A Novel Idea of Video Encryption using Hybrid Cryptographic Techniques

Sridhar C. Iyer
M.E Student,
Dept. of Computer Engineering.
TCET, Mumbai, India
c.sridhar89@gmail.com

Dr.R.R Sedamkar
Dean (Academics),
Dept. of Computer Engineering.
TCET, Mumbai, India
rr.sedamkar@thakureducation.org

Mrs. Shiwani Gupta
Asst. Professor,
Dept. of Computer Engineering.
TCET, Mumbai, India
Shiwanigupta3005@gmail.com

Abstract—The concept of video encryption is growing in popularity mainly because of the increasing use of communication techniques such as video conferencing for carrying out business meetings and presentations. The video data that travels to and fro between the sender and the receiver has to pass through the most unsecure medium of communication, the internet. The existing methods for providing security to the video data relies mainly on heavy signal processing algorithms which require a lot of bandwidth and takes a lot of time to carry out the encryption resulting in lags in communication. On the other hand, no single encryption algorithm is secure enough to provide a completely flawless and lossless result. Symmetric algorithms are faster but easier to break into, whereas asymmetric algorithms are more secure but take longer time. The novel idea proposed in this article makes use of the advantages of both the methods by presenting a hybrid technique of encryption, resulting in a much secure and faster alternative of video encryption.

Keywords—Video Encryption; Cryptography; ECC; AES; Hybrid Encryption; Symmetric Encryption; Asymmetric Encryption;

I. INTRODUCTION

There are a number of algorithms available which provide different alternatives and approaches towards video encryption. The methods such as Symmetric ciphers make use of a single key for encryption as well as decryption of the video file by breaking them into different set of frames, applying the algorithm to each frame, combining the result of each and agglomerating them into a single encrypted video file. On the other hand asymmetric algorithms make use of two different keys, one for encryption and the other for decryption. The encryption process makes use of one key whereas the decryption process makes use of a different key. These two keys make up a key pair which work together hand in hand to carry out the encryption and decryption process.

The existing techniques such as symmetric ciphers provide simplicity in design at the cost of security whereas asymmetric ciphers provide a better security at the cost of time. Both the techniques have some advantages over each other but when it comes to a full proof cipher, both the ciphers are not able to live up to the expectations. The motivation behind the research work lies in the fact that there are very few video encryption techniques available which could provide better security at the cost of very little time, also reducing the complexity of the design to a great extent.

The proposed system makes use of a hybrid cryptographic technique which comprises of a symmetric as well as an asymmetric cipher. The mixed encryption model exploits the simplicity of the symmetric counterpart Advanced Encryption Standard (AES) [1] and the highly secure asymmetric counterpart Elliptic Curve Cryptography (ECC)[2]. The standard AES makes use of 128, 192 and 256 bit keys depending upon the number of rounds such as 10, 12 and 14 respectively.

AES is the most efficient and favorite method of choice when it comes to symmetric encryption. It has found many applications such as 128 bit encryption of communication happening over the internet through web browsers and websites. It also provides encryption of voice calls over a GSM network. On the other hand, ECC has gained in popularity as an asymmetric cipher because of its virtually unbreakable security at the expense of a very short key as compared to RSA [3] which makes use of minimum 1024 bit keys. The overall encryption process is explained in the further sections.

II. LITERATURE REVIEW

The following research articles are selected for review, keeping in mind the traditional and conventional approaches of video cryptography and encryption in general:

In the article [4], the authors have discussed about the encryption of the video files with the help of region permutation followed by AES and Data encryption Standard (DES). This scheme applies the algorithm to the fragments of data individually rather than applying on the whole video file itself. The algorithm is quite complex because of the use of a mixed permutation and AES encryption followed by DES. The usage of DES adds up to the time complexity and provides very little security because of its weak resistance to brute force attacks and low key size. The experimental results too show that the execution time can be improved further improved.

