Volume 5, Issue 2, F ebruary 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Secure Video Transfer

Neethu. J, Drisya. A. R, Midhun. A, Swathi Krishna .N .K, Pranav .P .T
CSE at Sreepathy Institute of Management and Technology &
Calicut University, Kerala, India

Abstract— Cryptography is the art and science of protecting information form undesirable individuals by converting it into a form non-recognizable by its attackers while stored and transmitted. The main goal of video encryption is keeping video secure from unauthorized attackers. The reverse of video encryption is video Decryption, which regenerates the original video. There are many encryption algorithms .Each has its own disadvantages and advantages. It is impossible to solve all encryption issues. But it is possible to reduce those issues by introducing new algorithms.

Combination of AES algorithm and a shuffling algorithm can be used to encrypt a video effectively. First the video will be cut into frames and then it will be shuffled. These frames are randomly placed to form a video and the shuffling key will be encrypted using AES along with the video. Here a random key is generated to perform the shuffling. Random key is generated using a random key generation algorithm. Here we are using midsquare as the random key generation algorithm.

Keywords—Cryptography, Video encryption, Image processing, Encoding, Video cutting, Code word extraction, Shuffling, Video Decryption.

I. INTRODUCTION

Due to the development of multimedia communication technology, wireless mobile terminals, such as PAD and smartphones, are no longer just for calls and SMS, and instead, become especially popular nowadays for transmission or storage of multimedia data, such as images and videos. In real-world applications, a video encryption algorithm should take various requirements into account, which include security, computational efficiency, compression efficiency, format compliance and so forth. Different video applications require variable levels of security. For example, for Video on Demand (VoD) or pay-TV, low security is required, and sometimes, even non-paying users are allowed to access low-quality versions to promote them to buy high-quality versions, whereas for military secrets or financial information, strict security is demanded to completely prevent unauthorized access.

An attack is a deliberate attempt to compromise a system. It usually exploits weaknesses in the systems design, implementation, operation, or management. Hence we can say that security is about how to prevent attacks. An encryption scheme is secure in a given adversary model if it is computationally in feasible for the adversary to determine the target decryption key under assumptions of the given model. Some encryption schemes are provably secure, however these schemes are often inefficient.

Encryption is the process of converting the plain text to a cipher text. Decryption is the reverse process of encryption. With the fast growth of multimedia technology many armies across the world are using videos to train newly recruited troops. Such sensitive data has to be protected either in transmission or storage. One possible way to protect multimedia information is to stop unauthorized access. But this method is practically impossible. To protect the data we can encrypt it using a suitable secure encryption algorithm.

Encryption can be done using any encryption algorithms such as AES or DES. Videos generally possess a large amount of data and require real-time operations. In wireless mobile systems, there is limited processing, memory and bandwidth, and is rarely able to handle the heavy encryption processing load. Therefore, a selective encryption algorithm must be used which provide high security, computational efficiency and compression efficiency. In this method, only parts of video content are encrypted, thereby reducing the computational requirement. This method is suitable because the full content of the video is not critical. But using a single AES or DES alone can't make the encryption process secure. To provide a secure video encryption a new approach is needed. The new approach uses a partial encryption method with AES. For partial encryption we can use VEA. To increase the efficientcy of this method a shuffling algorithm can be applied. Hence it can reduce computational time and increase security.

II. SYSTEM ARCHITECTURE

Input a video which need to be encrypted. The video encryption is the process of converting the secret video to encrypted video. To make the encryption more effective and secure we can use more than one algorithms. Input the video to a video converter which converts the video format to H.264.

Once the video is converted to the specified format it is divided into a number of frames. A frame is composed of picture elements just like a chess board. Each horizontal set of picture elements is known as a line. When the moving

picture is displayed, each frame is flashed on a screen for a short time and then immediately replaced by the next one. The frame is also considered as a unit of time. After cutting the video to frames, depending on the frame number the frames must be classified to even and odd. Even frames and odd frames are classified to different folders.

Once the frames are classified then the even frames are encrypted using the AES (Advanced Encryption Standard). The bag of words model (BoW model) can be applied to image classification, by treating image features as words. To represent an image using BoW model, an image can be treated as a document. AES is one of the most effective symmetric key algorithm contains mainly four functions bytesub, shiftrow, mixcolumn and addroundkey [2, 6].

After encrypting even frames, both odd and even frames are shuffled using a frame shuffling algorithm. To generate the key for shuffling algorithm we can use any random key generation algorithm such as midsquare. Once the shuffling is completed the frames are stitched together to form an encrypted video. Now this video can be transmitted over the network.

