Video Encryption Using Cryptography – A Review

Sarla[1], Anuj Kumar[2], Deepthi Sehrawat[3]

[1]M.TECH Student, Amity University, Haryana

[2,3]Asst. Professor, Amity University, Haryana

Abstract: **With the rapid development of the technologies, the multimedia data are generated and transmitted over the network. The security of the data from the unauthorized access over the network is the major issue. We are using several applications for the communication, the images, videos and other data are shared by us with our friends or in the social community. The encryption methodologies are needed that can protect videos from attacks during transmission. Our main issue of the paper is to discover and study the approaches for securing video files from unauthorized access. So we study and discuss about the security of the video files and suggest some future suggestions.**

Keywords**: video security, video encryption, key, encryption and decryption**

I. INTRODUCTION

With the growth of multimedia technologies many applications are popularized like video-on demand (VOD), video conferencing, video calling etc. for video on demand the low level of security is required whereas for the military purposes and financial information high level of security is required. For the real world applications a video encryption algorithm has to take in account various parameters like security, computational efficiency and compression efficiency etc. The confidentiality of the video data during transmission is main issue. The one way of protecting data, video and other information is to stop the unauthorized view. The original data that to be transmitted or stored is called plaintext, the one that can be readable and understandable either by a person or by a computer. Whereas the disguised data so-called cipher text, which is unreadable, neither human nor machine can properly process it until it is decrypted. A system or product that provides encryption and decryption is called cryptosystem. Cryptosystem uses an encryption algorithms which determines how simple or complex the encryption process will be, the necessary software component, and the key (usually a long string of bits), which works with the algorithm to encrypt and decrypt the data [1] [2]. The Cryptography is the process of keep the data secure from the unauthorized access. In cryptography the encryption is done on the plain text to create the cipher text and decryption is just opposite of it.

From fig-1 any plaintext can be hidden inside the curve image and other sources. For this purpose there is a need of private key to encrypt the plaintext to Ciphertext. Similarly for decrypting ciphertext to plaintext enter the same key which was used for encrypting the text.

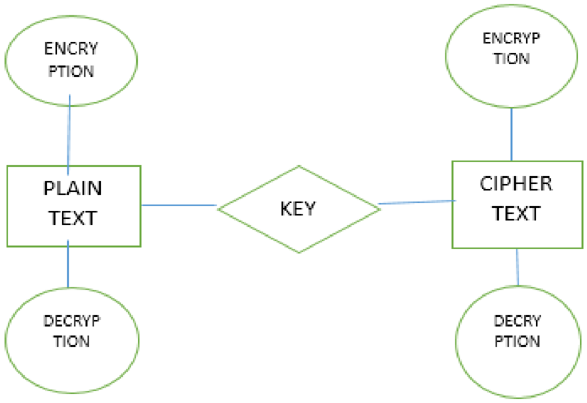

FIG-1. Cryptographic System Process.

II. TYPES OF ATTACK

There are numerous techniques for performing cryptanalysis, depending on what access the cryptanalysis has to the plaintext, cipher text, or other aspects of the cryptosystem. Below are some of the most common types of attacks:

2.1 Known-plaintext analysis

with this procedure, the cryptanalyst has knowledge of the plaintext from the cipher text. Using this information, the cryptanalyst attempts to deduce the key used to produce the cipher text.

2.2 Chosen-plaintext analysis

The cryptanalyst is able to have any plaintext encrypted with a key and obtain the resulting cipher text, but the key itself cannot be analyzed. The cryptanalyst attempts to deduce the key by comparing the entire cipher text with the original plaintext. The Rivest-Shamir-Adelman encryption technique has been shown to be somewhat vulnerable to this type of analysis.

2.3 Cipher-only analysis

The cryptanalyst has no knowledge of the plaintext and must work only from the cipher text. This requires accurate guesswork as to how a message could worded. It helps to have some knowledge of the literary style of the cipher text write and/or the general subject matter.

2.4 Man-in-the-middle attacks

This differs from the above in that it involves tricking individuals into surrendering their keys. The attacker places him or herself in the communication channel between two parties who wish to exchange their keys for secure communication.

2.5 Timing/differential power analysis

This is a new technique made public in June 1998, particularly useful against the smart card that measures differences in electrical consumption over a period of the time when a microchip performs a function to secure information.

III. CONCEPT OF VIDEO ENCRYPTION

When the two parties communicate to each other via encryption they need an algorithm, with data they use the single key or the two different keys to encrypt/decrypt the data.

3.1. Single Key

The sender and the receiver use the single key for encryption and decryption both sender and receiver keep the key secret into it [3][4]. Into it the security level is depend on how well the key is protected. If the key is known by any other then all the encrypted data with that key is decrypted. It is known as symmetric key algorithm. The symmetric key algorithm can provide confidentiality but cannot provide the authentication because if two people are encrypted the data with the same key we cannot recognized that who actually sends the data. It is fast and using the large key size for data encryption. The most common algorithm which uses the symmetric key algorithm are Data Encryption Standard (DES), Triple DES and Advance Encryption Standard.

