A HYBRID APPROACH FOR THE SECURE TRANSMISSION OF H.264/AVC VIDEO STREAMS

Sheena Sathyan (Corresponding author)
M.E (Cyber Security), Noorul Islam University, Kanyakumari, India
E-mail: sheena.sathyan007@gmail.com

Shaji R S
Professor, Noorul Islam University, Kanyakumari, India
E-mail: shajiswaram@yahoo.com

Abstract: In order to keep privacy and to maintain security of a data; it was necessary to keep the data in hidden manner or in a crypt format. The proposed work describes the encryption and data hiding techniques for an H.264/ AVC video in a cloud environment. And it clearly specifies how the integrity of the data should be relevant enough in an unsecured and constrained communication medium. The proposed scheme is based on the stream cipher, RC4 encryption; while encrypting a data, it is necessary to transfer the encryption keys in a secure manner for that the public key cryptosystem is proposed for the efficient key transferring. It also explains about the data embedding via compound mapping method in order secure the original video content, and then generating the hash value for the embedded data which may contain the encrypted video content, in order to check the integrity of the data. And at the receiver end, the processes; the verification of the hash value, the decryption and extraction of the video content may be done in an efficient manner. The results may clearly shows the size of the video is strictly preserved even after the encryption and the embedding techniques.

Keywords: *H.264/AVC video,* RC4 encryption, public key cryptosystem, compound mapping, hash value.

1. INTRODUCTION

Cloud computing is one of the latest trend and the efficient storage medium in the computing and the electronic world, in which the large collections of systems were connected in both private and public networks. Securing the data (video) in a cloud network is crucial and it is important to maintain security policies like confidentially, integrity and the availability over the cloud network as well as the other networks [1]. Due to the increased demand of video (VOD); there are different standards for videos

are evolved, but the latest form of video standard is H.264/AVC (Advanced Video Coding) [2], which may designed for the efficient compression performance and in the rate-distortion efficiency in comparison with the existing standards. The fig 1 illustrates the video encoding and decoding including the transmission and storage of video signal. As said above the cloud network is very sophisticate in advent security methods

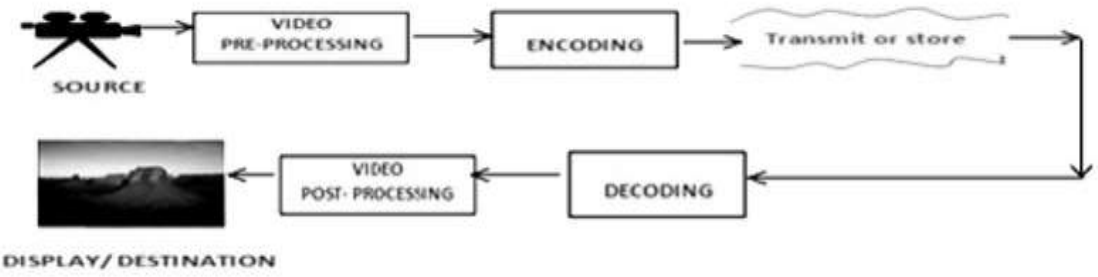


Figure 1: Video encoding/decoding standardization

Cryptic writing is a method to protect the data from a third party in order to keep the data in a confidential manner, the technique cryptography is very essential in securing the content over a network, so that the related technique; encryption is performed process of for the efficient communication between the sender and the receiver, Cryptography algorithms are of two types; symmetric algorithms (also called secret keys), or asymmetric algorithms (public and private keys) [4]. The encryption is a process in which the plaintext or the original text must be converted in an unintelligible form using a key, in order to maintain the security policy such as confidentiality and privacy [3].

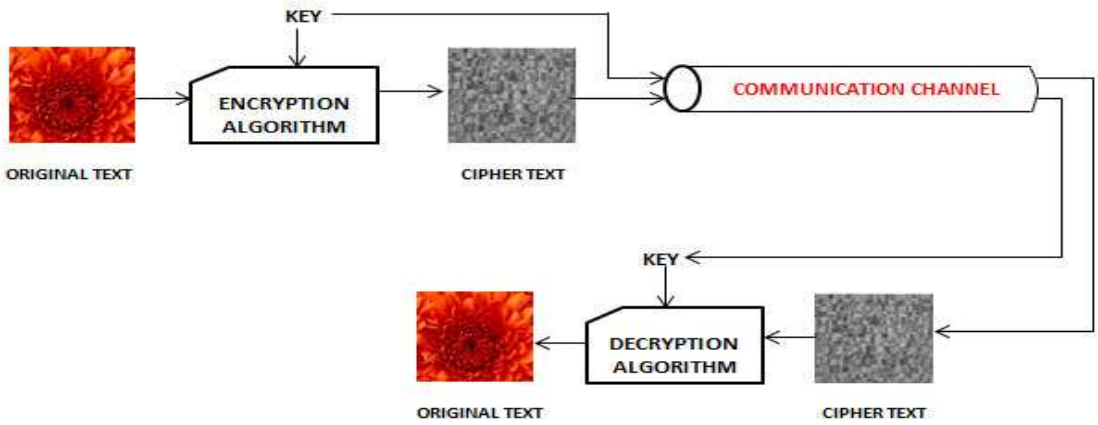


Figure 2: Encryption and Decryption of an image

The fig 2: illustrates that the encryption as well as the decryption process that may carried out in an image, it clearly specifies about the communication channel, there are possibilities for an attack in the communication channel by the attacker who will trace out the key that is used for the encryption as well as the decryption, so that a strict method or algorithm may be useful for the (Diffie Hellman key exchange algorithm) secure exchanging of the key and Diffie Hellman key exchange algorithm plays a vital role for secure transmission of key [5]. It is clear that encrypted data can't be recognized or decrypted by the attacker without the corresponding key, to betray the attacker or third party in some manner that encrypted data is covered by another data that is the embedding process.

