Use of AES Encryption Algorithm for High Secure Data Hidden Framework in the MPEG

VIDYA MOHANTY
Assistant Professor, Dept. of Computer Science & Engineering, Aryan Institute of Engineering & Technology, Bhubaneswar
SUJIT NAG
Department of Computer science and Engineering, Raajdhani Engineering College, Bhubaneswar, Odisha

Dr.GYANENDRA KUMAR PALLAI
Department of Computer science and Engineering, NM Institute of Engineering and Technology,Bhubaneswar , Odisha

***Abstract*-Steganography is the art of information hiding and invisible communication. Unlike cryptography, where the goal is to secure communications from the Snooper by make the data not understood. In this framework we will propose a collaborate approach between steganography and cryptography. This approach will invent high rate and high secure data hidden using secret key steganography and AES Rijndael method. As well, this paper will overview the use of data hiding techniques and its classification, furthermore we will assign the well-built of the AES algorithm, during this review the author will answer the question why they used AES algorithm. In additional to the security issues we will use the digital video as a cover to the data hidden. The reason behind opt the video cover in this approach is the huge amount of single frames image per sec Which in turn overcome the problem of the data hiding quantity, as the experiment result shows the success of the hidden, encryption, extract, decryption functions without affecting the quality of the video**

***Keyword*-Steganography, Hidden Data, Encryption, LSB, Decryption.**

I. INTRODUCTION

Steganography is the art of hiding and transmitting data through apparently innocuous carriers in an effort to conceal the existence of the data, the word Steganography literally means covered or hiding writing as derived from Greek. Steganography has its place in security. It is not intended to replace cryptography but supplement it. Hiding a message with Steganography methods reduces the chance of a message being detected. If the message is also encrypted then it provides another layer of protection [1]. Therefore, some Steganographic methods combine traditional Cryptography with Steganography; the sender encrypts the secret message prior to the overall communication process, as it is more difficult for an attacker to detect embedded cipher text in a cover [2].In the field of Steganography, some terminology has developed. The adjectives 'cover', 'embedded' and 'stego' were defined at the information hiding workshop held in Cambridge, England. The term "cover" refers to description of the original, innocent massage, data, audio, video, and so on. Steganography is not a new science; it dates back to ancient times. It has been used through the ages by ordinary people, spies, rulers, government, and armies. There are many stories about

Steganography. For example ancient Greece used methods for hiding messages such as hiding it in the belly of a share (a kind of rabbits), using invisible ink and pigeons. Another ingenious method was to shave the head of a messenger and tattoo a message or image on the messenger head. After allowing his hair to grow, the message would be undetected until the head was shaved again. While the Egyptian used illustrations to conceal message. Hidden information in the cover data is known as the "embedded" data and information hiding is a general term encompassing many sub disciplines, is a term around a wide range of problems beyond that of embedding message in content. The term hiding here can refer to either making the information undetectable or keeping the existence of the information secret. Information hiding is a technique of hiding secret using redundant cover data such as images, audios, movies, documents, etc. This technique has recently become important in a number of application areas. For example, digital video, audio, and images are increasingly embedded with imperceptible marks, which may contain hidden signatures or watermarks that help to prevent unauthorized copy [4]. It is a performance that inserts secret messages into a cover file, so that the existence of the messages is not apparent. Research in information hiding has tremendous increased during the past decade with commercial interests driving the field [4].

II. Related Work

In[5] a new system of information hiding is presented. The proposed system aim to hidden information (data file) in any execution file (EXE).The author also makes collaboration between stenography and cryptography in a very secure system the encryption method which has been used in this paper is AES method. In [4],[5] introduce an authentication protocol which serves as a proof of concept for authenticating an RFID tag to a reader device using the Advanced Encryption Standard (AES) as cryptographic primitive. The main part of this work is a novel approach of an AES hardware implementation which encrypts a 128-bit block of data within 1000 clock cycles. In [6] the author adapts image filtering and adaptive image segmentation with bits replacement on the appropriate pixels. These pixels are selected randomly rather than sequentially by using new concept defined by main cases with their sub cases for each byte in one pixel. This concept based on both visual and statistical, as well the author has used AES encryption to higher the security on the algorithm.

