An Analysis of Performace of Conatiner Video Encryptions

*Dinesh Goyal, *Shivam Sharma, **Dr. Naveen Hemrajani
*Suresh Gyan Vihar University, Jaipur
**JECRC University, Jaipur

Abstract – The video containers are the basic formats of video, developed to satisfy the requirements of different applications for various purposes, better picture quality, and more error robustness. AVI, MOV, MTS, DAT are some of such formats. In this paper, the various video encryption techniques are attempted on AVI, DAT & MTS formats and their performance is analyzed by encrypting them using chaotic map selective encryption. The parameter of analysis is size of video before and after encryption and time taken to encrypt the video file.

Keywords- AVI, DAT, MTS, video encryption, Chaotic MAP

I. INTRODUCTION

Multimedia is the combination of two or more media. The media in multimedia is in various forms such as graphics, photography, text, audio, video and animation. Each one serves as a powerful communication vehicle for both expressive and practical purposes.

Multimedia is usually recorded and played, displayed or accessed information content processing devices, such as computers and electronic devices, but can also be part of a live performance.
There are six basic multimedia elements, including video, audio, photography, animation, text and graphics. In the use of multimedia elements are present. Multimedia is powerful tool which is a combination of these elements.[2]

II. DIGITAL VIDEO

Digital Video is in binary format of video and audio. It is a digital sequence of data, rather than in a continuous signal.

In the nature of the information received through the five senses, is in analog form. This means that it is having infinitely variables. Digital A / V information, on the other hand, is having discrete units of data so that the human senses perceive them in a continuous stream to be placed. Analog data, as recorded on the video tape, transmitted as electron signal and added to a given carrier frequency of the different frequency or amplitude. In order to make this information, you can use a computer or a modern media player, analog Digital conversion of the analog signal is done in form of a series of 0 and 1, respectively, "negative" and "positive", "close" and ", "or" low "and" high.

III. VIDEO FORMATS

3.1 Containers and codec

Digital video format that may be relevant most confusing thing is that there's a "container" and "Decoder" idea - you might think it is enough to make your longing for the days when you could just the tape in the camera to start recording. Today, many, many more options exist and people are taking advantage of all of them - from high-end HD video display on the top line of home theater with surround sound, video streaming from your mobile phone - video everywhere, there are a variety of formats to grasp will ensure that your video to get where it needs the best way.

3.2 Container

We take a look at some of the container, and then in some codec. Video file extension usually refers to the container. Several containers, they almost always use the codecs and other containers tend to use many different codecs.

a. **Audio Video Interleave (AVI):** Developed and released by Microsoft with Windows 3.1. AVI digital video files have been a work. Despite its popularity has gradually subsided, left a lot of AVI video can be found all over the web. Recently, AVI has abandoned Microsoft's WMV (Windows Media Video).
b. **Advanced Systems Format (ASF)**: ASF is a proprietary Microsoft containers typically include file compression with Microsoft WMV codec – make things confusing, usually specified files, WMV, and ASF. ASF container has the advantage of many other formats, which can include a DRM (Digital Rights Management), a form of copy protection.
c. **The QuickTime (MOV or QT)**: QuickTime, which is developed by Apple, and supports a variety of codecs. Although this is a proprietary format and Apple decided to support it.
d. Advanced Video Coding, high definition (AVCHD): AVCHD is a very popular container H.264 data compression – it involves cooperation between Sony and Panasonic as a digital video camera format. This is a file-based format, it means a disk or other storage device storage and playback. It supports standard definition and high definition different from 720-1080.

e. Flash Video (FLV, SWF): Flash was originally developed by a company called Macromedia, which was acquired by Adobe in 2005. Flash has been around for some time, and there are several versions and some are better than others. Older Flash videos often use the Sorenson codec. This is an extremely wide range of containers for the entire network video streaming format. Its main drawback is that it will not play on iOS devices, such as an iPad or iPhone.