Decryption is the process of converting the encrypted video to original video. First video is cut in to frames and reshuffled using a reshuffling algorithm. Once reshuffling is done the frames are classified to even and odd frames. Even frames are decrypted using the AES and then stitched together with the odd frames to form the original video [3].

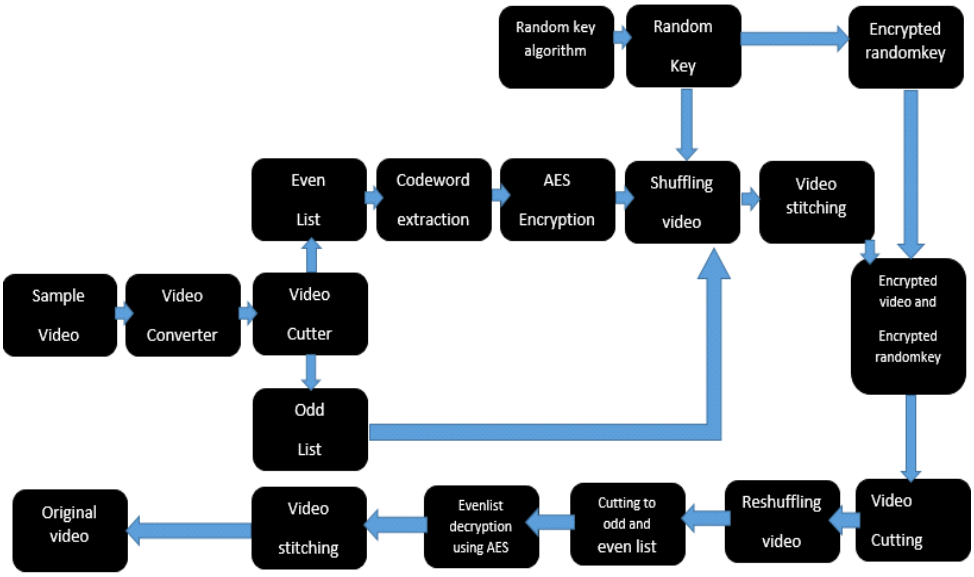


Figure 1.1 System Architecture

III. MODULE DECRYPTION

A. Video cutting block

Input the original video in to a video converter to convert the video format to standard h.264. H.264 is a standard for video compression which has more advanced compression methods than the basic MPEG-4 compression. One of the advantages of H.264 is the high compression rate. It is about 1.5 to 2 times more efficient than MPEG-4 encoding. This high compression rate makes it possible to record more information on the same hard disk. The image quality is also better and playback is more fluent than with basic MPEG-4 compression. The most interesting feature however is the lower bit-rate required for network transmission.

Once the video is converted, the video is given to the video cutter. The video cutter cut the video to a number of frames based on the size of the video. A frame is composed of picture elements just like a chess board. Each horizontal set of picture elements is known as a line. When the moving picture is displayed, each frame is flashed on a screen for a short time and then immediately replaced by the next one. The frame is sometimes used as a unit of time [6]. Historically, video frames were represented as analog waveforms in which varying voltages represented the intensity of light in an analog raster scan across the system. In moving picture (TV) the number of frames scanned per second is known as frame rate. The higher the frame rate, the better the sense of motion. But again, increasing the frame rate introduces technical difficulties [3].

B. Codeword extraction

Bag of features (BoF) representation has attracted an increasing amount of attention in large scale image processing systems. BoF representation treats images as loose collections of local invariant descriptors extracted from them. To build a compact and discriminative codebook, codeword selection has become an indispensable tool. However, most of the existing codeword selection algorithms are supervised and the human labeling may be very expensive. Images are usually represented by the low level visual features (e.g., colour, texture and shape) extracted from them, and relevant images are retrieved based on the similarity of their visual features. A small codebook may be lack of discriminative power, because dissimilar descriptors may be mapped to the same codeword. On the other hand, a large code-book may cause the problem that similar descriptors are mapped to different codewords. Notice that the dimension of the frequency histograms in BoF representation is equal to the size of the codebook. A large number of codewords not only requires more storage and computation resources cost of the existing codeword selection algorithms are supervised,

which largely limits their applicability in a variety of applications. With the growth of the number of images, providing label information to guide the selection of discriminative codewords becomes infeasible in both time and cost-wise.

The following three codeword selection algorithms are compared:

• Discriminative Codeword Selection (DCS) . The unsupervised codeword selection algorithm introduced in this paper.

