IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 3, March 2016

A Review on Video Encryption Technologies

Keshav S. Kadam[1], Prof. A.B. Deshmukh[2]

PG Student, SKNCOE Vadgaon (Bk) Pune, Maharashtra, India[1]

Assistant Professor, SKNCOE Vadgaon (Bk) Pune, Maharashtra, India[2]

Abstract: Security and privacy are important things in video communication for that reason from last few years different video encryption methods have applied to secure video transmission. large number of multimedia encryption schemes have been proposed and some of them are used in real products, cryptanalytic work has shown the existence of security problems and other weaknesses in most of the proposed multimedia encryption schemes .This review paper describe different video encryption method also give the comparison between encryption methods with respect not only to their encryption speed but also their security level and stream size. A trade-off between quality of video streaming and choice of encryption technologies is shown here. Flexibility, efficiency, security and privacy are the challenges for the design.

Keywords: Video encryption, video transmission, stream size.

I. INTRODUCTION

Cryptography is science in which information is transmitted securely by encryption and decryption of the data. so that unauthorized user cannot use these data. Cryptography is used in insecure network like internet so only intended recipient get the data. Data cryptography is nothing but scrambling of the content of data, such as text, image, audio, video make the data unreadable, invisible or unintelligible during transmission or storage called Encryption. The main aim of cryptography is to keep data secure form unauthorized attackers. The reverse process of data encryption is data Decryption by which data comes original data. Cryptography methodology is used in the World War II. For instance cryptography played an important role and was a key element that gave the allied forces the upper hand, and enables them to win the war sooner. When Egyptian force were able to dissolve the Enigma cipher machine which the Germans used to encrypt their military secret communications [1]

In modern days cryptography is used not only to secure sensitive military information but considered as one of the major components of the security policy of organizations and considered as industry standard for providing information security, trust, electronic financial transactions and controlling access to resources. The information which unprocessed or which is visible to all is called as plaintext. Processed information for security i.e. encrypted data is called as cipher text. Cipher text is unreadable until it is decrypted. The system in which encryption as well as decryption process is done is called cryptosystem. Cryptosystem uses an encryption algorithms which determines how simple or complex the encryption process will be, the necessary software components and the key, which works with the algorithm to encrypt and decrypt the data [2].

A famous theory has been proposed by Kerchhoff about the security principle of any encryption system. This theory state that security level of an encryption algorithm is measured by the size of its key space The larger size of the key space is, the more time the attacker needs to do the exhaustive search of the key space, and thus the higher the security level. this theory play an important role in designing a cryptosystem for researchers and engineers. Kirchhoff explained in his theory that if the encryption algorithms are known to the opponents. Thus, the security of an encryption system should rely on the secrecy of the encryption/decryption key instead of the encryption algorithm. For even though in the very beginning the opponent doesn't know the algorithm, the encryption system will not be able to protect the ciphertext once the algorithm is broken.

II. CRYPTOGRAPHY ALGORITHMS

There are two type of Cryptographic algorithm 1st is symmetric algorithms, which use symmetric keys also called secret keys and 2nd is asymmetric algorithms, which use asymmetric keys i.e. public and private keys.

A. Symmetric key Algorithms

In this algorithm same key is used for encryption and decryption and the key is only known to the sender and receiver so that symmetric key also called as secret key[3].So that security level of the symmetric keys encryption method is totally depending users how well they keep it. If the key is known by an attacker, then all data encrypted with that key can be decrypted.

Example of symmetric key algorithms are Data Encryption Standard (DES), Triple DES, and Advance Encryption standard (AES).

1) The Data Encryption Standard (DES)

In 1973 NIST issued a public request for a cryptographic algorithm become a national standard .The winning standard was developed at IBM, as a modification of the previous system called LUCIFER which is DES. DES is one of the most important examples of a block cipher. Namely, it breaks the plaintext into blocks of 64 bits, and encrypts each block separately. It is widely used for encryption of PIN numbers, bank transactions etc[3]

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 3, March 2016

2) Advance Encryption Standard (AES)
In 1997,NIST called for submissions of a new standard which replace DES. At the end of 2001 NIST selected winner out off 15 and chosen the Rijndael cryptosystem as the Advanced Encryption Standard (AES) [3]. the Rijndael cryptosystem uses 128-bit blocks, which arranged as 4 × 4 matrices with 8-bit entries. the latest specification allowed any combination of keys lengths of 128, 192, or 256 bits and blocks of length 128, 192, or 256 bits so it means that variable block length and key length.