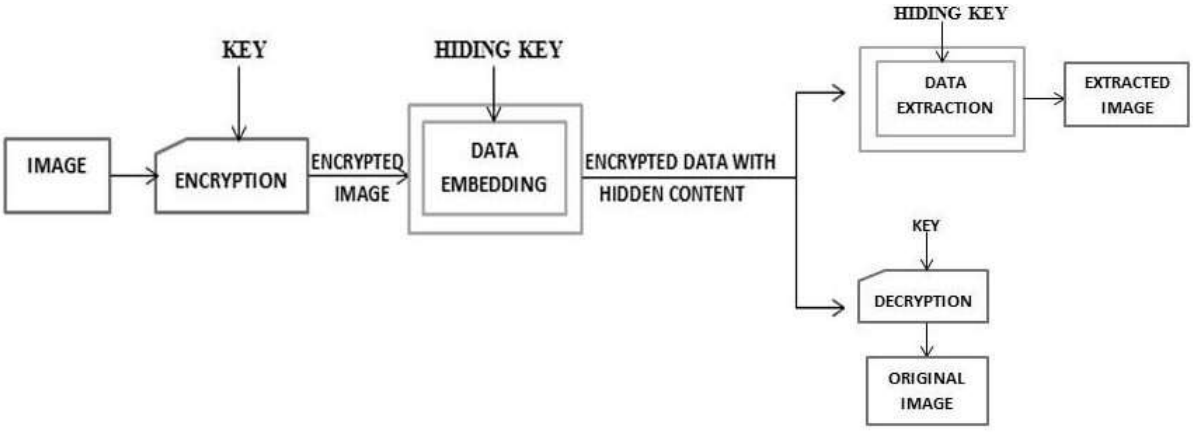


Figure 3: Reversible data hiding

Reversible data hiding (RDH) a technique is quiet familiar and congenial technique, by which the original cover can be losslessly recovered after the embedded message, is extracted [6][7]. Data hiding techniques are making used by medical imagery, military imagery and digital forensics etc. As discussed earlier the cloud security is a big concern, the security policies are confidentiality, integrity and availability (CIA) [3] [8], so that the security policies are to be followed for the better protection of data. Another method for authentication and digital signature verification is the cryptographic hash function in which the hash function maps a variable-length message into a fixed-length hash value, or message digest [3]. By definition, a cryptographic hash function is a hash function which is considered practically impossible to invert, that is, to recreate the input data from its hash vale or hash code [10]. Some examples of one-way hashing algorithms are: MD4, MD5 and SHA [9]. In embedding, hash functions is used to protect the data against some of the known attacks; for an image M, use the watermarking key KY_1 derived from a master key K by computing

$$KY_1 = MD5\ (MK; hash\ (K; I))$$

By using the cryptographic hash functions, strict authentication can be achieved [11]. Also the cryptographic hash functions can be used to produce the digital signature. The digital signature is similar to our handwritten signature the main function is maintain the authentication and it having the digital certificate using this verifies the identity of the both parties [12],[13].

2. RELATED WORKS

2.1 Data Hiding in Encrypted H.264/AVC Video Streams by Codeword Substitution[14], explains about a novel scheme of data hiding in the encrypted version of H.264/AVC videos is presented, which includes three parts, i.e., H.264/AVC video encryption, data embedding and data extraction. The content owner encrypts the original H.264/AVC video stream using standard stream ciphers with encryption keys to produce an encrypted video stream and the code word substitution for the data embedding purposes, that it eligible codewords can be substituted.

Merits are:

- ✓ Visual quality can be maintained.
- ✓ Video size can be preserved.
- ✓ Algorithm can preserve the bit-rate exactly even after encryption and data embedding.

Demerits are:

- ✓ Secure key transferring is not established.

2.2 Implementation of New Modified MD5-512 bit Algorithm for Cryptography [15], explains about the algorithm of modified MD5-512 and its security protection. Hashing algorithms are one of the vital components in many cryptographic applications and security protocol suites. A hash function may computes the hash value (message digest) of an input message of various lengths to a fixed length output. To provide higher security protection, MD5-512 has been proposed, MD5-512 accepts the same input format as that of MD5 hashing algorithm, and produces a 512-bit output. The major purpose of the MD5 hashing algorithm is to check the integrity of the data that it

shows, whether the data is modified or not. MD5 is an irreversible transformation transforming a set of data of any length into a hash value of 128-bit length and it is a consecutive processing method. Before operation, initially it fills data to be processed, and adds 64-bit binary digits to the end of data representing the bit length of the original data. After filling, the bit length of data which is being processed becomes a multiple of 512. Then the data are divided into groups of 512 bits and computations are performed on each group orderly.

Merits are:

- ✓ Cracking password is difficult.
- ✓ Simple and easy solution to implement the increasing length of HASH.

Demerits are:

- ✓ Longer HASH by more complex computing can obtain more secure document verification.

2.3 Cryptanalyzing of Message Digest Algorithms MD4 and MD5[16], explains about the comparison by analyzing the cryptic prons and cons between the MD4 and MD5 hashing algorithm the hashing algorithms MD5 as well as the MD4, is used to generate the message digest value for the corresponding input value. The main purpose of the hash function is used for checking the integrity of the messages, digital signatures and digital time stamping. Among the digest algorithms MD4 and MD5 are most popular. Both these algorithms perform a set of bitwise logical operations. They generate 128-bit digest values from a given message. Time complexity of MD5 is more than MD4 and hence somewhat slower to execute. It also explains about the attacks that may happen on the hashing algorithms. MD4 and MD5 is very important hash function which is being commonly used for file integrity checking and as a message digest in digital signature schemes. The following five steps are performed to compute the message digest of the message.

