Speeding up Video Encryption using Elliptic Curve Cryptography (ECC)

Lekha Bhandari [*]
M.E (CSE) 2nd Semester
Department of Computer Science & Engg.
G.H Raisoni College of Engineering, Amravati University

Mr.Avinash Wadhe
M-tech (CSE)
Department of Computer Science & Engg.
G.H Raisoni College of Engineering, Amravati University

Abstract— Advances in digital content transmission have been increased in the past few years. Security and privacy issues of the transmitted data have become an important concern in multimedia technology. In this paper, we propose a computationally efficient and secure video encryption algorithm. This makes secure video encryption feasible for real time applications without any extra dedicated hardware. In addition, special and reliable security in storage and transmission of digital images and videos is needed in many digital applications such as confidential video conferencing and medical imaging systems, etc. Unfortunately, the classical techniques for data security are not appropriate for the current multimedia usage. As a result, we need to develop new security protocols or adapt the available security protocols to be applicable for securing the multimedia applications. In this paper implementation of elliptic curve cryptography (ECC) and RC5 algorithm are mentioned. RSA based encryption has significant problems in terms of key size. Currently, the RSA algorithm requires the key length of at least 1024 bits for long term security, whereas it seems that 160 bits are sufficient for elliptic curve cryptographic functioning.

Keywords - Video encryption, ECC, RC5, Prime Field, MPEG.

I. INTRODUCTION

Advances in multimedia technologies have popularized applications like video conferencing, pay-per-view, Video-On Demand (VOD), video broadcast, etc. In such applications, confidentiality of the video data during transmission is extremely important. This necessitates secure video encryption algorithms. In the naive approach for video encryption, the MPEG stream (bit sequence) is treated as text data, and encrypted using standard encryption algorithms like DES (Data Encryption Standard), RC5 (Rivest Cipher), AES (Advanced Encryption Standard), etc. Though this approach is supposedly the most secure for video encryption, it is computationally infeasible for real time applications. Encryption for the video bit stream should be designed to be lightweight and format compliant. Since video decompression on the handheld devices is constrained by the limited power and other computation resources, conventional ciphers such as data standard encryption (DES) or advanced m encryption standard (AES) to wireless applications over handheld devices are intensive computation tasks. Therefore, it is not efficient to apply conventional ciphers for wireless multimedia applications. Selective encryption algorithms are proposed to be an economical and secure video encryption algorithm where only I-frames are encrypted. However, it has been reported as not good choices in the encryption of digital video since encrypting I-frames alone may not be sufficiently secure for digital video. ECC is one of the most used public key algorithms today. ECC based on the Discrete Logarithmic problem over the points on an elliptic curve. The principal attraction of ECC compared to RSA is that it offers equal security for a far smaller key size, thereby reducing processing overhead. The ECC has received considerable attention from mathematicians around the world, and no significant breakthroughs have been made in weaknesses in the algorithm.

II. RELATED WORK

Avinash P. Wadhe , N.A.Chavhan [1] has proposed that ECC has attracted much attention as the security solutions for wireless networks due to the small key size and low computational overhead. For example, 160 bit ECC offers the comparable security to 1024 bit RSA. They said that the implementation of ECC on primary field performance will increase substantially.

Trupti Dandamwar, Manish Narnaware [2] said that the secured networked continuous media requires the video streams over a network in a real time and requires that the transmitted frames are sent with a limited delay. Also, video frames need to be displayed at a certain rate; therefore, sending and receiving encrypted packets must be achieved in a certain amount of time utilizing the admissible delay. To achieve this they introduced a procedure for Encryption and Decryption of videos, also they introdused the concept of video transmission using parallel and distributed approaches.

Hao Wang and Chong-wei Xu [3] proposed a new lightweight, efficient, scalable and format compliant video encryption algorithm based on the DCT coefficients scrambling. They mentioned that the proposed encryption algorithm is based on the concept of permutation group. Scrambling DCT coefficients of the permutation groups maintains the statistical property of DCT distribution so that the encryption does not suffer from DCT vulnerability attack.