B. Asymmetric key Algorithms
Public Key Cryptography was first described by Martin Hellman and Whitfield Diffie publicly in 1976.They explained two-key cryptographic system in which communication could be secure over a non-secure communications channel and it didn't require to share a secret key. they Address the problem of secret key distribution by using two keys instead of a single key. Asymmetric key algorithm is also called as public key algorithm. In public key algorithm two keys are used one is public key, which can be known by everyone and another is private key, which should be kept secret only known by the owner. The most popular asymmetric key algorithm is Rivest-Shamir Adelman (RSA)[4].

1) Rivest- Shamir Adelman
In public key algorithms today RSA is one of the most used algorithm. This algorithm was invented by Ron Rivest, Adi Shamir, and Len Adelman in 1977. The RSA is based mathematical operation i.e. factorization of integers into their prime. Assume tht A and B want to communicate with one other. let B chooses two distinct large primes p and q and multiplies them together to form N, N = p*q. He also chooses an encryption exponent e, such that the, greatest common divisor of e and [(p-1)*(q-1)] is 1. That is GCD(e,[(p-1)*(q-1)])=1. He computes his decryption key d, d=1/e (mod [(p-1)*(q-1)]). Now he makes the pair (N,e) public and keeps p and q secret. This how to Generating keys, Encryption and decryption are of the following form, for some plain text block M and ciphertext block C: C=Me mod n, M=Cdmod n = (Me) mod n = Medmod n Both sender and receiver must know the values of n and e, and only the receiver knows the value of d. this make a public key encryption of KU = {e,n} and private of KR {d,n}.

Following figure show the tree diagram of cryptographic algorithm.

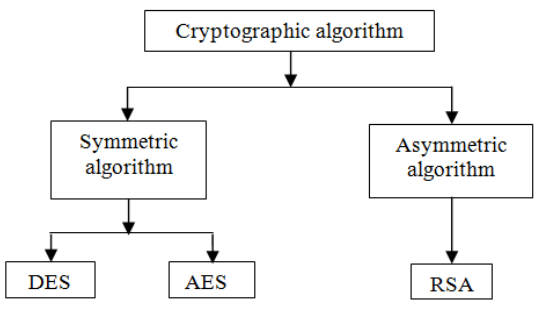

Fig.1 Tree diagram for Cryptographic algorithm

III. SURVEY OF VIDEO ENCRYPTION METHODS

With digital video transmission, encryption methodologies are needed that can protect digital video from attacks during transmission. Due to the huge size of digital videos, they are usually transmitted in compressed formats such as MPEG, or H.264/AVC [5]. Thus, the encryption techniques used for digital video are usually working in the compressed domain. Several encryption techniques to secure video streaming have been proposed. Most of them tried to optimize the encryption process with respect to the encryption speed, and display process.

C.-P. Wu, C.-C. J. Kuo in "Design of integrated multimedia compression and encryption systems," introduced most straight-forward method to encrypt every byte in the whole MPEG stream using standard encryption schemes such as DES or AES. Here naïve algorithm is used in which MPEG bit-stream work as text data and does not use any of the special structure. Security level of entire MPEG stream by standard encryption schemes so it high secure method of encryption. But this method is not applicable solution for big video; as it take too much time which not acceptable over real time communication [6]

Adam J. Slagell. In " Known-Plaintext Attack Against a Permutation Based Video Encryption" introduced The idea of encryption i.e by pure permutation method in which simply scrambles the bytes within a frame of MPEG stream by permutation. This method is extremely useful in situation where the hardware decodes the video while data decrypted by software.

This is vulnerable to known-plaintext attack, by comparing the ciphertext with the known frames, the attacker could easily figure out the secret permutation list. If Permutation list is figured out then all frames could be easily decrypted. [7]

L. Tang, in "encrypting and decrypting MPEG video data efficiently" introduced The advanced permutation approach for encryption by using a random permutation list (secret key) it maps the individual 8x8 block to a 1x64 vector instead of mapping the 8x8 block to 1x64 vector in "Zig-zag" order. Random permutation list have the same computational complexity like encryption and decryption add very little overhead to the video compression and decompression processes. Also this method decrease the video compression. Zig-Zag permutation method is vulnerable to the ciphertext only attack, the attack relies on the fact of statistical properties of the DCT coeffient, where none-zero AC coefficients are gathered in the upper left corner of the I-block[8]

L. Qiao and K. Nahrstedt, in "A new algorithm for MPEG video encryption," suggested a new video encryption method called VEA.This method uses the statistical properties of MPEG video standard and symmetric key algorithm standard to reduce the amount of data that is encrypted. Thus this method secure from known-plaintext attack, because the key will be changed for each frame(s).[9]