In the article [5], the authors have mentioned another technique in which they have used a modified version of the AES algorithm to do video encryption. The modification done is mainly limited to the shift row transformation phase of the AES internal rounds. The change made to the standard AES may confuse the attacker to some extent but it's not fully secure if a lucky guess is made about the internal structure of the shift row function. The time complexity remains the same giving it a slight increase in security. In the article [6], the idea put forward highlights the use of H.264 encoding and AES encryption for video conferencing. The system makes use of complex signal processing techniques such as DCT. AES is used to encrypt the DCT coefficients to be used by the system. The proposed system can provide rapid encryption and even secure the communication from wiretap attacks. The article discusses about the system capable of encrypting the video streams during video conferencing, but it doesn't discuss about security of the video files during transmission such as emails or from standalone computer systems.

In the article [7], a hardware implementation of video encryption is proposed which makes use of FPGA based programmable logic device. It makes full use of the parallel processing of the FPGA, hence increasing the speed. The video image encryption system is based on Altera DE2-70 development platform. The only drawback is the chances of hardware failures which may bring the entire system to a halt. The article [8] is designed to focus on the redundant parts of the video for example the syntax files which are used for indexing purposes but not used by the video based applications, hence reducing the overhead involved in reading the entire video files. The design is very novel but has a really complex methodology to understand. The time complexity is also high as the internal processing is really complex yet secure.

III. Background Of Technologies Involved

The hybrid encryption algorithm makes use of two underlying technologies viz. ECC and AES. Let's discuss each of these in brief.

- Advanced Encryption Standard

The Advanced Encryption Standard was proposed as a suitable replacement of the existing Data Encryption Standard (DES). It is a block cipher which takes as input a 128 bit plaintext, which is subject to an encryption with 128, 192 and 256 bit key depending upon the number of rounds i.e. 10,12 or 14 respectively. AES is different in concept from DES i.e. it is not based on the Feistel cipher.

Figure.1 explains the various internal rounds that take place for encryption and decryption using AES. It broadly consists of Substitution i.e. bit by bit substitution, shifting of rows i.e. transposition, mixing of columns based on modular arithmetic multiplication followed by adding of round key till n-1 rounds. Mix column round is omitted in the final nth round. After the nth round a 128 bit cipher-text is obtained.

- Elliptic Curve Cryptography

The use of elliptic curves in public key cryptography was independently proposed by Koblitz [9] and Miller in 1985 and since then, an enormous amount of work has been done on elliptic curve cryptography. A general elliptic curve takes the general form as:

$$E: y^2 = x^3 + ax + b \quad \ldots\ldots (1)$$

Where x, y are elements of GF (p) and a, b are integer modulo p, satisfying

$$4a^3 + 27b^2 \neq 0 \pmod{p} \quad \ldots\ldots (2)$$

The basic EC operations are point addition and point doubling. Simple multiplication could not be found in the case of elliptic curves. A single point suppose A(x,y) on the elliptic curve could yield a resultant point B(x',y') by following a series of point addition and point doubling instead of directly multiplying the point A with a scalar, hence A=zB , where z is a scalar multiple.