- Append Padding Bits.
- Append Length.
- Initialize MD Buffer.
- Process Message in 16 Word Blocks.

- Output.

Merits are:

- ✓ MD4 can be analyzed. If the message size is increased, the running time is also increased.
- ✓ It can ensure that the security aspects of the information.

Demerits are:

- ✓ Complexity in calculating the hash value

2.4 A robust data hiding algorithm for H.264/AVC video streams [17], explains about a robust readable data hiding algorithm for H.264/AVC video data without intra-frame distortion drift. There are 3 steps to be followed; initially, encode the embedded data using BCH (n, k, t) syndrome code before data hiding for the purpose of improving robustness. Next step is to embed the encoded data into coefficients of the 4 × 4 luminance discrete cosine transform (DCT) blocks in I frames. Final step is to recover the original video as much as possible when the hidden data is extracted out. The experimental results show that our scheme can get more robustness, effectively avert intra-frame distortion drift and get high visual quality. The main objective of H.264/AVC is used for recording, compression, and distribution of video content, video-processing operations, various attacks, and so on. Using this robust data hiding algorithm, embedded bits are not survive from network transmission, packet loss, video-processing operations, various attacks, and so on. The embedded message can be retrieved correctly because the embedded bits can be recovered without any error.

Merits are:

- ✓ Data hiding techniques based on error correction codes is that those techniques enable to hide the embedded data into a block of coefficients using many different ways.
- ✓ BCH code before data hiding to improve robustness.

Demerits are:

- ✓ Suffer from the subjective visual quality degradation due to the error propagation of the intra prediction used in H.264/AVC.

- ✓ Not handled the intra-frame distortion drift.
- ✓ Cannot extract the exact embedded content.

2.5 Hybrid Algorithm with DSA, RSA and MD5 Encryption Algorithm for wireless devices [18], explains the a study of hybrid encryption that can be carried out with DSA, RSA, MD5 algorithm, As Encryption became a vital tool for preventing the threats to data sharing and tool to preserve the data integrity so we are focusing on security enhancing by enhancing the level of encryption in network. The main objectives of the Study are: the issues of Security for Different networks and harden up the Encryption Process for Network Security, to study about the already implemented algorithms for public key exchange in communication of data. And to provide a stable encryption, this can make good communication without carrying about data integrity threat.

Merits are:

- ✓ Better security can be provided

Demerits are:

- ✓ complex in nature

2.6 Enhancing the Diffie-Hellman Algorithm [19], explains about the secure transferring of the cryptographic keys between the two authorised parties, it is necessary to secure the keys because if the attacker is supposed to gain the access to the key, it will lead to the end of the story. The proposed work explains about the key distribution through the "Diffie –Hellman algorithm". Diffie–Hellman key exchange is a specific method of exchanging cryptographic keys. The Diffie–Hellman key exchange method permits two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel.

Merits are:

- ✓ Secure cryptic keys transferring through the insecure communication channel.

Demerits are:

- ✓ Chance for brute force attacks.

3. MODELING AND ARCHITECTURE

In this section, it explains the of data hiding in the encrypted version of videos is presented, which may including five parts, i.e., H.264/AVC video encryption, data embedding, hashing ,verification and data extraction. The sender encrypts the video stream using the MD5 encryption algorithm and producing the encrypted video stream, and the key exchanging is secured by the public key cryptosystem; Diffie Hellman key exchange algorithm, then the data embedding process may carried out on the encrypted video streams using compound mapping algorithm, the hash value must be produced for the encrypted video with hidden content in order to optimize the authentication process and at the receiver side further extraction and decryption processes may carried out.