C. Narsimha Raju, Ganugula Umadevi, Kannan Srinathan and C. V. Jawahar [4] have proposed a computationally efficient, yet secure video encryption scheme. It uses RC5 for encryption of the DCT coefficients. The proposed scheme is very fast, possesses good security and adds less overhead on the codec. It slightly decreases the compression rate of the video, which is negotiable for higher security.

Davis Pan [5] said that the MPEG compression algorithm is the first international standard for digital compression for high-fidelity audio. MPEG is one part of three part compression standard. The MPEG standard addresses the compression of synchronized video and audio.

Dr. S.R. Ely [6] said that MPEG has been outstandingly successful in defining the standards for video compression coding, serving a wide range of applications, bit rates, qualities and services. The standards are based upon a flexible toolkit of techniques of bit rate reduction. The picture quality obtained through an MPEG codec depends strongly upon the picture content, but as experience with MPEG coding grows, the bitrates needed for a given picture quality is likely to reduce.

III. WORKING OF ECC

A. Introduction to ECC Cryptosystem

Cryptographic applications require fast and precise arithmetic. So elliptic curve groups over the finite fields are used in practice. The protocol described in this paper depends on the security of the elliptic curve primitive known as ECDH key generation function. This function utilizes the arithmetic of points which are elements of the set of solutions of an elliptic curve equation defined over a finite field. Following are the Operations Used in ECC:

- Point: An ordered pair of scalars satisfying the elliptic curve equation is called a point, denoted as P(x,y).
- Elliptic Curve Group: The set of solutions of the elliptic curve equation together with a special point called point at infinity form.
- Point Multiplication: The Multiplication of an elliptic curve point P, by an integer e will be denoted by K*P.

It is equivalent to adding P to itself K times, which yields another point on the curve. Elliptic Curve Cryptography (ECC) is a public key cryptography. The principal attraction of ECC compared to RSA is that it offers equal security for a far smaller key size, thereby reduces the processing overhead. Consider wireless mesh network, where authentication scheme require less computation overhead. Basically ECC is based on algebraic structure of elliptic curve over finite fields. An elliptic curve over a finite field GF (a Galois Field of order P) is composed of a finite group of points where integer coordinates (xi, yi) satisfy the long Weierstrass form: y2 + a1xy + a3y = x3 + a2x2 + a4x + a6.

B. ECC key Generation

An elliptic curve consists of the points satisfying the equation:

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

Where x, y, a and b are elements in GF (P) (a Galois Field of order, where P is a prime). Each choice of (a, b) yields a different elliptic curve. For example, Figure 1 shows an elliptic curve of $y^2= x^3 +7x$.