IV. VIDEO ENCRYPTION TECHNIQUES

In today's scenario there is an increasing demand for remote video communication. The development of encryption systems main objective is to provide a secure and reliable way of information exchanges. However, the security aspects of video exchanges have yet to be fully addressed. Existing video coding standards do not incorporate requirements to have encryption capabilities.

Recently, researchers are focusing a lot of attention on secure digital media over the network. The field of multimedia security is growing extremely fast. In order to deal with the problem of processing overhead and to meet the security requirements of real -time video applications with high quality video compression, several encryption algorithms to secure video streaming have been proposed which are as follows:

- Pure permutation algorithm which simply scrambles the bytes within a frame of an MPEG stream by permutation. It is extremely useful in situations where the hardware decodes the video, but decryption must be done by the software.
- Zig-Zag permutation approach maps the individual 8x8 block to a 1x64 vector using a random permutation instead of mapping 8x8 blocks to a 1x64 vector in a Zig-Zag order using a random permutation list (secret key).
- Video encryption algorithm: Bhargava, Shi, and Wang in 1996 and 1998 introduced four different video encryption algorithms : Algorithm I, Algorithm II (VEA); Algorithm III (MVEA); and Algorithm IV (RVEA).

The Joint Video Team (JVT) finalized the draft of the new coding standard for formal approval submission as H.264/AVC and was approved by ITU-T in March 2003. Researchers started work to make the H.264/AVC bit stream secure. Most of them tried to optimize the encryption process with respect to the encryption speed, and the display process.

V. EXPERIMENTAL SETUP

MATLAB is a numerical computing environment and programming language. Created by The Math Works, MATLAB allows easy matrix manipulation, plotting of functions and data, implementation of algorithms, creation of user interfaces, and interfacing with programs in other languages. Although it specializes in numerical computing, an optional toolbox interfaces with the Maple symbolic engine, making it a full computer algebra system. It is used by more than one million people in industry and academia and runs on most modern operating systems, including Windows, Mac OS, Linux and Unix.

MATLAB is used in every facet of computational mathematics. Following are some commonly used mathematical calculations where it is used most commonly:

- Dealing with Matrices and Arrays
- 2-D and 3-D Plotting and graphics
- Linear Algebra
- Algebraic Equations
- Non-linear Functions
- Statistics
- Data Analysis
- Calculus and Differential Equations
- Numerical Calculations
- Integration
- Transforms
- Curve Fitting
- Various other special functions

Some of the basic features of MATLAB are as follows:

- It is a high-level language for numerical computation, visualization and application development.
- It also provides an interactive environment for iterative exploration, design and problem solving.
- It provides vast library of mathematical functions for linear algebra, statistics, Fourier analysis, filtering, optimization, numerical integration and solving ordinary differential equations.
- It provides built-in graphics for visualizing data and tools for creating custom plots.
- MATLAB's programming interface gives development tools for improving code

quality and maintainability and maximizing performance.
- It provides tools for building applications with custom graphical interfaces.
- It provides functions for integrating MATLAB based algorithms with external applications and languages such as C, Java, .NET and Microsoft Excel.

MATLAB is widely used as a computational tool in science and engineering encompassing the fields of physics, chemistry, math and all engineering streams. It is used in a range of applications including:
- Signal Processing and Communications
- Image and Video Processing
- Control Systems
- Test and Measurement
- Computational Finance
- Computational Biology

Now, Image processing toolbox in MATLAB provides a comprehensive set of reference-standard algorithms, functions, and apps for image processing, analysis, visualization, and algorithm development. You can perform image enhancement, image deblurring, feature detection, noise reduction, image segmentation, geometric transformations, and image registration. Many toolbox functions are multithreaded to take advantage of multicore and multiprocessor computers.

Image Processing Toolbox supports a diverse set of image types, including high dynamic range, gigapixel resolution, embedded ICC profile, and tomographic. Visualization functions let you explore an image, examine a region of pixels, adjust the contrast, create contours or histograms, and manipulate regions of interest (ROIs). With toolbox algorithms you can restore degraded images, detect and measure features, analyze shapes and textures, and adjust color balance.