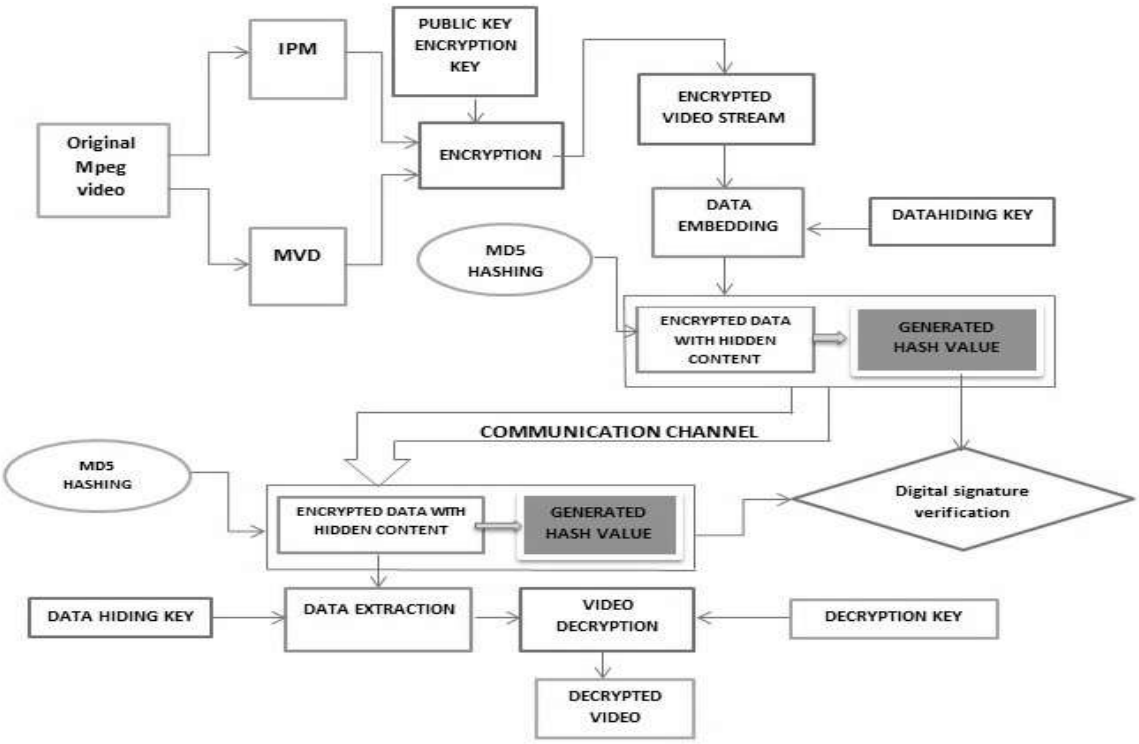


Figure 4: Architecture for the proposed work

3.1 ENCRYPTION OF THE VIDEO STREAM PUBLIC KEY CRYPTOSYSTEM

This section explains about the encryption process, in which the encryption is process of converting the original text in to a cipher text using the key. The symmetric stream

cipher RC4 [20], which may encrypt one byte at a time, which may be helpful to encrypt the video streams in an efficient manner. The rc4 algorithm may make use of the bitwise XOR operation for the encryption and the sequential decryption process. The following example may show the bitwise XOR operation,

101001011 ⊕ ←PLAIN TEXT
011001010 ←KEY STREAM
110000001 ←CIPHERTEXT

The following figure illustrates the encryption process for the video streams using the rc4 encryption algorithm, in which the pseudorandom byte generator is there to encrypt the byte of the video streams.

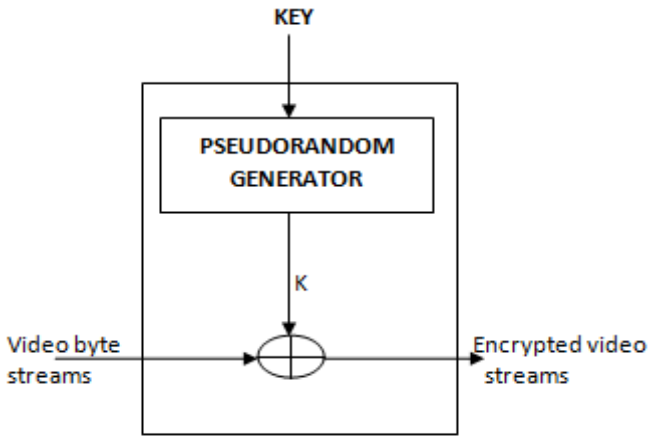


Figure 5: RC4 encryption on video streams

RC4 ALGORITHM DESCRIPTION

STEP 1: Initialize the state vector V (variable-length key of from 1 to 256 bytes) is used, with elements V[0], V[1], …, V[255].

STEP 2: A temporary vector VT, is also created.

STEP 3: If the key length is 256 bytes, then K is forwarded to temporary vector VT.

STEP 4: Otherwise, for key length *kylen* bytes, the first *kylen* elements of VT are copied from K.

STEP 5: Then k is repeated as necessary time in order to fill out VT

STEP 6: Temporary vector VT is used to produce the initial permutation of state vector V.

STEP 7: Once state vector s is initialized, stream generation is started and a swap over for each V[i] with another byte in V.

STEP 8: For encryption, XOR the value *K* with the next byte of plaintext.

STEP 9: For decryption, XOR the value *K* with the next byte of ciphertext.

The most vital part in an encryption process is that the transfer of the encryption key in a secure manner between the end users [21]. For secure key exchange the proposed scheme uses the Diffie Hellman key exchange algorithm [22],

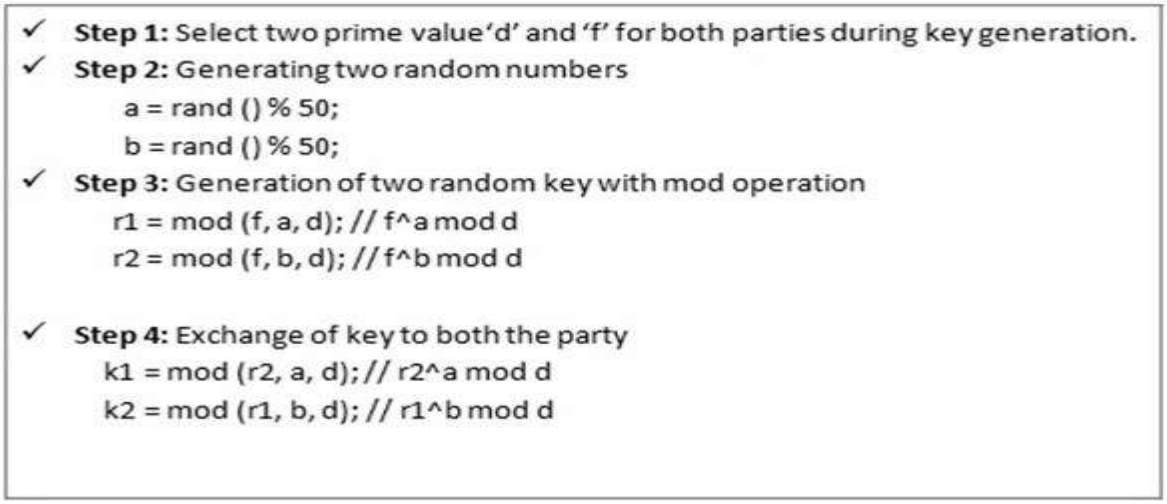


Figure 6: Diffie Hellman key exchange algorithm

3.2 DATA EMBEDDING PROCEDURE IN ENCRYPTED VIDEO

This section explains about the embedding process in which the compound mapping[23], Keeping generic lossless visible watermarking approach as the base paper, it implemented watermarking for image, the procedure has been extended to Encrypted video with that extraction module has one for module for extracting the watermark. Attacks against watermarking are regarded as common image recovery problems. To make watermark more useful, must care about its robustness against a various kind of possible attacks.