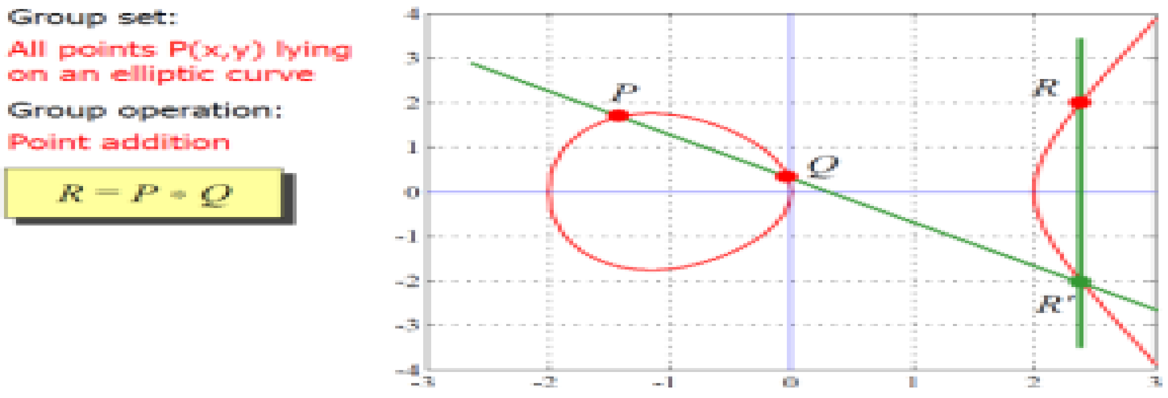

Figure 1: Elliptic curve and point addition

In case of the prime field arithmetic; the point addition and point doubling operations require computation of multiplicative inverse, which is an expensive operation. For Point addition: Let E (Fp) be an elliptic curve over the prime field Fp, where p > 3. Given two points **P** = (x_1, y_1) and **Q** = (x_2 , y_2) on E (Fp), where **P** ≠ ±**Q,** the addition **P+Q** = (x_3 , y_3) is obtained as follows:

$x_{3,}= \beta^2 - x_{1,} - x_{2,}$

$y_3=\beta (x_{1,}- x_{3,}) - y_1$ where $\beta = (y_2 - y_1) / (x_{2,} - x_{1,})$

The cost of above affine coordinate formula is one Inversion, two Multiplications and one Subtraction i.e. (1I+2M+1S)

For Point doubling:

Let E (Fp) be an elliptic curve over the prime field Fp, where p > 3. Given two points

P = (x_1, y_1) on E (Fp) where **P** ≠ −**P** the doubling **2P** = (x_3 , y_3) is obtained as follows:

$x_3 = \beta^2 - 2x_1$

$y_3 = \beta\,(x_1 - x_3) - y_1$ **Where** $\beta = {}^{3x_1^2}\!/_{2y_1}$.

C. Video encryption

MPEG video data is often compressed using DCT. Each video frame is divided into sub images and then DCT is applied on each 8 × 8 block. After coding, the 64 transformed coefficients are zigzag ordered such that the coefficients are arranged approximately in the order of increasing frequency. These DCT transform coefficients can be classified into two groups, DC and AC. The DC coefficient is the mean value of a block. All other coefficients describe the variation around this DC value and these are referred to as AC coefficients. However, most of the energy is contained in the DC and a few AC coefficients. In order to apply classical encryption algorithms, we perform statistical analysis to find out the variation in DCT coefficients in a video block. For various video streams, Figure 2 shows the stack bar occupied by different range of DC coefficients.