• Codeword selection based on the Q−α algorithm Q−α is a unsupervised feature algorithm which selects features to maximize the cluster coherence.

• Codeword selection based on the Unsupervised Feature Selection using Feature Similarity (FSFS) FSFS4 uses feature similarity for redundancy reduction

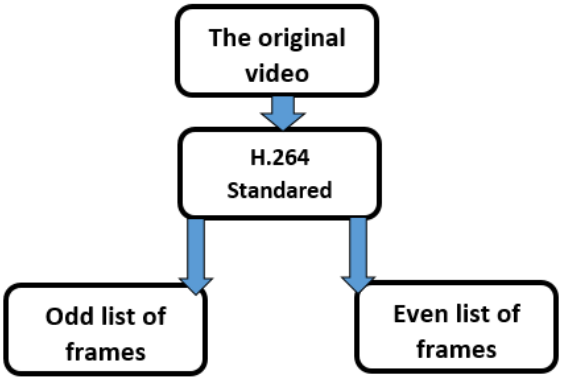


Fig 2.1, Cutting block

C. AES (Advanced Encryption Standard)

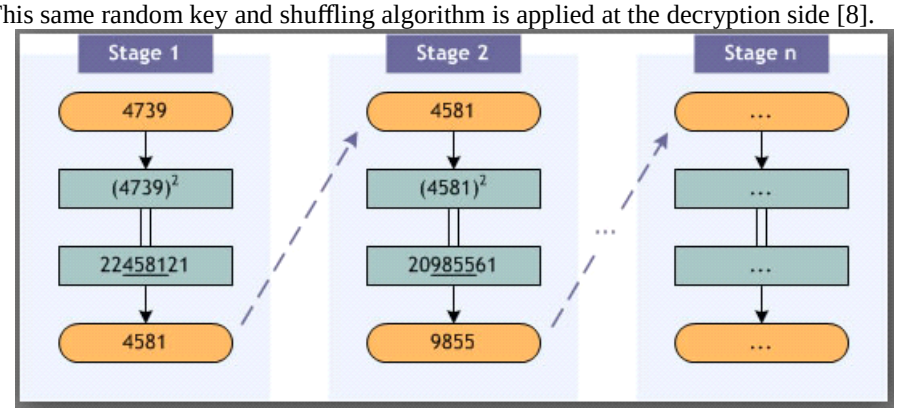
Brute-force attacks have become more sophisticated, groups of expert video analysts may sit together and analyse the entire video frame by frame and may bring together the original video. Hence there is a need to increase the security further to prevent such Brute force attacks. To do this AES is required.

AES is based on a design principle known as a substitution-permutation network combination of both substitution and permutation, and is fast in both software and hardware. Unlike its predecessor DES, AES does not use a Feistel network. AES operates as a matrix of bytes, termed the state. AES requires a separate 128-bit round key block for each round plus one more. The four major operations are byte sub, shift row, mix column and add round key. After applying AES encryption we have to shuffle the video frames to a disorder manner in order to prevent direct attack to the frames. We are not applying AES encryption to the odd list. Now the attacker can't break this method and he cannot find the original video even he gets the key. Hence we can ensure that the video is secure from attacker [4].

D. Shuffling and Random key generation

The frame is considered as the unit of time. Once the video is cut in to a number of frames the encryption is done at even list. Then a shuffling algorithm is used to change the order of frames. For shuffling process a key is needed. The key can be generated in a random manner. For generating random keys we are using a random number generation algorithm. Here we are using the midsquare algorithm which is also known as middle square method. This method is commonly used in hashing strategies but here we can use it for generating a key [1, 2].

The middle-square-method was one of the first methods (John von Neumann, 1946) used to generate pseudo random numbers. Here a seed value is taken and then it is squared. After getting the square value the middle numbers are taken and new seed is generated. This process can be repeated any number of time. Once the key is generated then we can use the key to change the order of the frames. Once order is changed the frames are stitched together to form the new encrypted video. This same random key and shuffling algorithm is applied at the decryption side [8].



E. Decryption

The final stage process is decrypting the video. After decrypting the video, the one who desires to receive a video can understand the actual content of video. The encrypted video is retrieved and with the help of decrypted key restitching

can be done to form the even and odd list. That is, as in encryption process splits into two halves namely even and odd lists. Then only even list is considered and decrypted. Then video stitched back and thus we get the original video.

