the block.
Though this method can easily with stand against the cipher text only attack but again it fail against the plain text attack. Tendency of non zero AC coefficients together in the left upper corner is main reason behind it.

d. Video Encryption Algorithm

Qiao and Nahrsted in their paper[16] suggested a new method of video encryption which is called VEA. This algorithm also based on the statistical properties of the MPEG video standard. This method reduce the data to be encrypted.
In this method, first of all the input video is divided in to a chunks i.e. (a_1 a_2 a_3 $_{a4}$,.....a_{2n-1},a_{2n}).
These chunks later on divided in to two different list i.e even list and odd list. Even list contain all the odd chunks i.e. (a_1 a_3 a_5 a_7....) while the even list contain all the even chunks i.e. (a_2 a_4 a_6 .....).
In the next step, encryption key is applied to the even list E (a_2 a_4 a_6 .....), here E represents the Encryption function.
Cipher text is obtained by concatenating the encryption algorithm output XOR with the odd list. From this discussion it is clear that due to the change in key for each frame, this method has the immunity against the known plain text attack.

e. Video Encryption Algorithm (VEA)

Bhargava, Shi and Wang proposed four different video encryption method in their paper[17] [18]. These algorithms are Algorithm I, algorithm II, Algorithm III(MVEA) and Algorithm IV(RVEA).

i. Algorithm I

In algorithm I, Permutation of Huffman codeword is used in I frame for encryption. This method combine the encryption and compression in single4 step.
In this method, permutation p is used to for permuting the Huffman code word of standard MPEG format. For ensuring the compression ratio, permutation p permute the Huffman codeword with same number of bits. In [19], Daniel Socek described that this algorithm is easily decoded by known plain text and cipher text attack. Knowing some of the frame in advance can easily make it possible to figure out the secret permutation p by mere comparison of known frame with the encrypted corresponding frames. This method is also not immune to cipher text attack. Paper presented in [20] describes how it can be affected by the low frequency error attack. In this algorithm, permutation p has special characteristics that it can shuffle only those code word which are of same length. Shuffling 16 bit code word of AC coefficient entropy table gives the maximum security to this method. Since there are only few code word whose length is less than the 16 bit therefore it is not difficult to figure out all the dc coefficients and most frequent occurred AC coefficients (As these coefficients are occurring more so these coefficients can be encoded with less than 16 bit codeword). In this regard, the only difficult part is to estimate hoe permutation p shuffle the 16 bit code word.

ii. Algorithm II (VEA)

This algorithm is suggested in[18]. This method is based on tha ssumtion that the I block carry most important information about the video pixel so if some how this block is encrypted with some proper algorithm then video can be encrypted. So in this scheme only the sign bit of DC coefficients of I block are encrypted by XORing it with the secret key.
Length of the key in this method decides the security of this method. The more the better and securer. Taking too long key size is impractical and infeasible. Taking short length key make it quite insecure it because it will be easy to figure out the short secret key with known algorithm

iii. Algorithm II(MVEA)

In their paper [21], Bharagava and Shi proposed a modification to algorithm II to increase its security. Instead of encrypting the siogn bit of DC coefficients, they encrypted the differential value of the sign bit of DC coefficients of I block by XORing it with the motion vector of P and B frame along with the secret key.
One of the drawback of this system is that the proposed improvement makes the video very random and some time unacceptable for viewing. Size of the key also decides the security of this system as in the case of algorithm II(VEA).

iv. Algorithm IV(RVEA)

This method was suggested by Baraga[18]. In this method, traditional symmetric key cryptography is used to encrypt the sign bit of Dc coefficient and the sign bit of motion vector. This method improve the speed of the system by encrypting the selected sign bit in MPEG video stream. This algorithm is considered as the best among than the previous three algorithm in security front. Computational time of this method is also much lesser than the previous three approach.

f. Selective Encryption algorithm

Processing time or overhead is the main constraint in so far presented encryption algorithm. It is very important to reduce the processing time of the encryption algorithm for making the encryption suitable for ream time implementation. This method is designed to achieve this goal. The main theme of this algorithm to apply encryption on selective part of the MPEG video steam By utilizing the MPEG layered structure. i.e. applying encryption process to all the headers and all the I frames, Applying encryption process to all the I frames and all I block of B and P frames. So this method based on the I-frame, P-frame and B frame structure of MPEG. This method basically encrypt the I frames only P-frames and B-frames depends on the I frames and without I frames these frames are useless.

i. AEGIS Method(Encrypt Only I frames)

AEGIS method is introduced by the maples and Spanos [22][23] for encrypting the MPEG video stream.

This method apply encryption algorithm to only I frames of the MPEG video stream while keeping the P-frames and B-frames unencrypted. In order to enhance the security of the MPEG video stream this method also apply encryption process to sequence haeder. Sequence header has some very crucial initialization parameter about the video sequence like width and height of the video frames, bit rate, frame rate and buffer size.

Making the sequence header encrypted conceal the identity of video stream unrecognizable. In the last, IOS end code which is last 32 bit of MPEG is also encrypted for concealing the bit stream of MPEG identity.