III. Steganography Types

As it is known there is much communication between people and organizations through the use of the phone, the fax, computer communications, radio, and of course all of these communication should be secure. There are basically three Steganography types:-

A. Pure Steganography

Pure Steganography is a Steganography system that doesn't require prior exchange of some secret information before sending message; therefore, no information is required to start the communication process: the security of the system thus depends entirely on its secrecy [7].
The pure Steganography can be defined as the quadruple (C, M, D, and E) where:
C: the set of possible covers.
M: the set of secret massage with $|C| \geq |M|$.
E: $C \times M \rightarrow C$ the embedding function.
D: $C \rightarrow M$ of the extraction function with the property that D (E(c,m))=m for all m Є M and c Є C

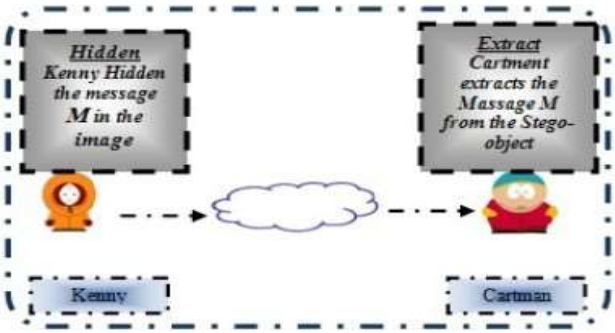

Figure 1: Pure Steganography

In most applications, pure Steganography is preferred, since no stego-key must be shared between the communication partners, although a pure Steganography protocols don't provide any security if an attacker knows the embedding method

B. Secret key Steganography

A secret key Steganography system is similar to a symmetric cipher, where the sender chooses a cover and embeds the secret message into the cover using a secret key. If the secret key used in the embedding process is known to the receiver, he can reverse the process and extract the secret message. Anyone who doesn't know the secret key should not be able to obtain evidence of the encoded information[7].
The secret key Steganography can be defined as the quintuple (C, M, K, DK, EK) where:
C: the set of possible covers.
M: the set of secret message.
K: the set of secret keys.
Ek: $C \times M \times K \rightarrow C$
With the property that DK (EK(c,m,k),k)=m for all m Є M, c Є C and k Є K

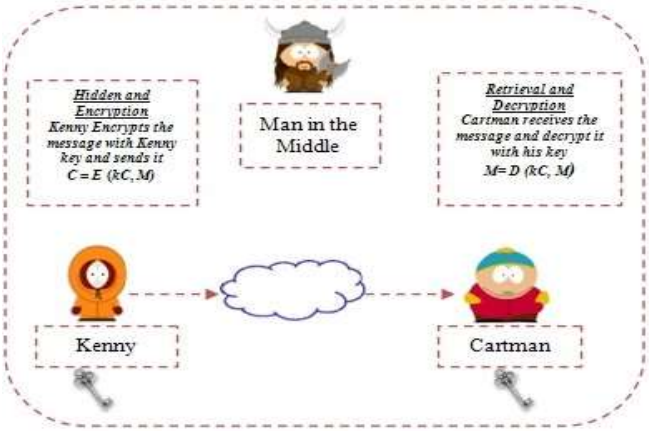

Figure 2: Secret Key Steganography.