In the process of decrypting the encrypted video, the decryption block will decode the random key which is encrypted using AES [2]. Use the key to reshuffle the frames to its original position. Since the random key is encrypted, we can ensure that the video is secure because the selected random key is known only to the sender and receiver. When we use this random key we can assure the security. The frame stitching block stitch the even and odd list. In order to say a complete video transferring has occurred both encryption and decryption have to be done.

F. Tools and Languages

We are using MATLAB as our project tool. Because MATLAB is a tool that can be used for a better image processing. Since our project is video encryption and image processing is necessary so it is a better option to select MATLAB as a tool.

MATLAB stands for matrix laboratory. It is a high-level language for technical computation, visualization and programming in an easy way to use environment. The main advantage of MATLAB is that use of wealth in built functions. Each module in MATLAB uses tool boxes. Using toolboxes we can develop applications. MATLAB supports automatic storage allocation and also has high computation speed. MATLAB uses IDE (integrated development environment). MATLAB is written in C and FORTRAN languages. They are referred as cousins of MATLAB.

Now consider the MATLAB windows, such as command window, editor window and figure window. Output is displayed on command window. We create the programs at editor window. The MATLAB Application Program Interface (API) is a library that allows you to write C and FORTRAN programs that interact with MATLAB. It include facilities for calling routines from MATLAB (dynamic linking), calling MATLAB as a computational engine, and for reading and writing MAT-files. Everything in MATLAB is a matrix.

MATLAB is an interpreted language, no compilation needed (but possible) MATLAB does not need any variable declarations, no dimension statements, has no packaging, no storage allocation, no pointers Programs can be run step by step, with full access to all variables, functions etc.[7].

Common Uses for Mat lab is in research are data acquisition multi-platform, multiform at data importing analysis tools (existing, custom), statistics, graphing, modelling etc. The features of multi-platform, multi format data importing are data can be loaded into Mat lab from almost any format and platform, Binary data files (egg. REX, PLEXON etc.), ASCII Text (egg. Eyewink I, II) Analogy/Digital Data files. Analysis tool provides a framework for the design, creation, and implementation of any custom analysis tool imaginable.

IV. CONCLUSION

Transferring a video securely is an immersive task. As the technology is progressing the scope of performing attacks for intruders are also great. This is the greatest challenge which we face throughout our project implementation. Shuffling the video using suitable algorithm shaved one successfully. In later, decryption process and AES is need to be completed. Encryption algorithm focusing on various requirements, which include security, computational efficiency, compression efficiency and format compliance.

Here we are using a random key generation algorithm called midsquare.Midsquare generated random keys by taking a seed value as input. Since there is possibility for generating zero as output, so we modified the algorithm midsquare in an effective manner.AES is one of the strongest algorithm used for encryption. It is the core part of our project. AES, code word extraction and the decryption part will be implemented in upcoming days. So far the shuffling algorithm, frame classification and the random key generation is implemented successfully.

REFERENCES

[1] Ajay Kulkarni, Sarah Kulkarni, Kati Harridans and Anika More, Proposed Video Encryption Algorithm v/s Other Existing Algorithms: A Comparative Studyl, International Journal of Computer Applications (0975 - 8887) Volume 65No.1, March 2013

[2] William stallings,"Cryptography and Network Security", Pearson 5th edition 1999

[3] Narsimha Raju C, UmaDevi Ganugula, Kannan Srinathan, C. V. Jawahar, A novel video encryption technique based onsecret sharing International Institute of Information Technology- Hyderabad, India 2013

[4] Jayshri Nehete, K. Bhagyalakshmi, M. B. Manjunath, Shashikant Chaudhari, T. R. Ramamohan,A Real-time MPEG Video Encryption Algorithm using AES Central Research Laboratory Bharat Electronics Ltd., Bangalore-560013,2011

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

[6] JollyshahandDr.VikasSaxena, VideoEncryption: ASurvey, IJCSIInternational Journal of Computer Science Issues, Vol. 8, Issue 2, March 2011

[7] Ilya Mikhelson MATLAB Function Tutorial.https://www.youtube.com /watch? v=PiAl0L1rXKA Oct 12, 2013.

[8] Hamed Rahimov, Majid Babaie, Hassan Hassanabadi,"Improving Middle Square Method RNG Using Chaotic Map"International Journal of applied mathematics, April 2011

[9] Chandra Kurnia wan "Convert Video to Frames with Matlab" http://www.youtube.com/watch?v=hk7BLPHpHUs,nov 27 2011

[10] Arindam Bose "Video Cutter Program in MATLAB" http://arindambose.com/blog/?p=49,august 15 2013