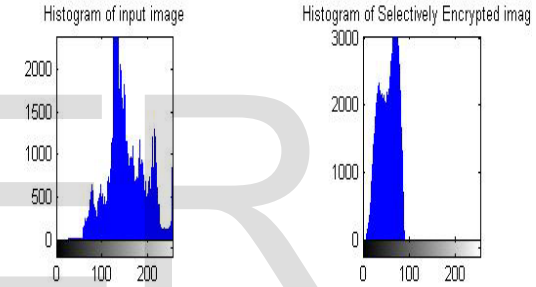
MATLAB also provides the functionality of basic video processing using short video clips and a limited number of video formats. The only video container supported by built-in MATLAB functions was the AVI container, through functions such as aviread, avifile, movie2avi, and aviinfo. Here, aviread is used to read an AVI movie and store the frames into a MATLAB movie structure whereas aviinfo returns a structure whose fields contain information about the AVI file passed as a parameter. Also, mmreader used to constructs a multimedia reader object that can read video data from a variety of multimedia file formats.

Processing of video files consists of the following steps:
1. Convert frame to an image using frame2im.
2. Process the image using any technique.
3. Convert the result back into a frame using im2frame.

The MATLAB functions associated with writing video files are as follows:
- avifile: creates a new AVI file that can then be populated with video frames in a variety of ways.
- movie2avi: creates an AVI file from a MATLAB movie.

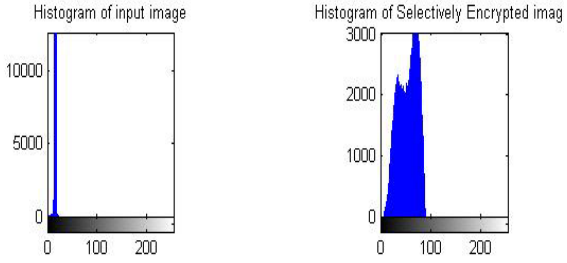
In this experiment comparative analysis of Selective encryption is performed on AVI, DAT & MTS video using MATLAB.

Scenario 1, Here Selective Encryption is performed on 10 frames of an AVI Video format of size 89 KB



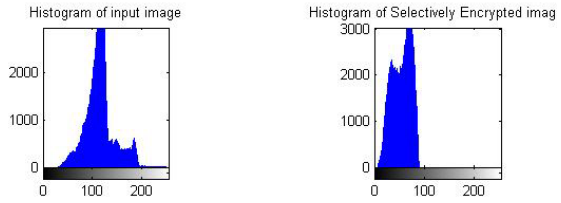
Picture 1. Histogram Results of Selective Encryption of AVI Video

Scenario 2, Here Selective Encryption is performed on 10 frames of an DAT Video format of size 51 KB



Picture 2. Histograms Results of Selective Encryption of DAT Video

Scenario 3, Here Selective Encryption is performed on 10 frames of an DAT Video format of size 3509 KB



Picture 3. Histograms Results of Selective Encryption of MTS Video

VI. RESULT ANALYSIS

In this the results of three types of the video formats are encrypted using selective encryption technique and compared with their respective results.

The results shown in previous chapter are taken after performing chaotic map based selective encryption on monochrome video.

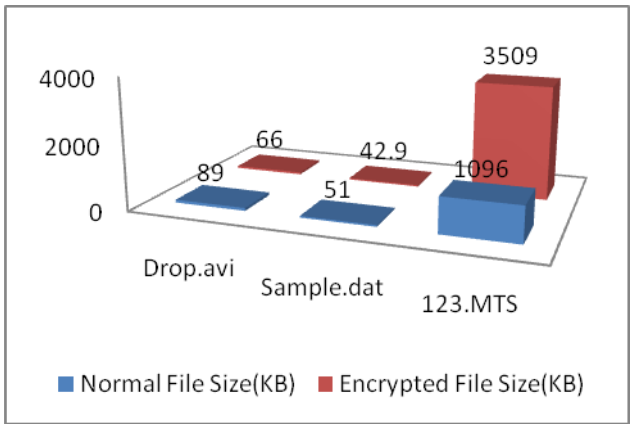
1. In this work in AVI format the normal input video is encrypted using pre-defined chaotic map based selective encryption (symmetric key).
2. In case of DAT format i.e. during encoding we have encrypted video by implementing chaotic map based encryption.
3. For AVCHD video the encryption is performed on using chaotic based video encryption.