The fig 8 illustrates the compound mapping method that can be used for the embedding process. Let us consider the pixel values for color image video source A=(220,156,120), P=(230,134,70), B=(30,13,70) then E2=(40,35,120) where,

Q - Original video source

A-Original encrypted image

B-Data to hide,

P-Nearest pixel value in encrypted image

E1- encrypted (Q),

E2-encrypted image with additional data, which can be computed by the following equation

$$E2 = E1(F^{-1}{}_{B}(F_A(P))$$

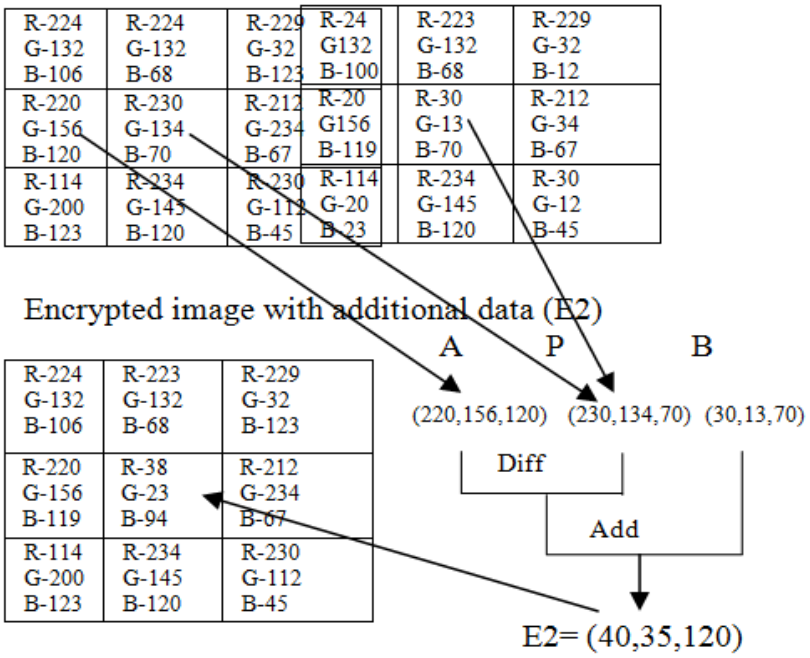


Figure 7: compound mapping method

3.3 HASHING

Hashing [24] is process of achieving the binary equivalent (hash value or message digest) of data which may be useful for authentication and checking the integrity of the data. It is important in checking the hash value while data must be transmitted in an unsecure communication channel, because if the communication channel is vulnerable

so that there is a chance for an attacker to intercept and do the unwanted things like modification , gaining the information etc.. therefore the sender have the responsibility to generate a hash code of the content they were wish to forward, then encrypts it and send it with the content. There are so many algorithms that produce the hash value, MD5, SHA1, RIPEMD [3] etc...

The proposed scheme uses MD5 hashing algorithm, created by Ronald .L. Rivest in 1991 [25], which is an one-way hash function it denoting that it takes a message or input and converts it into a fixed string of digits called message digest

Example for Message digest5 = "9b5b8f6ce6c4024b35bbo29388d94ee1"

MD5 algorithm takes input message of arbitrary length and generates 128-bit long output hash. MD5 hash algorithm may consist of 5 steps

- ✓ **Step 1. Append Padding Bits**
- ✓ **Step 2. Append Length**
- ✓ **Step 3. Initialize MD Buffer**
- ✓ **Step 4. Process Message in 16-Word Blocks**
- ✓ **Step 5. Output**

And the verification part is done through the method digital signature, ie a digital code that can be produced and attach with the message which uniquely identifying the sender of the message or said to be the content owner. The main purpose of the digital signature is for authentication [26]

3.4 DATA DECRYPTION AND EXTRACTION

This segment explains about the sequential data extraction and decryption. The data can be extracted from the encrypted video by the compound mapping [23] function by using this function can recover the original source video and can extract the data without any loss. it is necessary to perform the decryption and extraction in an efficient manner. For extraction may carried out using the data hiding key which may essential for the further decryption process [20] of the encrypted video streams. For decryption, perform bitwise XOR operation between cipher text and key stream to get the plain text

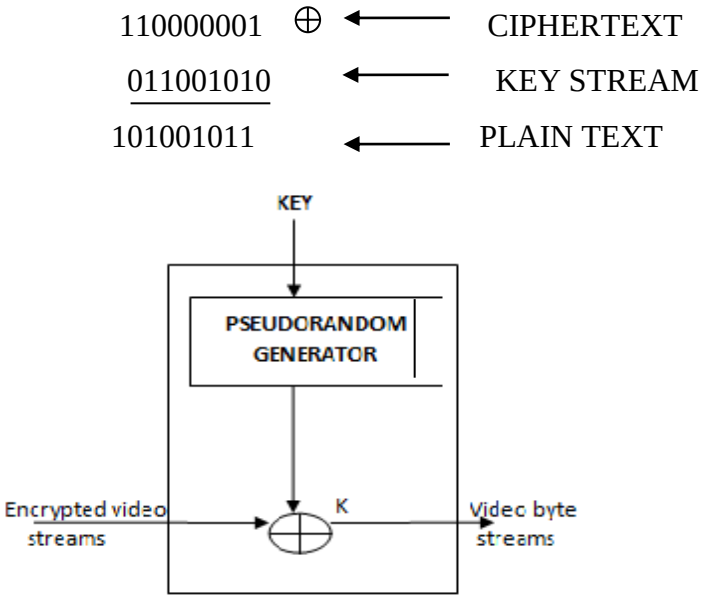


Figure 8: Decryption of the encrypted video streams

The figure 8 above shows the how the decryption process may carry out in the encrypted video streams. The encrypted video streams are XOR with the random keys generated by the pseudorandom generator with produces the original video streams out.