3.1.1. Data Encryption Standard (DES)-

DES is the example of the block cipher. DES is develop at IBM, as as a modification of Previous system called LUCIFER in 1977. It is widely used for bank transactions, PIN numbers etc. It operates on blocks of 64 bits at a time, with an input key of 64 bits. Every 8th bit in the key is a parity check bit which means that in fact the key size is effectively reduced to 56 bits.[11]

3.1.2. Advance Encryption Standard (AES)

In November 2001 Rijndael introduce a new cryptosystem as the Advance Encryption Standard (AES). It operaes on 128-bit blocks, arranged as 4*4 matrices with 8-bit entires. The algorithm use the variable block length and key length; it allow combination of keys lengths of 128, 192, or 256 bit and block of length 128, 192, or 256. [3][12]

3.2. Public key

In the two key crypto system the sender and receiver using the two different keys one key is used to encrypt the data which is the public key and known to everyone and other key is used to decrypt the data is known as the private key which is known to only owner. The both keys are mathematically related to each other [3]. It is known as the asymmetric key algorithm.
The asymmetric key algorithm provides the confidentiality as well as the authentication because the public key known to everyone but the private is known to only the receiver is provide the confidentiality. To provide the authentication the private key is used to encrypt the data so the receiver knows that the person who has the private key is encrypt the data and the data is secured to the unauthorized access. The popular encryption algorithm by using the asymmetric key algorithm are Rivest-Shamir Adelman (RSA) and Elliptic Curve Cryptography (ECC).

3.2.1. Rivest-Shamir Adelman (RSA)

RSA is one of the most used public key algorithms today. This algorithm was invented in 1977 by Ron Rivest, Adi Shamir, and Len Adelman. The RSA is based on the idea of factorization of integers into their prime. Assume that Alice and Bob want to communicate with one other. Bob 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 cipher text 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}.

3.2.2. Elliptic Curve Cryptography (As discussed in section 3.3)

3.3 Elliptic Curve Cryptography (ECC)

Elliptic curves (EC) were suggested for cryptography by Victor Miller and Koblitz in 1985 in the form of Elliptic Curve Cryptography (ECC)[10]. ECC Follows Public

Key encryption Technique and the security provided is based on the Discrete Logarithm Problem (DLP). One main advantage of ECC is that it provide same level of security with the smaller key size.
It uses the elliptic curve for the cryptography which consist of the point satisfying the equation:

$$y^2 = x^3 + ax + b$$

The public key cryptographic system involves arithmetic operations on Elliptic Curve over finite fields which is determined by elliptic curve domain parameters.

3.3.1 Elliptic Curve Cryptography parameters

ECC make use of elliptic curves in which the variable and coefficients are all restricted to elements of a finite field [4]. Two families of elliptic curve are used:

3.3.1.1. Prime Curve over Zp

it uses a cubic equation in which variable and coefficient all taken on values in the set of integers from 0 to p-1 and calculations are performed modulo p.

y^2 mod p $= (x^3 + ax + b)\ mod\ p$

The prime curve are best for the software applications.

3.3.1.2. Binary Curve over GF (2^m)

It also uses the cubic equation in which variable and cofficients all taken on values in GF (2^m) and in calculations are performed over GF (2^m).

$y^2 + \mathrm{xy} = x^3 + ax + b$

The binary curves are best for hardware applications, where it takes remarkably few logic gates to create a powerful, fast cryptosystem.

3.3.2 Elliptic Curve Encryption/ Decryption

The encryption/decryption system or the key exchange system requires a point G and a elliptic group Ep(a,b) as parameters. [4]
m – Plain text message

P_m – x- y point

Let a user A select a private key n_A and generates a public key.

$P_A = n_A \times \mathrm{G}$

To encrypt and send a message P_m to B(another user) , A a uses a random positive integer and produce the cipher text C_m

$C_m = \{ \mathrm{kG}, P_m + \mathrm{k}\, P_B \}$

A has used the B's public key P_B. To decrypt the ciphertext, B multiplies the first point in the pair by B's secret key and subtract the result from the second point:

$P_m + \mathrm{k}\, P_B - n_B(\mathrm{kG}) = P_m + \mathrm{k}(n_B\mathrm{G}) - n_B(\mathrm{kG}) = P_m$

3.3.3 Security of Elliptic Curve Cryptography

The security of ECC depends upon how difficult it is to determined key. For equal key size, the computational effort required to ECC and RSA is comparable. Thus, there is a computational advantage to using ECC with a shorter key length than a comparably secure RSA.

IV. RELATED WORK

There are various paper available in many journals which are based on the video encryption. Some of them are as:-

4.1 M. Abomhara, Omar Zakaria, Othman O.khalifa [5] proposed that all videos are needed to be protected from the unauthorized access. To solve this problem many encryption techniques have been discussed in this paper. Into this paper comparison between encryption and representative video encryption algorithms are discussed. It discussed this aspect to show their encryption speed, security level and stream size.