DES encryption algorithm have been used for encryption process in this method. Iskender Agi and Li Gong in paper [24] describe that by encrypting only the I-frames does not secure some types of video. They have shown that it is possible figure out some scene from the P-frames and B-frames of the video.

Iskender Agi and Gong further explained that by encrypting the I block of B and P frames along with the I frames, security of the algorithm can be enhanced. They also explained that increasing the frequency of the I frames can enhance the security even more. Increasing length of string and hence more computational time for encryption are the drawback of this method. Even after this it can be concluded that the security offer by this method is not sufficient for the area where security is the top most priority(like in military application). But the security is enough for the pay video broadcast services as this method produce least distortion in the decrypted video.

ii. Sign Bit of DCT coefficients

Shi and Bharagava[17] are the proposer of this method. In this method a secret key is used to transform or encrypt the sign bits of the DCt coefficient of the MPEG video stream.

Secret key (k^1, k^2, k, …..k^{2m}) used in this method is of length 2m and it is randomly generated. User can use any number of keys and any length of key. If S represent the sign bit of AC and DC coefficients

$$S=(s^1, s^2, s^3, \ldots..s^{2m})$$

then encrypted data is given by

$$Ek(Si) = bi \text{ xor } si$$

This encryption method randomly change the sign bit of DCT coefficients. Decryption process Ek^{-1} is the copy of encryption process Ek i.e.

$$Ek^{-1} \text{ x } Ek=S$$

If the key length is m then 2m trial are required to find a right key. Instead of using single key, this method uses the several key to enhance the security manyfold. For a 2 key based encryption system one key is used for Y block while for Cb and Cr block, key2 is used for encryption process. Similarly in the three key system, I frames, P frames and B frames are encrypted by key1 , key2 and key3.

Selective encryption for MPEG-2 video standard is proposed by Lookabaugh [25]. This is used in most of the current digital television application.

In MPEG-2 standard, only small portion of the bits are used in important headers. This facts supports the encryption process to much extent due to the vagueness in such headers. Down part of this is that the field in such header is not able to withstand the attack even if making it obscure by applying selective encryption process. This is due to the fact that the fields are generally static and can be predictable by manipulating the other information of the video stream with available crypto-analytic tool.

iii. Byte Encryption

Byte encryption method was proposed by Griswold [26][27]. This method encrypts all the bytes of MPEG video data and transferred it to the legitimate user in encrypted form. Instead of encrypting all the bytes, this method encrypt the bytes at random positions. Authors claimed that encrypting only 1% of video data is sufficient to make the video unrecognizable. However crypto-analysis of this method showed that this method is also vulnerable to different attack.

For example consider the situation in which only header information is encrypted then it is easy to reconstruct the header information if the encoder in use is known. In this paper, different encryption based attack is also not considered. It is very important that in order to enhance the security, large number of bytes need to be encrypted.

J.Wen[28] proposed more appropriate approach for MPEG4 standard. This method is known as the syntax Unaware run-length Based selective encryption(SURSLE).

In this method, X-bits are encrypted then next Y-bits are left unencrypted, then next Z-bits are again encrypted and so on.

Both the scheme carry the above mentioned security problems and both the scheme disturb the MPEG bit stream syntax which causes the decoder to crash.

3. CONCLUSION

In this paper, a review work on video encryption standard has been presented. Symmetric key based and asymmetric key based video encryption methods were highlighted and evaluated in term of different metrics.

Three metrics i.e. Security level, encryption speed and encrypted MPEG stream size are used for evaluating the video encryption algorithms. From the discussion it is clear that Naïve algorithm and Video encryption algorithm (VEA) has the highest security while the zig-zag permutation algorithm has many security loop-holes which makes it vulnerable to known plain text and cipher text attack. As far as speed is concern, zig-zag permutation algorithm is the winner as it is the fastest among all the algorithms discussed in this paper. Naïve algorithm is slowest algorithm due to the DES encryption method. In term of stream size metric, VEA, Naïve and permutation method preserve the original stream size while zig-zag permutation method increase the size of stream

significantly. From the discussion and comparison it is clear that video encryption algorithm (VEA) meets most of the multimedia application requirement. This method preserve the size, provide better encryption speed and guaranteed high security.

REFERENCES

[1] Kahn, David , (1980). Cryptology Goes Public, Communications Magazine, IEEE, available from: http://ieeexplore.ieee.org/iel5/35/23736/01090200.pdf (Accessed December 28, 2008).

[2] Kessler , Gary C., (1998). An Overview of Cryptography, available from: http://www.garykessler.net/library/crypto.html#intro. (Accessed December 28, 2008).

[3] B. White, Gregory, (2003). Cisco Security+ Certification: Exam Guide, McGraw-Hill.

[4] shon harris, (2007). SICCP Exam Guide, fourth edition, McGraw-Hall

[5] Stallings, William, (2007). Network Security Essentials, applications and Standards , Pearson Education, Inch.

[6] Wayne G. Barker, "Introduction to the analysis of the Data Encryption Standard (DES)", A cryptograph-ic series, Vol. 55, p. viii + 190, Aegean Park Press, 1991.