4. IMPLEMENTATION AND DISCUSSION

The proposed scheme is data hiding in an encrypted h.264/AVC video. The video frame taken for the proposed work is 50 from the video sequence, wherein size of each frame is 256x256. The GOP (Group of Pictures) structure is "IPPPP: one I frame followed four P frames".

4.1 SECURITY

It may concern about both the cryptographic security *(security against cryptographic attacks)* as well perceptual security (*whether the encrypted video is intelligible or not*) [14]. It is secure enough to produce a pseudorandom byte key generation scheme to scramble over or to encrypt the video stream using the stream cipher RC4 which is enough to keep the perceptual security, but for further resistance over the communication network protecting the key is also a very big concern, for the secure transmission of the key can be done through the Diffie Hellman key exchange algorithm and the authentication and the integrity checking is based on the MD5 hashing

algorithm. This video has been encrypted using a range of 0 to 255-bit long key which is produced randomly by the key generator thereby generating all possible combination of the key to encrypt the video frames and tested over the encrypted video stream and further decryption may possible only via the exact combination that done by the generator. To evaluate the perceptual quality; PSNR (Peak Signal to Noise Ratio), SSIM (Structural Similarity Index) adopted [14]. PSNR (Peak Signal to Noise Ratio), SSIM (Structural Similarity Index) is widely used objective video quality metric, which it may explains the video quality between the original video and the video after performing the extraction and decryption process, if the PSNR value is high means , lesser the video degradation, that is the quality of the video can be maintained . The SSIM value also shows the quality of the video even after the extraction and decryption process. The PSNR [27] is defined via the mean squared error (MSE). Given a noise-free i x j monochrome image M and its corresponding noise approximation is K; MSE is calculated by the equation,

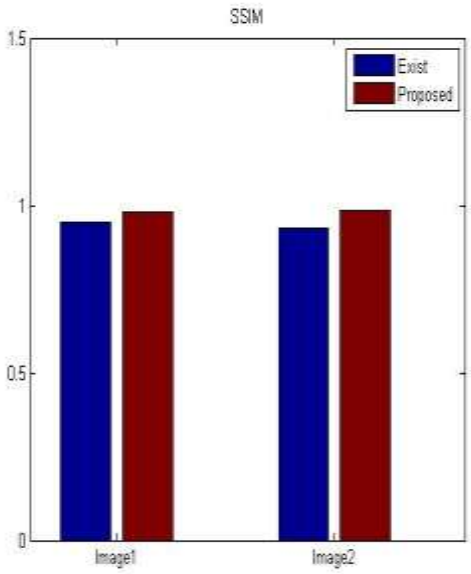
$$\text{MSE}= \frac{1}{i,j} \sum_{m=0}^{i-1} \sum_{n=0}^{j-1} \{M(m,n) - K(m,n)\}^2$$

Also the PSNR value can be calculated using the equation,

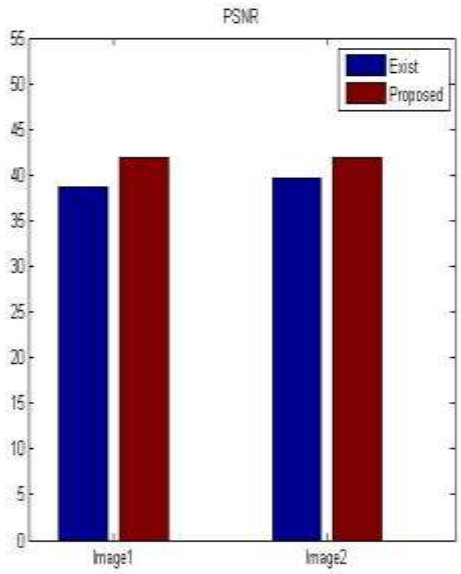
$$\text{PSNR} = 10.\log_{10} \left(\frac{MAX_M^2}{MSE} \right)$$, where the MAX_M denotes maximum possible pixel value.

The structural similarity (SSIM) index is the method to calculate the similarity between two images, if the measure between two images ‘a’ and ‘b’ of same size i x i is calculated by [28],

$$\text{SSIM (a, b)} = \frac{(2\mu_a\mu_b+c1)(2\sigma_{ab}+c2)}{(\mu_a^2+\mu_b^2+c1)(\sigma_a^2+\sigma_b^2+c2)}$$



Graph 1: PSNR analysis



Graph 2: SSIM analysis

Based on the analysis of the related works and the proposed work, the above graph illustrates the proposed work has the PSNR value ‘41.8995’ which is comparatively higher than the existing works with an range existing between 35 to 40 and the graph which showing the mean value of the overall PSNR value. Similarly the SSIM value ‘0.985571’ which is good enough when comparing the existing works, thereby the visual quality can be maintained even after the reconstruction of the video. For further performance evaluation variation in the bit rate [14], is also calculated which is caused by the encryption and the embedding process which is 0.745887and will shows the security has been sufficiently maintained in the proposed work.