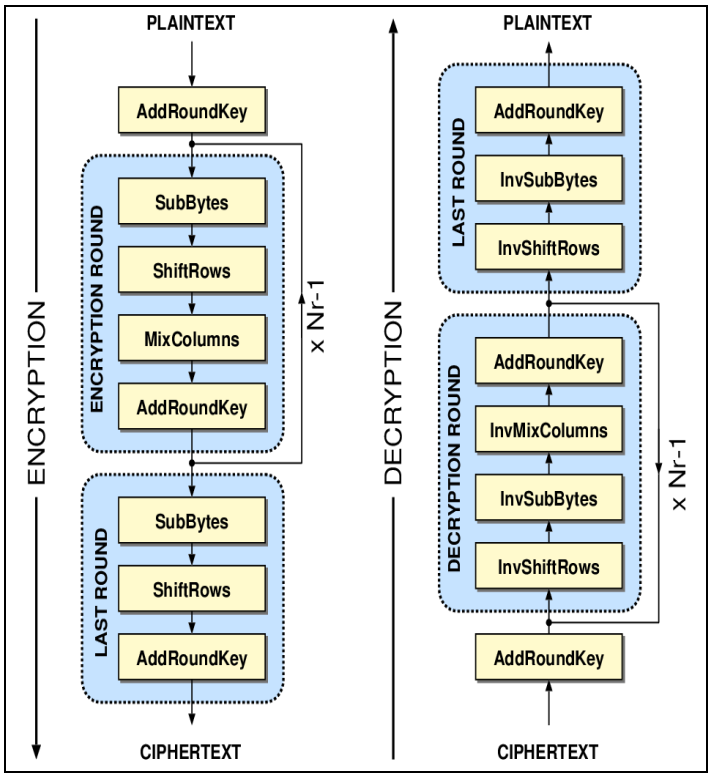

Figure 1. Advanced Encryption Standard (AES) Block Diagram

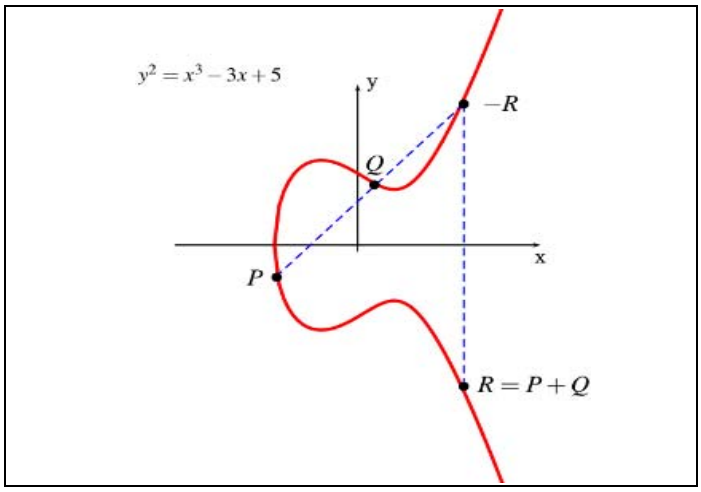

Figure 2. ECC Point Addition

Figure 2 shows the ECC point addition where R is the result of the addition of P and Q. Whereas Figure 3 shows the ECC point doubling where the intercept in the negative axis gives the resultant double of the point y.

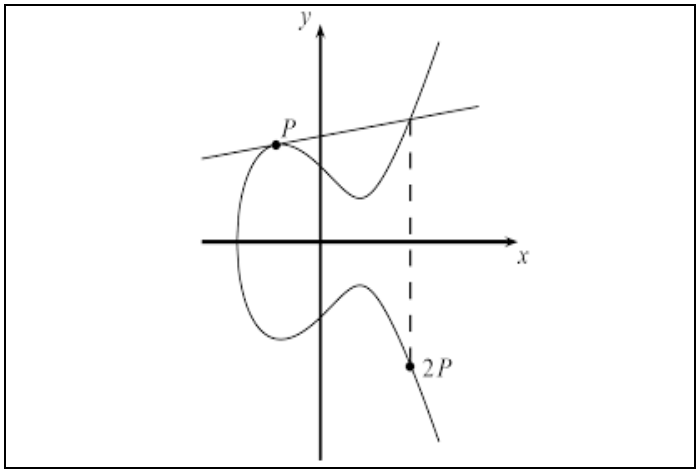

Figure 3. ECC Point Doubling

IV. Proposed Idea

The idea proposed in this research article is simple yet powerful. The existing systems discussed in the previous section were all focusing upon complex strategies involving image processing, signal processing and complex mathematical functions to provide security to the video files. These systems are capable of doing their job pretty well, i.e. to provide encryption and decryption to video files, but they lack in one or the other parameters such as speed, throughput, security, memory constraints, etc. The system discussed in this article makes use of intermediate text files instead of video frames or images. It converts the original video stream into a text file by reducing it into a base64 [10] equivalent of the same. This text file is then subjected to a dual encryption, i.e. ECC and AES to provide a double security. The Base64 converted file is really quick to encrypt as compared to the original video stream, thus adding novelty to the idea. The overall video encryption process is as follows:

- Read the input video from the user.
- Convert the video into a Base64 format text file.
- Generate ECC private and public keys and the AES symmetric key.
- Encrypt the Base64 file with the ECC public key.
- Encrypt the file obtained in the previous step with the AES symmetric key.
- Create a QR code of the final encrypted file, the AES Key and the ECC private key.