C. Public key Steganography

Public key Steganography does not depend on the exchange of a secret key. It requires two keys, one of them private (secret) and the other public: the public key is stored in a public database, whereas the public key is used in the embedding process. The secret key is used to reconstruct the secret message. One way to build a public key Steganography system is to use a public key crypto system. The sender and the receiver can exchange public keys of some public key cryptography algorithm before imprisonment. Public key Steganography utilizes the fact that the decoding function in a Steganography system can be applied to any cover, whether or not it already contains a secret message. The public key Steganography relies on the fact that encrypted information is random enough to hide in plain sight. The sender encrypts the information with the receiver's public key to obtain a random-looking massage and embeds it in a channel known to the receiver, thereby replacing some of the natural randomness with which every communication process is accompanied. Assume that both the cryptographic algorithms and the embedding functions are publicly known. The receiver who cannot decide a priori if secret information is transmitted in a specific cover will suspect the arrival of message and will simply try to extract and decrypt it using his private key. If the cover actually contained information, the decryption information is the sender's message[7].

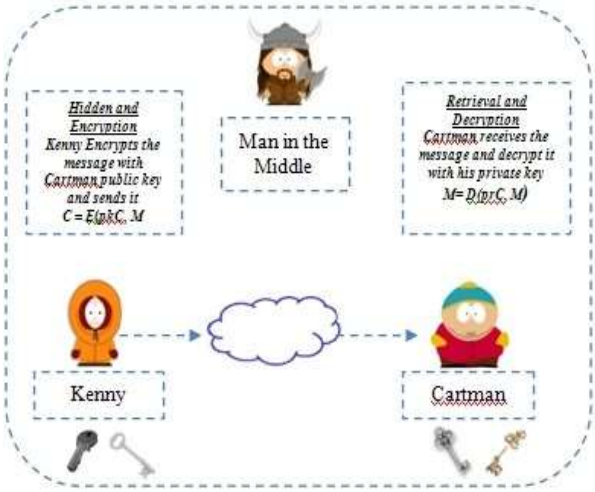

Figure 3: public key steganography

IV. ADVANCED ENCRYPTION STANDARD

In the late 1990s, the U.S. National Institute of Standards and Technology (NIST) conducted a competition to develop a replacement for DES. The winner, announced in 2001, is the Rijndael (pronounced "rhine-doll") algorithm, destined to become the new Advanced Encryption Standard. Rijndael mixes up the SPN model by including Galios field operations in each round. Somewhat similar to RSA modulo arithmetic operations, the Galios field operations produce apparent gibberish, but can be mathematically inverted.AES have Security is not an absolute; it's a relation between time and cost. Any question about the security of encryption should be posed in terms of how long time, and how high cost will it take an attacker to find a key?

Currently, there are speculations that military intelligence services possibly have the technical and economic means to attack keys equivalent to about 90 bits, although no civilian researcher has actually seen or reported of such a capability. Actual and demonstrated systems today, within the bounds of a commercial budget of about 1 million dollars can handle key lengths of about 70 bits. An aggressive estimate on the rate of technological progress is to assume that technologies will double the speed of computing devices every year at an unchanged cost. If correct, 128-bit keys would be in theory be in range of a military budget within 30-40 years. An illustration of the current status for AES is given by the following example, where we assume an attacker with the capability to build or purchase a system that tries keys at the rate of one billion keys per second. This is at least 1 000 times faster than the fastest personal computer in 2004. Under this assumption, the attacker will need about 10 000 000 000 000 000 000 000 years to try all possible keys for the weakest version, AES-128.The key length should thus be chosen after deciding for how long security is required, and what the cost must be to brute force a secret key. In some military circumstances a few hours or days security is sufficient – after that the war or the mission is completed and the information uninteresting and without value. In other cases a lifetime may not be long enough. There is currently no evidence that AES has any weaknesses making any attack other than exhaustive search, i.e. brute force, possible. Even AES-128 offers a sufficiently large number of possible keys, making an exhaustive search impractical for many decades, provided no technological breakthrough causes the computational power available to increase dramatically and that theoretical research does not find a short cut to bypass the need for exhaustive search. There are many pitfalls to avoid when encryption is implemented, and keys are generated. It is necessary to ensure each and every implementations security, but hard since it requires careful examination by experts. An important aspect of an evaluation of any specific implementation is to determine that such an examination has been made, or can be conducted [8]