4.2 SPEED

A high quality video at the frame rate of 30 fps (frames/s) is used for simulation which may be fast enough to encrypt the data in order to transmit it in a real time communication channel. The figure shown below illustrates the screen shot of the sender side processes which is encryption, embedding and hashing of the embedded data

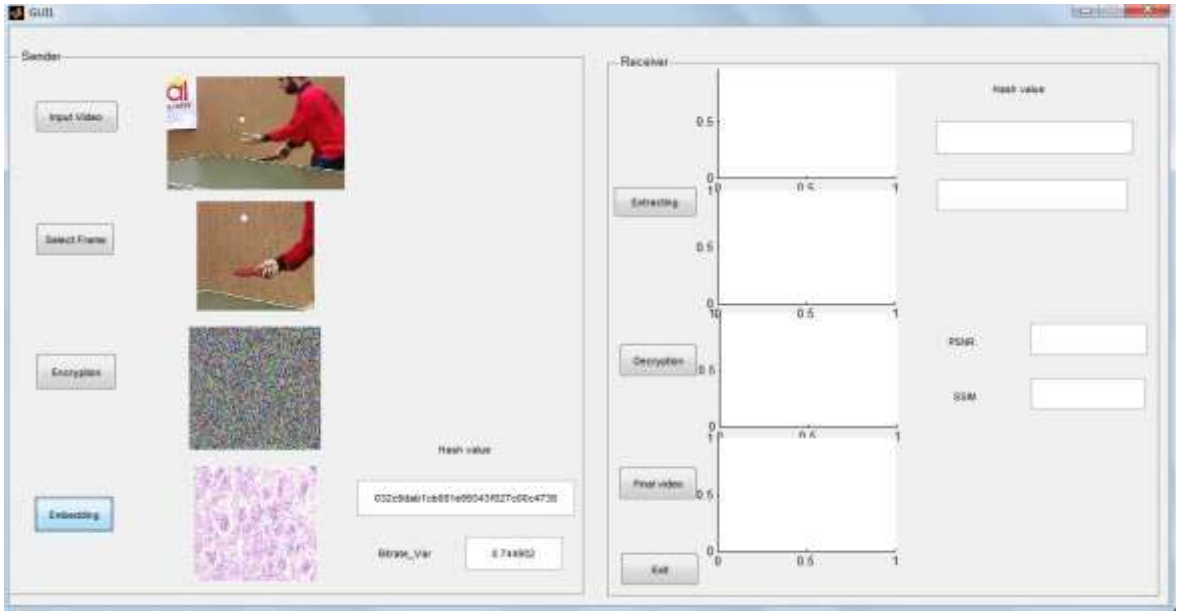


Figure 9: Sender side processes

4.3 DATA EMBEDDING AND CORRESPONDING LOSSLESS RECOVERY

Since the pixels valued manipulation is used in the embedding algorithm which is the mapping function for each frame of the video which is efficient in some manner to embed the data and extracted out the data without any loss.

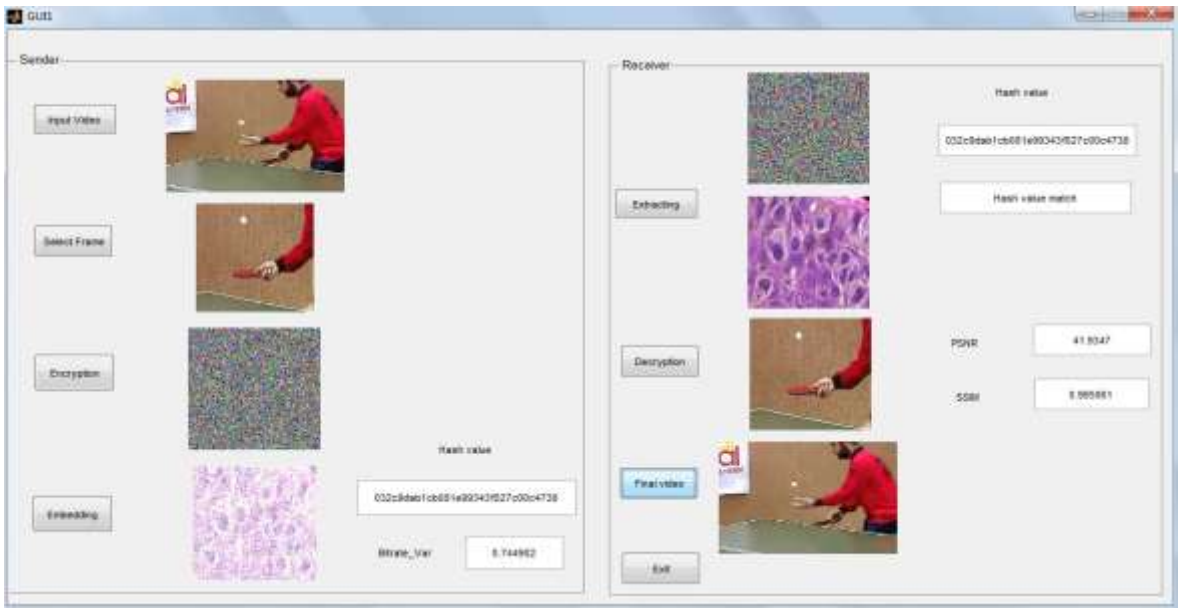


Fig 13: Receiver side processes.

5. CONCLUSION

The hybrid method which may strictly concern with the cryptographic security and perceptual security also the authentication between the end users is considering via md5 hashing technique, which may fulfilling the security policy. The encryption is based upon the scrambling method which may use a stream cipher RC4 for efficient key generation and combination with a random effect. The key transferring through a constrained and unsecured bandwidth communication is prevented or possible via the Diffie Hellman key exchange algorithm, the embedding of data via compound mapping function which is based up on pixels valued manipulation which is an efficient enough to preserve the size of the file as well as the degradation of the video quality is comparatively less caused by the data hiding technique. And the MD5 hashing technique is used in this implementation which is necessary for the integrity checking and to keep the authentication between the end users. Signature verification, the sequential decryption and extraction process can be also carried out on the receiver end.