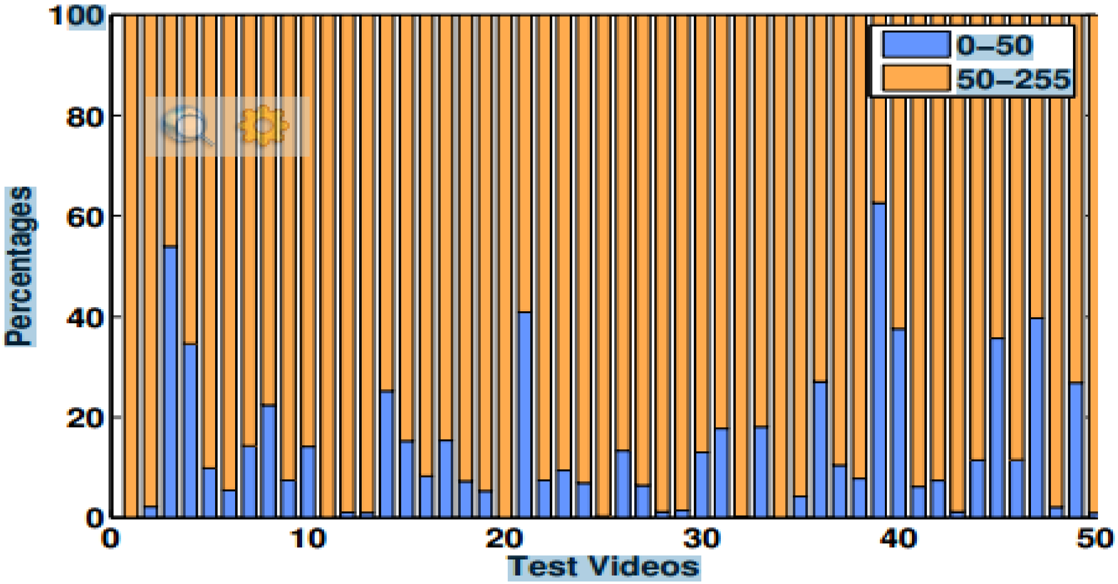

Figure 2: Percentage Variation Plot of DC Coefficients

Observed from the figure that each stack bar is predominant with orange color, this pertains to the DC range of 50-255. Similarly dark blue color pertains to DC range of 0-50. From this it can be inferred that a high percentage (86.53%) of the DC coefficients values lie in the range of 50-255. Note that there could be isolated blocks and frames with high frequency DC values, but the average over a video clip is in the range 50 − 255 most of the time. Similar analysis is conducted on the AC coefficients. Since the variation of the AC is quite different from the DC, we changed the ranges accordingly. We observed that around 94.04% of the ACs lie in the range of 0 to 20. This is due to the fact that lower frequency AC coefficients carry less energy [4].

IV. Video Encryption Using ECC And RC5

This section of the paper describes the proposed encryption scheme using ECC and RC5. Though we can use any of the algorithms like DES (Feistel Structure), RC5 for encryption, we used RC5 to encrypt the DCT coefficients. RC5 has following suitable characteristics: it is a block cipher with varying block size (32, 64 or 128 bits), varying key size (0 to 2040 bits) and variable number of rounds (0 to 255) (so that the user can choose the level of security appropriate for his application). It is a fast block cipher with a simple and easy to analyse structure. It also has adaptable word size in order to suit processors of different word lengths and flexibility of changing the parameters easily.

Figure 3 shows the block diagram of the encryption process. Our approach uses RC5 [4] algorithm with key size of 128 bits and 20 rounds of operation. The pre-processing step of our algorithm is shown in Algorithm 1. The look up table generated is used in the encryption and decryption stages of the algorithm. It is never modified in the entire process of encryption/decryption.

```
Algorithm 1:
Pre-processing step: Look up Table Construction:
    Step 1: Generate all the combinations of quadruples from −20 to 20.
    Step 2: Encrypt each quadruple using the ECB mode of RC5 encryption.
    Step 3: Use the list of coefficients and their encrypted values as a look-up table for encryption of the AC coefficients.
```

Algorithm 2:

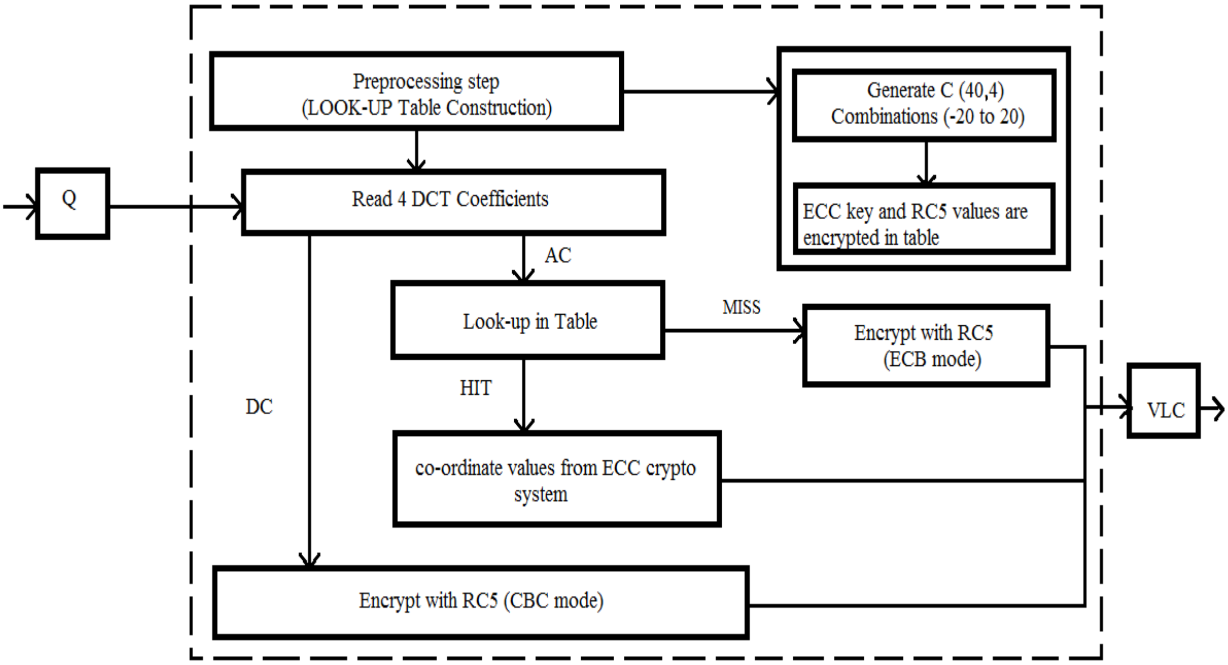
Preprocessing step
(LOOK-UP Table Construction)
Generate C (40,4)
Combinations (-20 to 20)
ECC key and RC5 values are encrypted in table
Q
Read 4 DCT Coefficients
AC
Look-up in Table
MISS
Encrypt with RC5
(ECB mode)
VLC
HIT
DC
co-ordinate values from ECC crypto system
Encrypt with RC5 (CBC mode)

Fig 3: Block Diagram of Encryption Process

```
Step 1: for each and every block of a frame do
Step 1.1: Consider four consecutive ACs (ACt, ACt+1, ACt+2, ACt+3).
Step 1.2: Compare these coefficients against the lookup table for a hit or miss if hit then replace the 4 AC coefficients with their encrypted values.
else
Apply the ECB mode of RC5 encryption with these ACs as input.
                                   end if
Step 1.3: When DC coefficients are considered, collect four DC coefficient values in a block and encrypt them using the CBC mode of RC5 algorithm.
end for
```

Figure 4: Main Encryption Algorithm

The pre-processing step could be done before the encryption phase and in fact even before the input (video to be encrypted) is known. For frequently occurring AC quadruple, instead of undergoing the entire process of encryption, a mere look-up serves the purpose, The proposed scheme of encryption gains its advantages from not only the look-up table but also the dynamism of changing the mode of encryption based on the type of coefficient. Algorithm 2 explains the main encryption.

At the receiver end, the authorized recipient first generates the look-up table for all the combinations of −20 to 20 quadruples and encrypts the quadruples in the way similar to the pre-processing step of the algorithm using the key. In the generated lookup table, the columns are exchanged and sorted in order to look up for the plain values when the cipher values are known. For obtaining the DC coefficients, the recipient can directly apply general RC5 decryption with the CBC mode. We concentrate only on the encryption of I frames because for real-time applications like pay-per-view there is no need to encrypt the motion vectors. Partial leakage of image information from the I-blocks in P/B frames might persuade a non-paying consumer to buy the video. In order to use our algorithm for applications where the entire video content is important, motion vectors of P and B frames are also encrypted along with I frames. The same look-up table (used for encryption of AC coefficients) can be used for encryption of these motion vectors.