A. Comparison between AES, 3DES and DES

Advance Encryption Standard (AES) and Triple DES (TDES or 3DES) are commonly used block ciphers. Whether you choose AES or 3DES depend on your needs. In this section it would like to highlight their differences in terms of security and performance [8]. Since 3DES is based on DES algorithm, it will talk about DES first. DES was developed in 1977 and it was carefully designed to work better in hardware than software. DES performs lots of bit manipulation in substitution and permutation boxes in each of 16 rounds. For example, switching bit 30 with 16 is much simpler in hardware than software. DES encrypts data in 64 bit block size and uses effectively a 56 bit key. 56 bit key space amounts to approximately 72 quadrillion possibilities. Even though it seems large but according to today's computing power it is not sufficient and vulnerable to brute force attack. Therefore, DES could not keep up with advancement in technology and it is no longer appropriate for security. Because DES was widely used at that time, the quick solution was to introduce 3DES which is secure

enough for most purposes today.3DES is a construction of applying DES three times in sequence. 3DES with three different keys (K1, K2 and K3) has effective key length is 168 bits (The use of three distinct key is recommended of 3DES.). Another variation is called two-key (K1 and K3 is same) 3DES reduces the effective key size to 112 bits which is less secure. Two-key 3DES is widely used in electronic payments industry. 3DES takes three times as much CPU power than compare with its predecessor which is significant performance hit. AES outperforms 3DES both insoftware and in hardware[7][8]. The Rijndael algorithm has been selected as the Advance Encryption Standard (AES) to replace 3DES. AES is modified version of Rijndael algorithm. Advance Encryption Standard evaluation criteria among others was [9][10]:

- Security
- Software & Hardware performance
- Suitability in restricted-space environments
- Resistance to power analysis and other implementationattacks.

V. SYSTEM OVERVIEW

The main goal of our plan is to build a system program that is able to hide data in digital video files, more specifically in the images or frames extracted from the digital video file MPEG; as shown in figure 4.

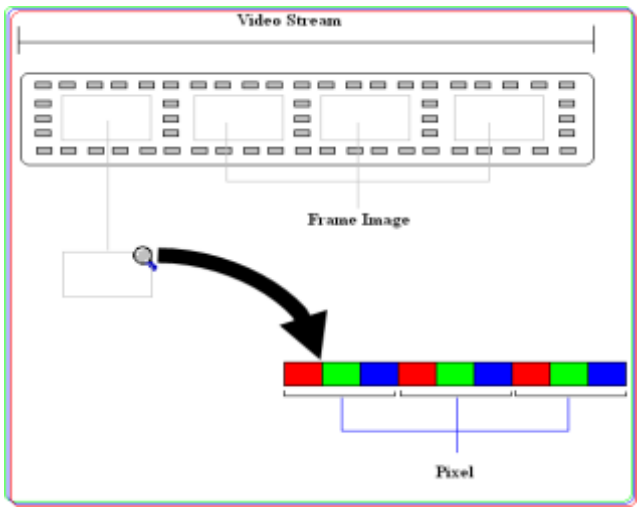

Figure 4: Extracting frames from video file

The main function in this framework is steganography and cryptography these two approaches carry out the dreamily protection for the information and make the attackers dream on getting data back. The algorithm work as the chart shows below, where unsuspected carrier with the strongest symmetric encryption algorithm building the characteristic of our framework. The main function of the proposed approach is:

1. Encrypt data
2. Hidden the encrypt data
3. Extract the data
4. Decrypt the data

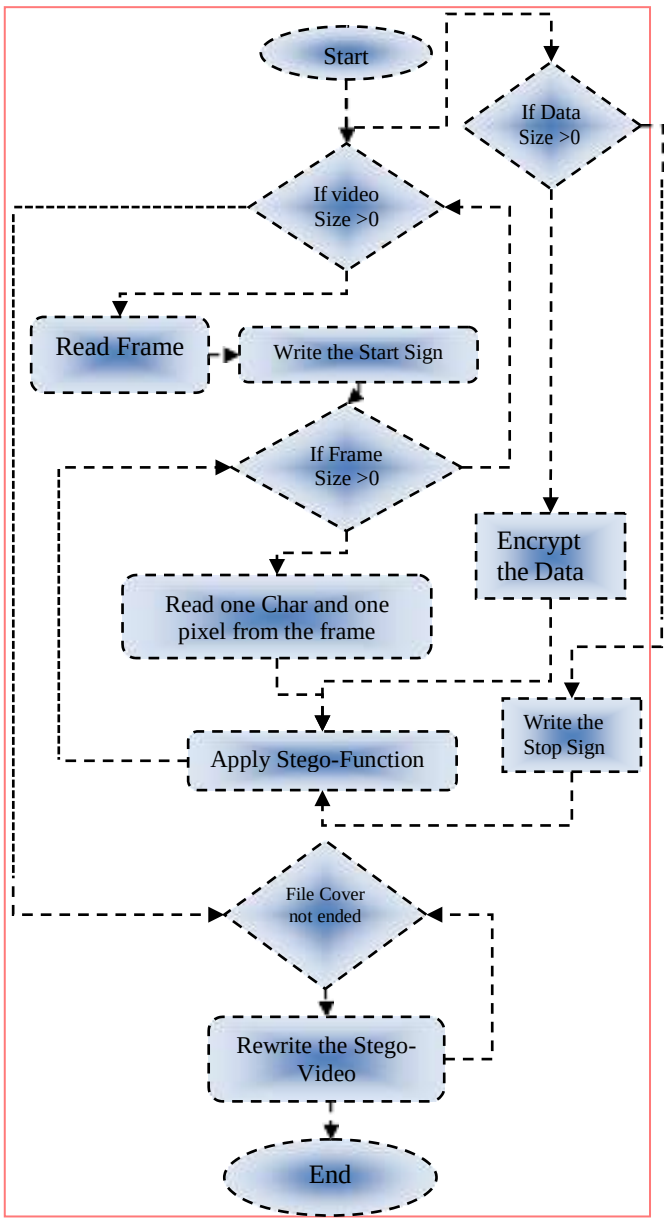

Figure 5: the encode algorithm

The figure above showing the encryption with hidden operation this framework give more flexibility to appoint the start point at which frame as well the end point, this new feature make the system more secure in term of avoiding discover the data hidden using the statistical techniques. Figure 6 is the extraction operation with the decryption