6. REFERENCES

[1]. http://www.thbs.com/downloads/Cloud-Computing-Overview.pdf.

[2]. Thomas Wiegand, Gary J. Sullivan, Gisle Bjøntegaard, and Ajay Luthra, "Overview of the H.264/AVC Video Coding Standard", ieee transactions on circuits and systems for video technology, vol. 13, no. 7, july 2003, pp. 560-576.

[3]. William Stalling, A Handbook on "Cryptography and network Security" by Pearson Education, 2009

[4]. 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, pp. 103-110.

[5]. Ms. Jyoti Gaba, Ms. Neha Rani and Dr. Mukesh Kumar, "A Review Based Study of Key Exchange Algorithms", International Journal of Recent Trends in Mathematics & Computing, IJRTMC Vol. 1, Issue 1, Oct 2012, pp.25-29.

[6]. Sunita.G.J and Syeda Asra," Reversible Data Hiding For Embedding Data Securely in Encrypted Image by Reserving Room Before Encryption", IJEDR Vol. 2, Issue 2 © 2014, pp. 2889- 2893.

[7]. K.S.AISWARYA, RAMJI D.R, Dr. SREEJA MOLE S.S," A SURVEY PAPER ON DATA HIDING TECHNIQUE BASED ON CODEWORD SUBSTITUTION ALGORITHM", International Journal of Engineering Research-Online, Vol.3, Issue.1, 2015, pp.7-13.

[8]. Sattarova Feruza Y. and Prof.Tao-hoon Kim, "IT Security Review: Privacy, Protection, Access Control,
Assurance and System Security", International Journal of Multimedia and Ubiquitous Engineering
Vol. 2, No. 2, April, 2007,pp.17-31

[9] B. Schneier, "Applied Cryptography", John Wiley and Sons, 1996.

[10]. http://en.m.wikipedia.org/wiki/Cryptographic_hash_function.

[11] Jansi Mohamad Zain, "Strict authentication watermarking with JPEG compression for medical images", *European Journal of Scientific Research*, Vol. 42, No. 2, 2010, pp. 232-241.

[12]. A. Umamageswari and G. R. Suresh, "Performance Analysis Of Secure Medical Image Communication With Digital Signature And Reversible Watermarking", ictact journal on image and video processing, august 2013, volume: 04, issue: 01,pp.647-651.

[13]. M.Sreerama Murty, D.Veeraiah, A.Srinivas Rao," Digital Signature and Watermark Methods
For Image Authentication using Cryptography Analysis", Signal & Image Processing : An International Journal (SIPIJ) Vol.2, No.2, June 2011, pp.170-179.

[14]. Dawen Xu, Rangding Wang, and Yun Q. Shi, *Fellow, IEEE, "*Data Hiding in Encrypted H.264/AVC Video Streams by Codeword Substitution", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 9, NO. 4, APRIL 2014, Pp:592-606.

[15]. Priyanka Walia and Vivek Thapar, "Implementation of New Modified MD5-512 bit Algorithm for Cryptography", International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349-2163, Volume 1 Issue 6 (July 2014), pp:87-97.

[16]. Md. Alam Hossain, Md. Kamrul Islam, Subrata Kumar Das and Md. Asif Nashiry, "Cryptanalyzing of Message Digest Algorithms MD4 AND MD5", International Journal on Cryptography and Information Security(IJCIS),Vol.2, No.1,March 2012, pp:1-13.

[17]. YunxiaLiua, Zhitang Li, XiaojingMa and JianLiua, "A robust data hiding algorithm for H.264/AVC video streams", The Journal of Systems and Software 86 (2013), pp. 2174-2183.

[18]Khushdeep Kaur and Er. Seema, "Hybrid Algorithm with DSA, RSA and MD5 Encryption Algorithm for wireless devices", International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 5, September- October 2012, pp.914-917

[19]. Rohini and Er.Meenakshi Sharma, " Enhancing the Diffie-Hellman Algorithm", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 6, June 2014, pp: 448-452

[20]. http://cse.spsu.edu/afaruque/it6833/rc4.pdf

[21]. Y. Amir, Y.Kim, C. Nita-Rotaru, " Secure communication using contributory key agreement", IEEE Transactions on Parallel and Distributed systems, pp. 468-480,2009.

[22]. Mr. Randhir Kumar, Dr. Ravindranath C. C, "Analysis of Diffie Hellman Key Exchange Algorithm with Proposed Key Exchange Algorithm", *International Journal of Emerging Trends & Technology in Computer Science* , Volume 4, Issue 1, January-February 2015,pp.40-43.

[23]. K.Madhu Kumar, Mr. M.Katta Swamy, Mr. Brahma Reddy, " Lossless Visible Watermarking Using Compound Mapping", International Journal of Engineering Research and Development, Volume 4, Issue 9 (November 2012), PP. 27-35

[24]. http://www.webopedia.com/TERM/H/hashing.html.
[25].http://nepsin.com/mem/projects/md5.html.

[26]. D. W. Xu, R. D. Wang, and J. C. Wang, "Prediction mode modulated data-hiding algorithm for H.264/AVC," *J. Real-Time Image Process.*, vol. 7, no. 4, pp. 205–214, 2012.

[27]. http://en.m.wikipedia.org/wiki/Peak_signal-to-noise_ratio

[28]. http://en.m.wikipedia.org/wiki/Structural_similarity.