C. Shi and B. Bhargava in "A Fast MPEG Video Encryption Algorithm," have introduced video encryption by using the permutation of Huffman code words in I-frames. By this method encryption and compression done in one step. The secret part of the method is a permutation p which is used to permute standard MPEG Huffman codeword list. To save compression ratio, the permutation p permutes the code words with same number of bits. But Daniel Socek, and el in [11] showed that the this method is highly unsecure to both known plaintext attack, and cipher text-only attack. If same video frames known in advance to enemy could easily figure out and reconstruct the secret permutation p by comparing the known frames with the encrypted frames[10]

B. Bhargava and C. Shi, "An Efficient MPEG Video Encryption Algorithm" have made an improvement to previously suggested method Instead of encrypt only the sign bite of DC coefficient in the I-frame block, the sign bite of the differential. values of DC coefficient and motion vectors in P-frames and B-frames can is encrypted by XORs them with the secret key. This type of improvement makes the video playback more random and more un viewable. So the security level is relies on the secret key size.[12]

G.A. Spanos and T.B. Maples in "Security for Real-Time MPEG Compressed Video in Distributed Multimedia Applications," have introduced a new secure MPEG video mechanism called Aegis. This method encrypts only the I-frame of all MPEG groups of frames in MPEG video stream and B-frame and P-frame are unencrypted.

To make the MPEG video stream more secure Aegis also encrypts the sequence header which contains all of the decoding initialization parameters. But the drawback of this method is that it is not highly secure so it is not used in application where security has high priority like military or teleconferencing. This method is sufficient for entertainment videos.[13]

C. Griwotz, in "Video protection by partial content corruption, "have proposed to a method in which randomly encryption of bytes in an MPEG stream for free distribution and original bytes at the corresponding positions are transferred in encrypted form to authorized users. It is nothing but encrypting byte at random positions.

The authors said that encrypting 1% of the data is sufficient to make a video detectable or at least invisible. But the cryptanalysis given is entirely insufficient. By considering the worst case If by chance only MPEG header data is encrypted using this approach.

Then header data may be reconstructed easily provided the encoder in use is known. Also in this paper no attack scenario is considered but while playing the protected video in a standard decoder is covered. So to guarantee a certain level of security, a more amounts of bytes need for encryption and efficient selection of bytes for encryption are considered [14]

IV. COMPARISONS OF VIDEO ENCRYPTION SCHEME

Sr. no.	Authors	Methods	Security	Speed	Size	Encryption Ratio
1	C.-P. Wu, C.-C. J. Kuo[6]	Naïve approach	High	Slow	No change	100%
2	Adam J. Slagell[7]	Pure Permutation	Low	Super fast	No change	100%
3	L. Tang[8]	Zig-Zag Permutation	Very Low	Very fast	Big increase	100%
4	L. Qiao and K. Nahrstedt[9]	VEA	High	Fast	No change	50%
5	C. Shi and B. Bhargava[10]	Permutation of Huffman code words	Moderate	Fast	No change	100%
6	C. Shi and B. Bhargava[12]	Permutation of Huffman code words	High	Fast	No change	100%
7	G.A. Spanos and T.B. Maples[13]	AEGIS mechanism	low	Fast	Increase	10%-90%
8	C. Griwotz[14]	Byte-Encryption	moderate	Fast	Increase	1%-100%

V. CONCLUSION

In this paper a survey of the known method of cryptography were presented. Two type encryption standard Symmetric key encryption and Asymmetric key encryption were explained and analyzed with respect to their security level and encryption speed. also the advantages and disadvantages of each of them are discussed. In the third part of paper different video encryption technologies for video streams encryption were described. Naïve approach and video encryption algorithm are the most secure method, while zig-zag permutation has serious security flaws. With the respect to encryption speed, pure permutation and zig-zag permutation mechanism are very fast, and Naïve approach is very slow specially while applying DES on whole video. So finally we can say that there trade-offs when applying different encryption methods to MPEG video stream and its choice rely on the applications.

ACKNOWLEDGMENT

Author would like to thanks to Prof. A. B. Deshmukh for his support as a project guide, co-operation and valuable suggestions.

REFERENCES

[1]. Kahn, David,(1980).Cryptology Goes Pulic, Communications Magazine, IEEE, available from http://ieeexplore.ieee.org/iel5 /35/23736/01090200. pdf?tp=& is number= &arnumber=1090200. (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]. Shon harris, (2007). SICCP Exam Guide, fourth edition, McGraw-Hall

[4]. 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).

[5]. Ostermann, J., Bormans, J., List, P., Marpe, D., Narroschke, M., Pereira,F., Stock hammer, T., Wedi, T. "Video coding with H.264/AVC: tools, performance, and complexity. IEEE circuits and system magazine, Vol4,issue 1 , pp. 7-28, 2004.

[6]. 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.

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

[8]. 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.

[9]. 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.

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

[11]. 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.

[12]. 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.

[13]. 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.

[14]. 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.