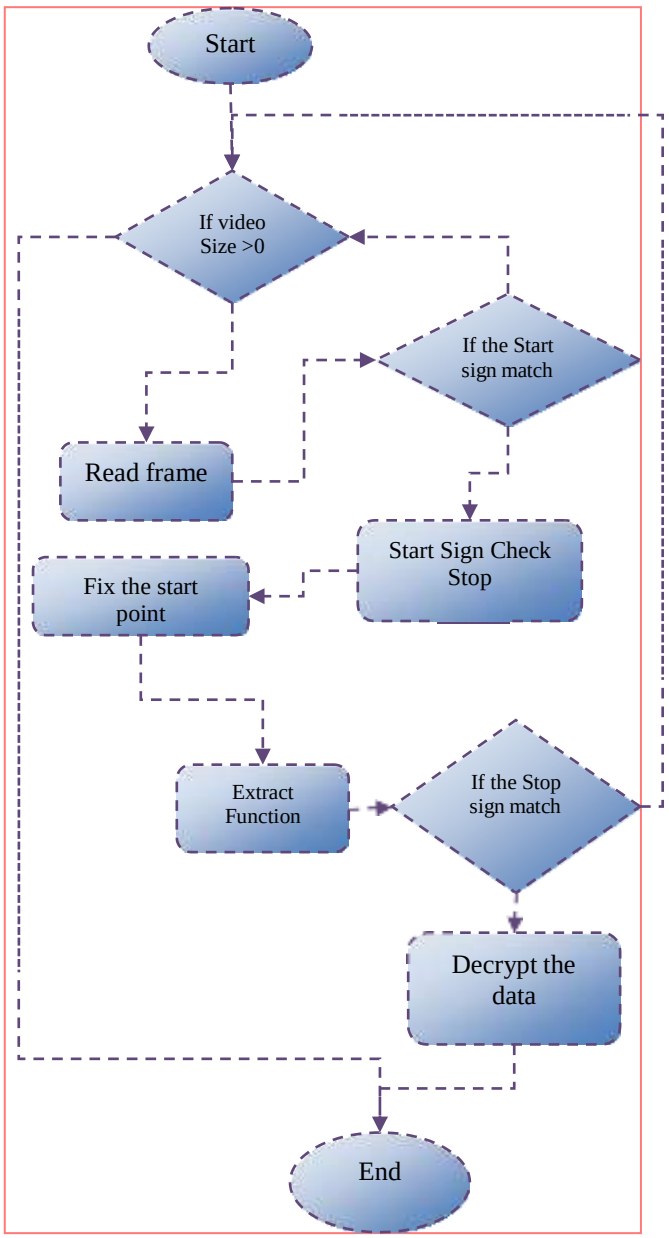

Figure 6: decoding algorithm

VI. EXPIREMENTAL RESULTS

Due to the difficulty of showing the result as a video stream on paper, the author prefers to display the result on the frame of the digital video file along with histogram of each a single frame. The following here are extracted frames of a digital video file. Figure 7 shows the frames from the famous movie "The Godfather" before applying the algorithm, while Figure 8 shows the frame after applying the algorithm. We can see here that there are no much differences between the two sets of frames especially for human vision system. This can tell that the algorithm can be applied successfully on video frames also to verify the algorithm by the histogram, to see the divergences on the frames before and after hiding data. From the histogram for both single frame in figure 7 & 8, its clear there is no differences between the two sets before and after hiding data which prove that the algorithm successfully hid the data into the frames without making a noticeable difference for the human vision system.