V. KEY DISTRIBUTION

This part of the paper covers the RC5 key distribution to the end user. To withstand brute force attacks, the RC5 128 bit key is changed periodically and transmitted to the receiver in an encrypted form. The key can be encrypted using the standard public key cryptosystems such as ECC. This means that two keys are used for the encryption and decryption process. One key is public (asymmetric) and the other key is private (symmetric). This setting has an additional advantage that the cryptanalyst needs to apply two different attacks since symmetric and asymmetric cryptosystems have to be tackled separately. This enhances the security level considerably [4]. In our method of encryption, the transmitter uses the ECC public key of the intended recipient to encrypt the RC5 key. At the receiver end, the recipient uses his private ECC key to decrypt this RC5 key. The decrypted RC5 key is then used to decrypt the rest of the bit stream by generating the decryption lookup table. The ECC standard is not directly used to encrypt or decrypt the MPEG bit stream because the processing time required by it is proportional to the size of the data. In this work, we use a single 128 bit key, and hence the time required to encrypt this key using the ECC algorithm is very small when compared to the encryption of MPEG frame.

A.ECC key establishment

From above (Figure 1) generated point, let select P (1, 23) as a point and randomly select any integer from 1 to p -1

and d act as private key .Multiply d with point P in other words add point P with d times this point act as public key .as explain with below snapshot. So public key is (p, P, Q, n) and private key is d.

VI. RESULT AND SECURITY ANALYSIS

It succeeds in using text based algorithms for videos by managing the computational overhead and hence suiting real time applications. The security level provided is as good as security provided by RC5 and ECC. It is selective, i.e., based on the criticality level of the DCT coefficient, the algorithm adjusts to provide optimum security (like CBC mode for DC coefficients). The algorithm succeeds in exploiting the statistical properties of the video for providing better encryption speed.

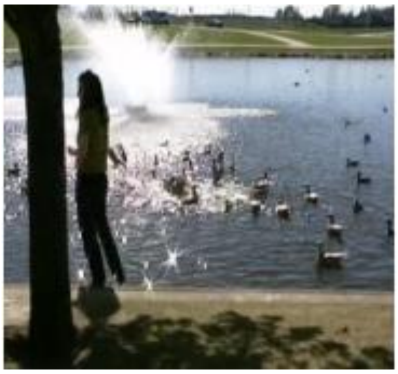

Figure 5: pond video

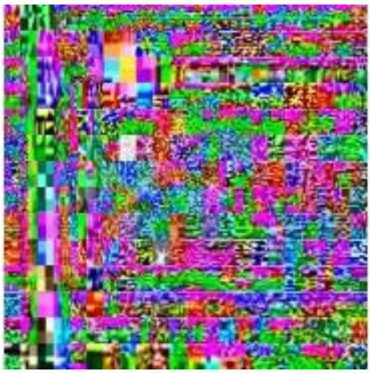

Figure 6: Encrypted Pond Video

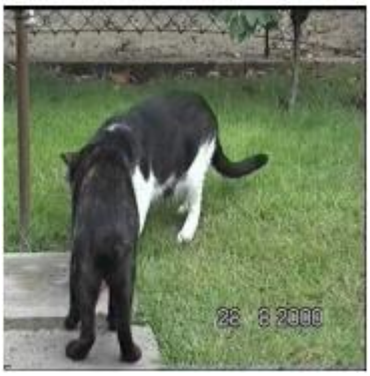

Figure 7: Cat playing video

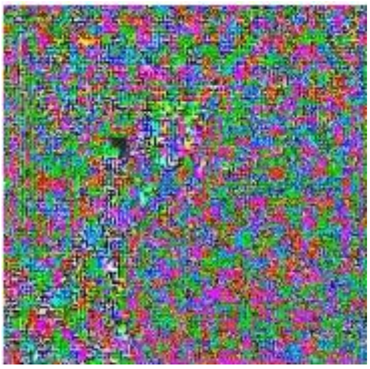

Figure 8: Encrypted Cat playing video

The security of the algorithm is checked against cipher text only, known-plaintext and chosen plaintext attacks as these are the most important attacks.

Cipher text-only attack: Cipher text only attack is a model for cryptanalysis where the attacker is assumed to have access to a set of cipher texts and knows the encryption algorithm. This is the most difficult attack since the crypt analyst has access only to the encrypted data. It is shown hat, RC5 with four rounds of encryption and key size of 128 bits, can be broken if 217 cipher texts are available. Our scheme uses RC5 with 20 rounds of encryption and 128 bit key size. Hence, the security of the proposed method is certainly higher, which is not easy to break. So, the propose algorithm is secure against cipher text only attack.