[7] Kofahi, N.A., Turki Al-Somani, Khalid Al-Zamil. "Performance evaluation of three encryption/decryption algorithms" 2005 IEEE International Symposium on Micro-NanoMechatronics and Human Science, Publication Date: 30-30 Dec. 2003. Volume: 2, pp 790-793.

[8] Diffie , Whitfield & Hellman, Martin E, (1976) . New Directions In Cryptography, IEEE TRANSACTIONS ON INFORMATION THEORY, available from: http://www-ee.stanford.edu/~hellman/publications/24.pdf. (Accessed on Decemper 28, 2008).

[9] MPEG Technology Group, \http://www.chiariglione.org/mpeg/," (Accessed on March 2, 2009).

[10] Ostermann, J., Bormans, J., List, P., Marpe, D., Narroschke, M., Pereira, F., Stockhammer, T., Wedi, T. "Video coding with H.264/AVC: tools, performance, and complexity. IEEE circuits and system magazine , Vol 4,issue 1 , pp. 7-28, 2004.

[11] Salah Aly. A Light-Weight Encrypting For Real Time Video Transmission. Available from http://www.cdm.depaul.edu/research/Documents/TechnicalReports/2004/TR04-002.pdf. (Accessed on March 2, 2009).

[12] S. Lian, Multimedia Content Encryption: Techniques and Applications. CRC, 2008.

[13] C.-P. Wu, C.-C. J. Kuo, "Design of integrated multimedia compression and encryption systems," IEEE Trans. Multimedia, vol. 7, no. 5, pp. 828-839, 2005.

[14] Adam J. Slagell. Known-Plaintext Attack Against a Permutation Based VideoEncryption Algorithm. Available from http://eprint.iacr.org/2004/011.pdf .(Accessed on March 2, 2009).

[15] L. Tang, For encrypting and decrypting MPEG video data efficiently," in Proceedings of The Fourth ACM International Multimedia Conference (ACM Multimedia'96), (Bosten, MA), pp. 219{230, November 1996.

[16] L. Qiao and K. Nahrstedt, \A new algorithm for MPEG video encryption," in Proceedings of The First International Conference on Imaging Science, Systems, and Technology (CISST'97), (Las Vegas, Nevada), pp. 21{29, July 1997.

[17] C. Shi and B. Bhargava, "A Fast MPEG Video Encryption Algorithm," Proceedings of the 6th International Multimedia Conference, Bristol, UK, September 12-16, 1998.

[18] C. Shi, S.-Y. Wang and B. Bhargava, "MPEG Video Encryption in Real-Time Using Secret key Cryptography," 1999 International Conference on Parallel and Distributed Processing Techniques and Applications (PDPTA'99), Las Vegas, NV, June 28 - July 1, 1999.

[19] T. Seidel, D. Socek, and M. Sramka, "Cryptanalysis of Video Encryption Algorithms ," to appear in Proceedings of The 3rd Central European Conference on Cryptology TATRACRYPT 2003, Bratislava, Slovak Republic, 2003.

[20] T. Seidel, D. Socek, and M. Sramka, "Cryptanalysis of Video Encryption Algorithms ," to appear in Proceedings of The 3rd Central European Conference on Cryptology TATRACRYPT 2003, Bratislava, Slovak Republic, 2003.

[21] B. Bhargava and C. Shi, "An Efficient MPEG Video Encryption Algorithm", IEEE Proceedings of the 17th Symposium on Reliable Distributed Systems, 1998, Pages 381 – 386.

[22] T.B. Maples and G.A. Spanos, "Performance study of selective encryption scheme for the security of networked real-time video," in Proceedings of the 4th International Conference on Computer and Communications, Las Vegas, NV, 1995.

[23] G.A. Spanos and T.B. Maples, "Security for Real-Time MPEG Compressed Video in Distributed Multimedia Applications," in Conference on Computers and Communications, 1996, pp. 72-78.

[24] Iskender. Agi and L. Gong, \An emprical study of MPEG video transmissions," in Proceedings of The Internet Society Symposium on Network and Distributed System Security, (San Diego, CA), pp. 137{144, Febuary 1996.

[25] T. Lookabaugh et al., \Selective encryption of MPEG-2 video," in Proceedings of the SPIE Multimedia

Systems and Applications VI, (Orlando, FL), September 2003.

[26] C. Griwotz, \Video protection by partial content corruption," in Proceedings of Multimedia and Security Workshop at the 6th ACM International Multimedia Conference, (Bristol, England), pp. 37{39, 1998.

[27] C. Griwotz, O. Merkel, J. Dittmann, and R. Steinmetz, \Protecting vod the easier way," in Proceedings of Multimedia and Security Workshop at the 6th ACM International Multimedia Conference, (Bristol, England), pp. 21{28, 1998.

[28] J. Wen, M. Severa, W. Zeng, M. Luttrell, and W. Jin, \A format compliantcon¯gurable encryption framework for access control of video," IEEE Transactions on Circuits and Systems for Video Technology, vol. 12, pp. 545{557, June 2002.