The overall architectural diagram for the encryption process is as shown in Figure 4.The QR codes sent to the receiver consists of the final cipher-text, AES symmetric key and ECC private keys. The overall video decryption process works exactly in the reverse direction as follows:

- Read the QR code.
- Extract the AES symmetric key
- Extract the cipher-text from the QR Code.
- Apply AES decryption
- Extract the ECC private key from the QR Code.
- Apply ECC decryption.
- Convert the intermediate file back to the original media file using Base64 decryption.

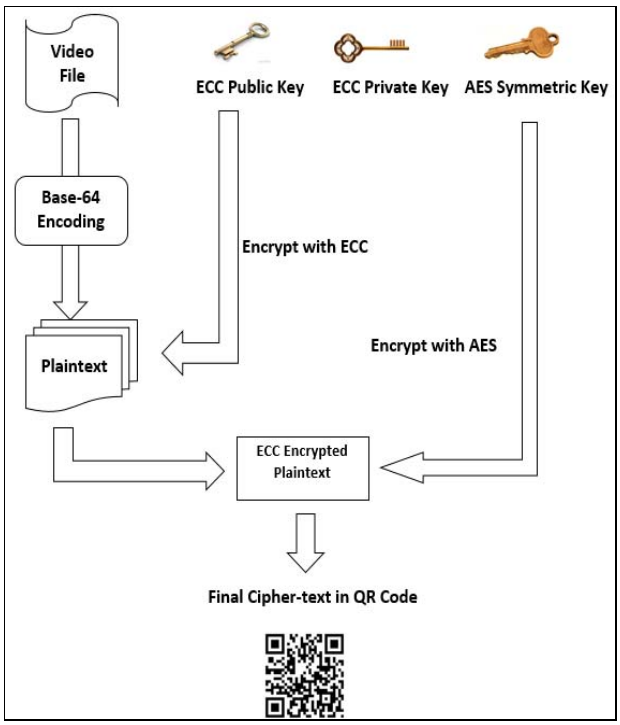

Figure 4. Schematic diagram of Hybrid Encryption

The overall architectural diagram for the decryption process is as shown in Figure 5.

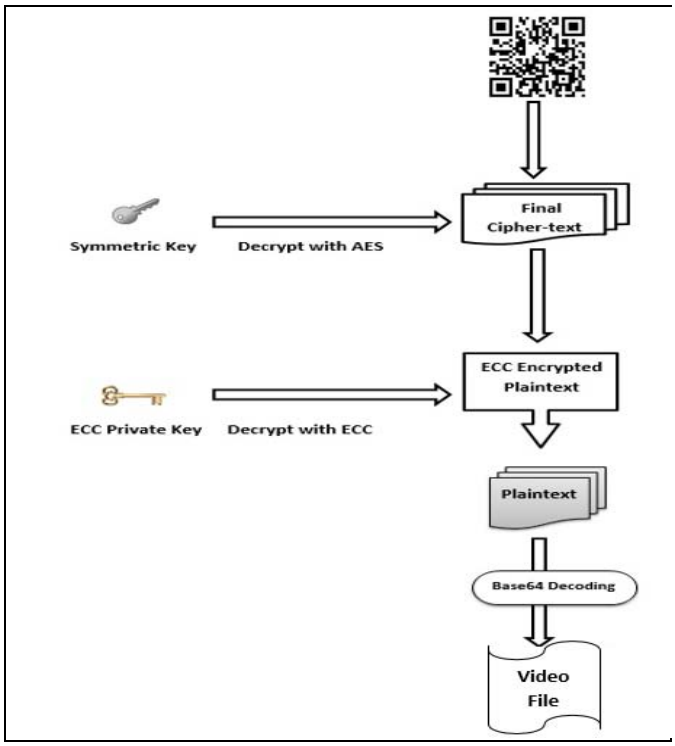

Figure 5. Schematic diagram of Hybrid Decryption

V. Experimental Results and Analysis

The implementation of the above mentioned proposed algorithm is carried out in a Java Runtime Environment using the cryptographic libraries developed by FlexiCore's Brainpool160 provider. ECC makes use of 160 bit keys, whereas AES makes use of 128 bit keys. These keys are generated with the help of these providers. A total of 288 bit keys are needed to carry out the encryption process. The performance comparisons are as shown below:

- Performance Comparison based on Execution Time

The following table shows the comparison between the proposed hybrid system and the nearest existing technology in terms of execution speeds.