The comparison between the results of three video encryptions is as follows:

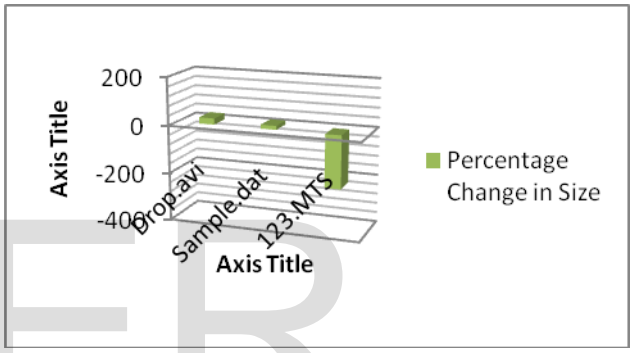
	AVI Format	DAT Format	AVCHD Format
Name of File	Drop.avi	Sample.dat	123.MTS
No. of Frames	10	10	10
Normal File Size(KB)	89	51	1096
Encrypted File Size(KB)	66	42.9	3509
Encryption time	26.009	26.225	30.27

Table 1. Comparison Table of Selective, Layered and Naïve

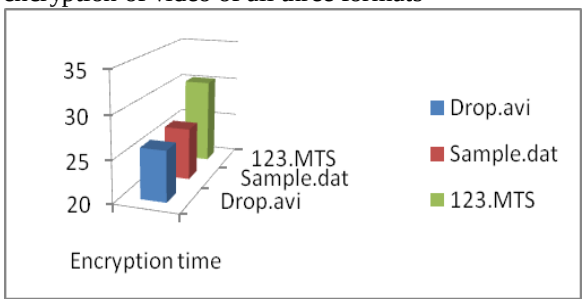
In figure 1, we have compared the size of encrypted video and normal video of all three formats



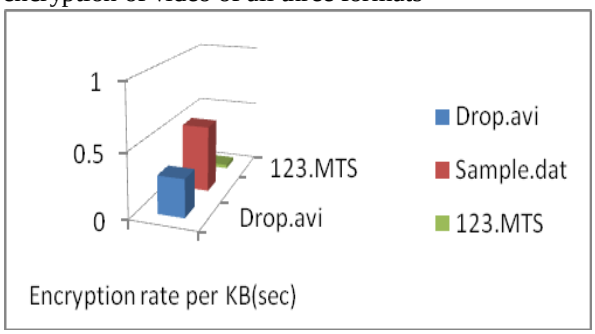
In figure 2, we have compared the percentage change in size of encrypted video with respect to normal video of all three formats



In figure 3, we have compared the time taken for encryption of video of all three formats



In figure 4, we have compared the encryption rate for encryption of video of all three formats



VII. CONCLUSION AND FUTURE WORK

Conclusion

In this work We take a look at some of the container, and then in some codec. Video file extension usually refers to the container. Several containers , they are almost always tend to use a number of different codecs codecs and other container.

The AVI format, DAT format and AVCHD format are container video formats which are encrypted using chaotic map video encryption technique and results are taken depending upon these analyses, using MATLAB Image and Video Processing Tool.

Analysis of results prove the following points :

1. Encryption of AVCHD increases its size while encryption of other two decreases their size.
2. Encryption rate is least in AVCHD i.e. time taken to encrypt the AVCHD is least in terms of KB
3. Encryption time for AVCHD is most in terms of frames(10 each).
4. AVI video is reduced to 75% during encryption this can save lot of time for transmission

Future Work

In future this work can further be extended to codec and container codecs too.