Known-plaintext attack: In known-plaintext attack, the attacker has access to both the cipher text and plaintext along with the encryption algorithm. The attacker first constructs a partial table with both the plaintext and the corresponding encrypted coefficients from the videos collection. Since we used a 128 bit key for encryption he needs to try on an average 2127 combinations to know which combination of key being used, very difficult to break. Furthermore, the key is renewed at periodic intervals, making it more difficult for a cryptanalyst to break using known-plaintext attack. Hence the proposed method is robust against known plaintext attack also.

Chosen-plaintext attack: A chosen plaintext attack is an attack model for cryptanalysis which presumes that the attacker has the capability to choose arbitrary plaintexts to be encrypted and obtain the corresponding cipher texts. According to the latest cryptanalysis, 12 round RC5 (with 64-bit blocks) is susceptible to a differential attack using 244 chosen plaintexts. Even though the video size may look as an encouraging factor for the attacker, who wishes to get many cipher text from a single video. The hidden strength of the algorithms is, he needs to get different combinations of cipher text which is difficult because the analysis of ACs varies from (0 to 20). So he needs a large collection of videos encrypted with single key. This is made very difficult by renewing the key. Apart from that in, increasing the number of rounds to at least 16 will increase security against differential cryptanalysis. This was in fact suggested by Rivest that security will increase when the number of rounds of encryption is increased. Even though we used a 32 bit version of RC5, we increased the number of rounds to 20 so as to have good computational security.

VII. CONCLUSIONS

This paper, proposes a computationally efficient, yet secure video encryption scheme. It uses RC5 for encryption of the DCT coefficients and ECC for small key sized generation .The proposed scheme is very fast, possesses good security and adds less overhead on the codec. It slightly decreases the compression rate of the video, which is negotiable for higher security. In future it would be to reduce the encrypted video size by modifying the default Huffman tables and hence come up with an ideal video encryption algorithm which takes less encryption time and causes no overhead on video size. It can also be extended to videos like MPEG-4, H.261, and H.264 etc

.

REFERENCES

[1] Avinash P. Wadhe , N.A.Chavhan, "*Practical Approach for Improving Security in Wireless Mesh Network Through Ecc and Two Way Authentication Scheme"*, National Conference on Innovative Paradigms in Engineering & Technology (NCIPET-2012), Vol 16, Issue NO. 3

[2] Trupti Dandamwar, Manish Narnaware, *"Introduction to Real Time & Secure Video Transmission using Distributed & Parallel Approach"*, International Journal of Computer Science and Network (IJCSN), Volume 1, Issue 5, October 2012

[3] Hao Wang and Chong-wei Xu, *"A new lightweight and scalable encryption algorithm for streaming video over wireless Network."*

[4] C. Narsimha Raju, Ganugula Umadevi, Kannan Srinathan and C. V. Jawahar. *"Fast and Secure Real-Time Video Encryption",* Sixth Indian Conference on Computer Vision, Graphics & Image Processing .

[5] Davis Pan*, "A Tutorial on MPEG".*

[6] Dr. S.R. Ely, *"MPEG video coding".*

[7] M. Abomhara, Omar Zakaria, Othman O. Khalifa, *"An Overview of Video Encryption Techniques"*, International Journal of Computer Theory and Engineering, Vol. 2, No. 1, *pp 103-110*, February, 2010

[8] Patrick Longa, and Catherine Gebotys, *"Efficient Techniques for High-Speed Elliptic Curve Cryptography"* 2010 University of Waterloo, Canada

[9] Fuwen Liu, Hartmut Koenig. *"A survey of video encryption algorithms"*, Journal of Computers and Security, pp 3-15, 2010.

[10] Fuwen Liu, "*A Tutorial on Elliptic Curve Cryptography*".

[11] www.certicom.com