TABLE I. PERFORMANCE COMPARISON BETWEEN PROPOSED SYSTEM AND EXISTING TECHNOLOGIES

Size of File	**Encryption Time (in Sec)**		
	Proposed System	***AES***	**Existing System [5]**
1.11 Mb	0.79	0.925	0.917
1.20 Mb	0.85	1.245	1.12
4.45 Mb	1.24	2.57	2.47

The results clearly show that the proposed system gives a better efficiency in terms of time.

- Performance based on Gray levels

The following images show the comparison of the video file before encryption and after encryption.

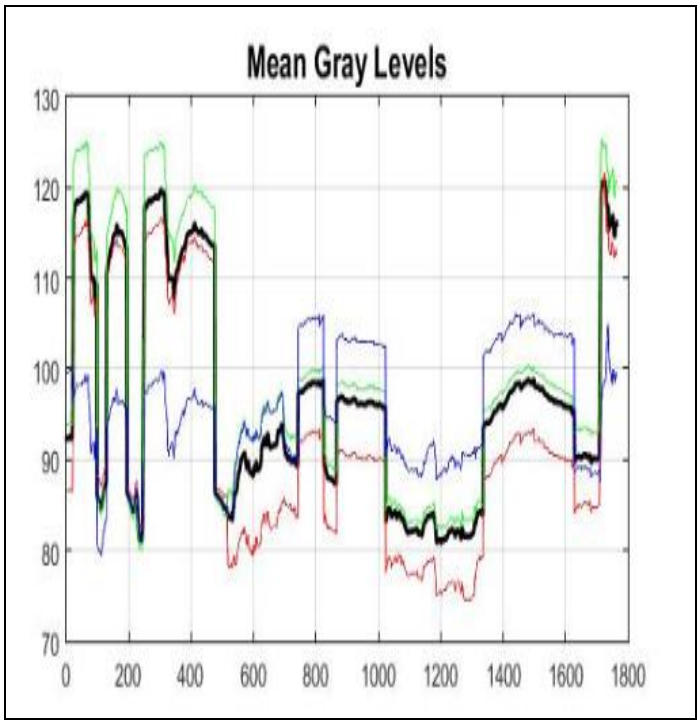

Figure 6. Gray level plot of the video file "Video 1.mp4" before encryption.

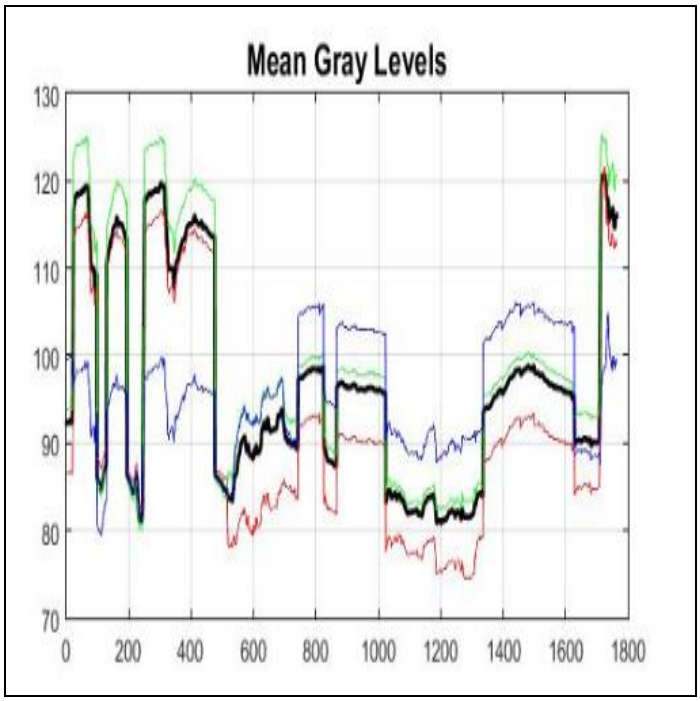

Figure 5. Gray level plot of the video file "DECODED-FILE-MP4.mp4" after decryption.