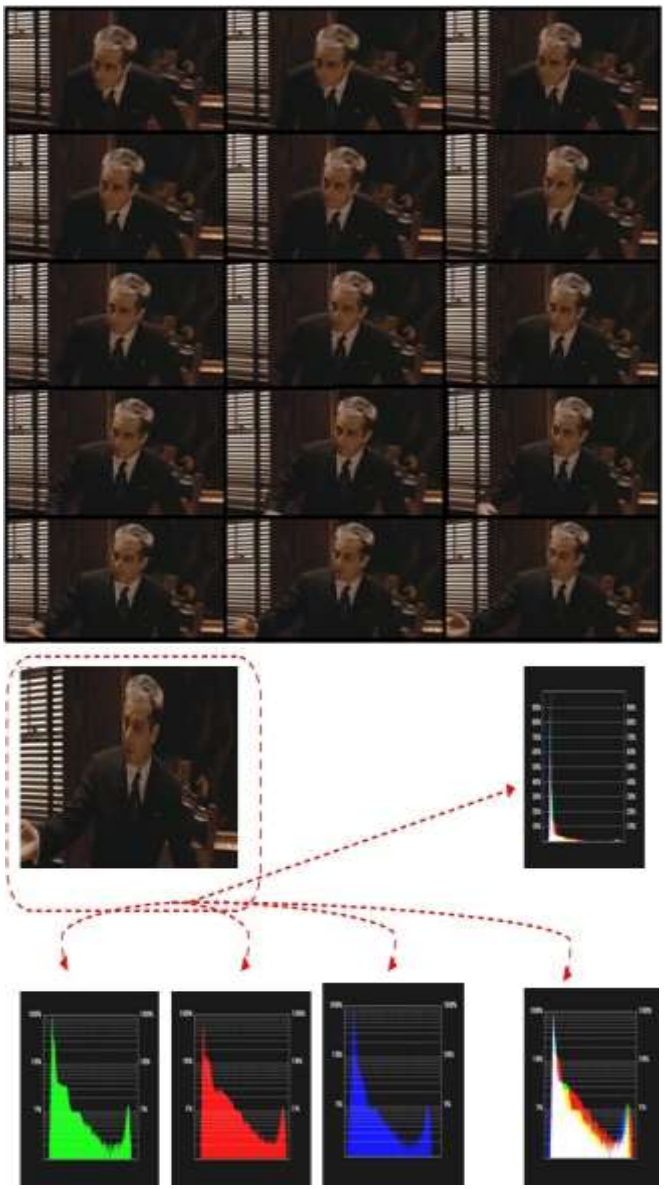

Figure 7 fifteen image frames has taken from a much known movie."Godfather" before any hidden operation, the first frame under the histogram also the three channel on RGB has been separated for more accuracy on the test

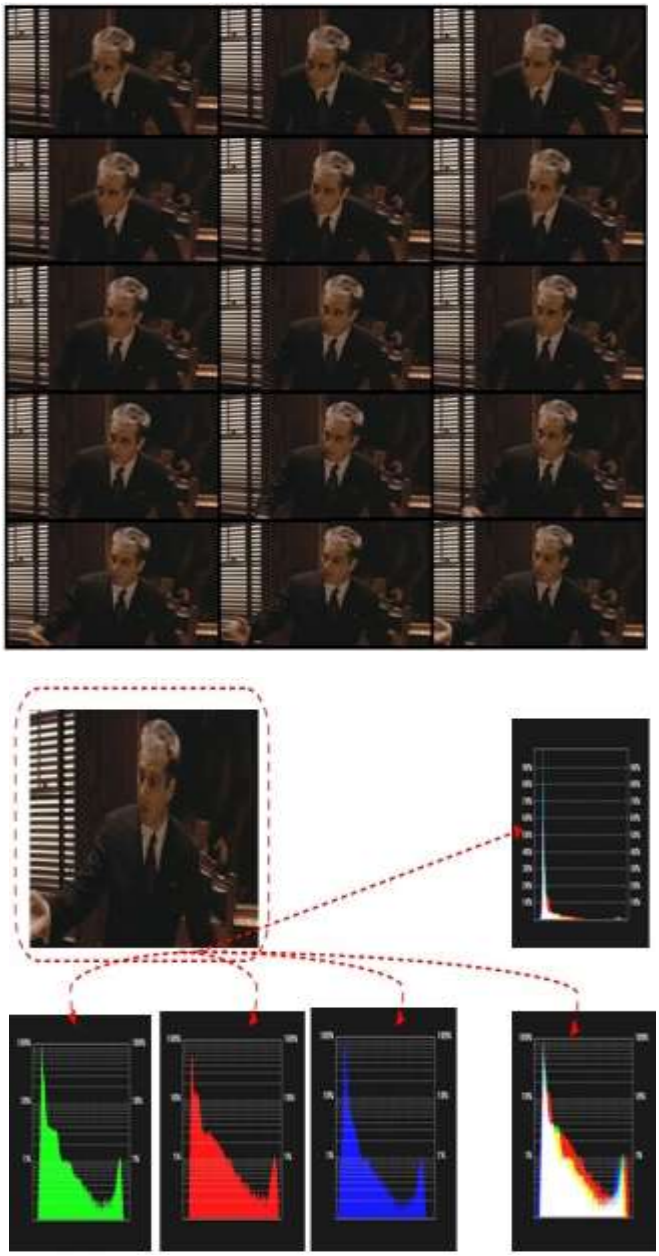

Figure 8 fifteen image frames has taken from a very known movie "Godfather" after hidden operation, the first frame under the histogram also the three channel on RGB has been separated,