These formats can also be analyzed for block based and other video encryption techniques.

New encryption techniques may be devised for reducing the size and encryption rate for the purpose of streaming applications.

VIII. REFERENCES

1. Su- Wan park, Sang-Uk shin. " Efficient Selective Encryption Scheme for the H.264/Scalable Video Coding(SVC)" , Fourth International Conference on Networked Computing and Advanced Information Management, Volume 01, pp 371-376 , 2008.
2. Iain Richardson, "An Overview of H.264 Advanced video coding". 2007 white paper. http://www.vcodex.com/files/H.264_overview.pdf (retrieved March 02, 2009).
3. Yuanzhi Zou, Tiejun Huang, Wen Gao, Longshe Huo. Nov, "H.264 video encryption scheme adaptive to DRM". IEEE Transactions on Consumer Electronics, pp. 1289 – 1297, 2006.
4. Lian, S., Liu, Z., Ren, Z., and Wang, Z., "Selective Video Encryption Based on Advanced Video Coding," Lecture Notes in Computer Science, Springer-Verlag 3768, 281–290 (2005).
5. Z. Shahid, M. Chaumont, W. Puech,"Fast Protection of H.264/AVC by Selective Encryption of CAVLC and CABAC for I & P frames", Journal of IEEE transactions on circuits and systems for video technology.
6. A A Muhit, M R Pickering, M R Frater and J F Arnold, "Video Coding using Elastic Motion Model and Larger Blocks," IEEE Trans. Circ. And Syst. for Video Technology, vol. 20, no. 5, pp. 661-672, 2010.
7. A A Muhit, M R Pickering, M R Frater and J F Arnold, "Video Coding using Geometry Partitioning and an Elastic Motion Model," accepted for publication in Journal of Visual Communication and Image Representation.
8. S. Lian, J. Sun, G. Liu and Z. Wang, "Efficient video encryption scheme based on advanced video coding," Multimedia Tools Appl, Vo138, No.1, pp.7S-89, May. 2008.
9. T.Wieg. Draft ITU-T Recommendation H.264 and Draft ISO/IEC 14496-10 AVC. Joint Video Team of ISO/IEC JTC 1/SC29IWG 11 & ITU-T SG16/Q6 Doc.JVT -GO5O, 2003.
10. J Ahn, H. 1. Shim, B. Jeon and I. Choi, "Digital Video Scrambling Method Using Intra Prediction Mode," in Pacific Rim Conf. Multimedia, Tokyo, Japan, pp.386-393, 2004.
11. Lingling Tong, Gang Cao, Jintao Li, "Layered Video Encryption Utilizing Error Propagation in H.264/AVC," in IEEE Symposium on Electrical & Electronics Engineering (EEESYM), 2012.
12. M. Abomhara, Omar Zakaria, Othman O. Khalifa, A.A Zaidan, B.B Zaidan, "Enhancing Selective Encryption for H.264/AVC Using Advanced Encryption Standard," in International Journal of Computer Theory and Engineering, Vol. 2, No. 2 April, 2010.
13. Jay M. Joshi, Upena D. Dalal, "Selective Encryption using ISMACryp in Real Time Video Streaming of H.264/AVC for DVB-H Application," World Academy of Science, Engineering and Technology 55 2011.
14. Rajinder Kaur, Er. Kanwalpreet Singh, "Comparative Analysis and Implementation of Image Encryption Algorithms," International Journal of Computer Science and Mobile Computing (IJCSMC), Vol. 2, Issue 4, April 2013, Pg.170-176.
15. Ibrahim S. I. Abuhaiba, Hanan M. Abuthraya, Huda B. Hubboub, Ruba A. Salamah, "Image Encryption Using Chaotic Map and Block Chaining," International Journal of Computer Network and Information Security, July, 2012, Pg. 19-26.