4.2 Jolly Shah and Dr. Vikas Saxena [9] proposed the classification of encryption algorithm in two categories. Full Encryption and the partially or selective encryption. The full encryption requires the more computational cost and has less speed due to large data to be encrypted. Whereas the partial encryption encrypt the byte within video frames, it reduces the computational complexity. The classification is also done on the basis of various performance parameters such as Encryption ratio, Cryptographic security, Compression Friendliness.

4.3 Amit Pandey, Prasant Mohapatra, Joseph Zambreno [6] proposed encryption in video and image using chaotic maps. It is based on the encryption scheme based on the arithmetic coding, which gives the Chaotic Arithmetic Coding (CAC). In this paper, a large number of chaotic maps can be used to perform coding, each achievingShannon optimal compression performance. The exact chaotic maps are given by the key. It allow encryption without any hindering any coding efficiency.

4.4 Mayank Arya Chandra, Dr. Ravinder Purwar, Dr. Navin Rajpal [7] proposed a new scheme for video encryption which based on encryption of video frame. Into this researcher has taken an idea from matrix calculation for generating the I-frame. Into it we collect all the frame, and then take frame one by one and add a frame as a key frame for encryption and decryption process. So the video frames are send as secure channel with this key frame. After that these encrypted video frames are combined and make a video which is in encrypted frame, send it from simple channel.

4.5 Lekha Bhandari, Mr. Avinash Wadhe [8] propose a computational efficient and secure video encryption algorithm. The proposed scheme is very fast, possesses good security and add less overhead on the code. The techniques for data security are not appropriate for the current multimedia so, we need to develop new protocol. In this paper, implemented elliptic curve cryptography

(ECC) and RC5 algorithm are mentioned. On comparing with RSA based encryption the main problem is the key size.

V. PERFOMANCE ANALYSIS

TABLE.1 Comparisons of cryptographic algorithms

Algorithm	Complexity	Speed	Memory Requirement	Key type	Key length	Key space size	Security level
DES	Complex	High	Not required	Private key (Symmetric key)	56 bits, 48 bits sub-key	2^{56}	Low
AES	Complex	High	Very Low	Private key (Symmetric key)	128 bits, 192 bits, 256 bits	2^{128}, 2^{192}, 2^{256},	High
RSA	Simple	High	Not required	Public key (Asymmetric key)	Variable	Variable	High
ECC	Simple	High	Very low	Public key (Asymmetric key)	Variable	Smaller key size	Very High

VI. CONCLUSION

In this paper various encryption techniques are discussed for the proposed to safely exchange highly confidential video. Two different type of encryption methods are discuss Symmetric and Asymmetric key algorithm, which are highlighted the security level according to their key size and encryption speed. The algorithm using the DES and AES algorithm which is symmetric algorithm using the single key for encryption and Decryption Whereas the RSA algorithm based on the Asymmetric key Algorithm which uses the two keys, public key for encryption and private key for decryption which is more secure. The principal of using ECC compared to RSA is that it offers equal security for a smaller key size, and reducing processing overhead. It provide high level of security with a good computational speed.

REFRENCES

[1]. Kessler, Gray C, (1998). An Overview of Cryptography, available from: http://www.garykessler.net/library/crypto.html #intro.

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

[3]. Shon Harris, (2007). SICCP Exam Guide, fourth edition, McGraw-Hall

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

[5]. M. Abomhara, Omar Zakaria, Othman O. Khalifa " An Overview Of Video Encryption Techniques", International Journal of Computer Theory and Engineering, Vol. 2, No.1 February, 2010 1793-8201

[6]. Amit Pande, Prasant Mohpara, Joseph Zambreno,"Using Chaotic Maps for Encryption Image and Video Content", 2011 IEEE International Symposium on Multimedia.

[7]. Mayank Arya Chandra, Dr. Ravindra Purwar, Dr. Navin Rajpal, "A Novel Approach of Digital Video Encryption", International Journal of Computer Applications (0975- 8875) Volume 49 No.4,july 2012

[8]. Lekha Bhandari, Avinash Wadhe, "Speeding up Video Encryption Using Elliptic Curve Cryptography (ECC)", International Journal of Emerging Research in Management & Technology, Volume-2, Issue-3 March 2013.

[9]. Jolly Shah and Dr. Vikas Saxena, "Video Encryption: A survey", International Journal of Recent Trends in Engineering, IJCSI

International Journal of Computer Sciences Issues, Vol. 8, Issue 2 March 2011 ISSN (Online): 1694-0814.

[10]. Randhir Kumar, Akash Anil, "Implementation of Elliptic Curve Cryptography", Internatioanl Journal of Computer Science, Volume 8, No-2, Issue- July 2011.

[11]. Wayne G. Barker, "Introduction to the analysis of the Data Encryption Standards (DES)", A Cryptographic Series, Vol. 55,p. viii + 190,Aegean Park Press, 1991.

[12]. Jean-Yves chouinard, Design of secure computer systems CSI4138/CEG4394 notes on the advanced encryption standards (AES), available from : http://www.site.uottawa.ca/~chouinar/Handout_CSI4138_AES_200.pdf.