VII. CONCLUSION

In this paper, a new Approach of high secure video steganography has been invented. The basis of this method is use the digital video as separate frames and hides the information inside. As the experiment result shows the success of the hidden, encryption, extract, decryption function without affecting the quality of the video. This framework overcome the defeat of the limitation of steganography approach by invited the biggest size cover file among the multimedia file which is the video. In the video steganography we have a flexibility of make a selective frame steganography to higher the security of the system or using the whole video to high a huge amount of data hidden. Due the security issues the author has chosen AES encryption method to guarantee the protection of data even the attacker somehow could hold the data

REFERENCES

[1] A.A.Zaidan, B.B.Zaidan, M.M.Abdulrazzaq, R.Z.Raji and S.M.Mohammed, "Implementation Stage for High Securing Cover-File of Hidden Data Using Computation between Cryptography and Steganography". International Association of Computer Science and Information Technology (IACSIT), indexing by Nielsen, Thomson ISI (ISTP), IACSIT Database, British Library and EI Compendex, Volume 20, 2009, Manila, Philippines.

[2] B.B Zaidan, A.A Zaidan, Fazidah Othman, R.Z.Raji, S.M.Mohammed, M.M.Abdulrazzaq, "Quality of Image vs. Quantity of Data Hidden in the Image", International Conference on Image Processing, Computer Vision, and Pattern Recognition (IPCV'09), 2009, Las Vigas, USA.

[3] Nameer N. EL-Emam, "Hiding a Large Amount of Data with High Security Using Steganography Algorithm" 2007, Journal of Computer

Science 3 pp. 223-232, 2007,ISSN 1549-3636

[4] Martin Feldhofer, Sandra Dominikus, Johannes Wolkerstorfe “Strong Authentication for RFID Systems Using the AES Algorithm”, springerlink, 2004, ISSN 0302-9743, pp 85-140.

[5] B.B.Zaidan, A.A.Zaidan, Fazidah Othman “Enhancement of the Amount of Hidden Data and the Quality of Image", Malaysia Education Security (MyEduSec08), Grand Continental Hotel, 2008, Kuala Trengano, Malaysia.

[6] A.W. Naji,Teddy S. Gunawan and Shihab A. Hameed, B.B Zaidan, A.A Zaidan " “Stego-Analysis Chain, Session One” Investigations on Steganography Weakness Vs Stego-Analysis System for Multimedia File ", International Conference on IACSIT Spring Conference (IACSIT-SC09) , Session 9, P.P 393-397**,** 2009, Singapore .

[7] A. W. Naji, Shihab A. Hameed, Md Rafiqul Islam, B. B. Zaidan,Teddy S. Gunawan, and A. A. Zaidan," “Stego-Analysis Chain, Session Two” Novel Approach of Stego-Analysis System for Image File ", International Conference on IACSIT Spring Conference (IACSIT-SC09) , Session 9, P.P 398-401 **,** 2009, Singapore .

[8] Mohamed Elsadig Eltahir, Laiha Mat Kiah, B.B.Zaidan and A.A.Zaidan," High Rate Video Streaming Steganography", International Conference on Information Management and Engineering (ICIME09), Session 10, P.P 550-553, 2009, Kuala Lumpur, Malaysia.

[9] Fazida.Othman, Miss.Laiha.Maktom, A.Y.Taqa, B.B.Zaidan, A.A.Zaidan**,** "An Extensive Empirical Study for the Impact of Increasing Data Hidden on the Images Texture", International Conference on Future Computer and Communication (ICFCC 09), Session 7, P.P 477-481, 2009, Kuala Lumpur, Malaysia .

[10] Johnson, N. F. S. D, Z., “Information Hiding: Steganography and Watermarking-Attacks and Countermeasures”, Center for Secure Information Systems (CSIS), Boston/Dordrecht/London, George Mason University, 2006.