Figure 6. PSNR comparisons of Original Video (Video 1) and Recovered Video (Video 2).

- Comparison based on PSNR value

The gray level of both the video streams may seem to look identical visually but these may or may not be the same, hence a more sophisticated comparison has to be made which is done with the help of the Peak Signal-to-Noise Ratio (PSNR). PSNR is calculated with the help of the Mean Square Error (MSE) which ideally should be as low as possible for a lossless decryption. The PSNR is calculated as follows:

$PSNR = 10.\log_{10}(M^2 / MSE)$ ……(3)

Where,

M = Maximum Possible Pixel Value of the Image.

MSE = Mean Square Error.

If the two images are exactly identical, the PSNR value would be maximum or infinity. The Figure 6 shows an execution of the proposed implementation. The results based on the three parameters as shown above, reflects the efficiency of the proposed hybrid system.

VI. Conclusion

It can be seen from the results and analysis that the proposed idea has given better outcomes as compared to the existing technologies. Better speed and accuracy yields better results. Applications such as Video Conferencing requires constant flow of data packets from one end to the other. In such cases, a fast encryption algorithm is required else the sender and receiver will keep on waiting for each other's acknowledgement. In such a situation, the existing algorithms may not be sufficient enough to provide assistance and justice to these applications.

References

[1] Daemen, Joan, Rijmen, Vincent, "AES Proposal:Rijndael," *National Institute of Standards and Technology (NIST)*, p.1, February2013.

[2] Koblitz.N, "Elliptic curve cryptosystems," *Mathematics of Computation,* 1987, pp. 203–209, doi:10.2307/2007884

[3] Rivest. R,Shamir. A, Adleman. L,"A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," *Communications of the ACM*, 1978, pp.120–126, doi:10.1145/359340.359342

[4] Pradeep Pai T, Raghu M.E,Ravishankar K C, "Video Encryption For Secure Multimedia Transmission - A Layered Approach," *3rd International Conference on Eco-friendly Computing and Communication Systems (ICECCS), IEEE*, 2014, pp.127-132, doi:10.1109/ICECCS.2014.35

[5] Pooja Deshmukh, Vaishali Kolhe, "Modified AES Based Algorithm for MPEG Video Encryption,"*ICICES- S.A.Engineering College, Chennai, Tamilnadu, India,IEEE,*2014,pp.1-5,doi:10.1109/ICICES.2014.7033928

[6] Hua-Zhen YAO, JING Ya-Tao, "The Design of Video-Conference Encryption System based on H.264," *International Conference on Multimedia Technology (ICMT), Ningbo, IEEE*, 2010, pp:1-4, doi: 10.1109/ ICMULT.2010.5630471

[7] Xuewen Ma, Mengyao Li, Hong Wang , Ting Gong, "Design and Implementation of Video Image Encryption System Based on FPGA," *International Conference on Computer Science and Automation Engineering(ICCSAE), Zhangjiajie, IEEE*, 2012, pp:68-72,doi: 10.1109/CSAE.2012.6272910

[8] Glenn V W, Andras B, Jan De Cock, Adrian M, Rik Van de Walle, "Encryption for High Efficiency Video Coding with Video Adaptation Capabilities," *IEEE Transactions on Consumer Electronics*, August 2013,Vol.59,Issue.3,pp:634-642,doi:10.1109/TCE.2013.6626250

[9] N.Koblitz, "Elliptic Curve Cryptosystems," Mathematics of Computation, VolA8, 1987, pp.203 -209

[10] Wikipedia. *Base64* [Online] . Available : https : / / en . wikipedia . org / wiki/Base64