PROFILE CONCEALING IN VIDEOS USING SELECTIVE ENCRYPTION AND GPGPU

Rucha Sahakari[1], Shubhada S. Kulkarni[2]

[1] PG research scholar,KLS's Gogte Institute of Technology, Belgavi, India
[2]Asst. Professor , Dept. of Computer Science, KLS's Gogte Institute of Technology, Belgavi, India

---***---

Abstract - *Today, communication through internet is common. Large amount of data is exchanged through internet which is secured using cryptographic techniques. Various algorithms are available to secure the content from attacks like, modification of message, release of message content etc. Security and privacy of data sent through internet is important. Video services are gaining importance these days because of large use of applications like video chat, video on demand etc. The important factor which needs to be considered is security of data. New method called Selective Video Encryption is developed which secures video in less time. Too many CPU calculation resources are used if we use full traditional encryption on data stream and it also slows down the process of Encryption. A new solution is to combine selective encryption with current General Purpose Graphic Process Unit (GPGPU) acceleration. This paper is focused on Profile Encryption in videos and improve the performance of encryption with respect to time using GPGPU(General purpose graphic processing unit).This can be applied in News Industry where sometimes victims profile are blurred to keep their identity unknown to viewers.*

***Key Words*: Selective encryption; GPGPU(General Purpose Graphic processing unit); DCT(Discrete cosine transform),Encryption, Decryption**

1. INTRODUCTION

With the broadened stockpiling of information publicly, it turns out to be increasingly essential for everyone to secure their own information like images, texts audios and videos. Traditional encryption frameworks, which are initially created for text, put entire image data stream into a standard figure system (DES, AES). As to security, this sort of encryption framework is not sufficiently quick with restricted count assets environment like a portable workstation or when large amount of data is to be processed. One issue specified in [1] is that all images in the content are of equivalent significance are contended non optimal for securing pictures as they simply overlook the nature of pictures. Video can be secured by using cryptographic techniques. The videos are encoded and decrypted so that they are visible only to receivers.

Today, the correspondence using "multimedia components" is on crest. Information like pictures, audio, text data & video is imparted through network. The data is secured from assailants using cryptographic technique. In the encryption technique, encryption algorithms are used to change data into ciphertext. Data is decrypted back to original using decryption algorithm.

Scientists are accomplishing another way of securing videos, audios and text messages through Selective Encryption(SE).SE method applies encryption on selected part of the content which is important. The fundamental objective of SE strategies is to secure data in less time as well as to decrease amount of data to be encoded.

1.1 CLASSIFICATION OF VIDEO ENCRYPTION ALGORITHM

According to [2] there are four basic categories of Video Encryption Algorithms:

1] Completely Layered Encryption

Here traditional algorithms like AES, DES are used to encrypt compressed video data.

.2] Encryption Using Permutation

In this strategy, video data is mixed utilizing a permutation algorithm. The whole video data might be mixed or just specific bytes. Here, mystery key used for encoding the data is utilize from permutation list.

3] Selective Encryption

In this strategy, specific video data is encrypted to decrease amount of time required for encryption. Computational complexity is lowered by encoding only some part of video stream.

4] Perceptual Encryption

Video will be detectable even after encrypting data using this procedure. Sound quality or video quality can be managed constantly.

1.2 TYPES OF VIDEO ENCRYPTION

Information like videos, text, images is transferred through internet. Securing this data is important issue. For the most part the advanced digital videos are big in size so generally videos are compressed and transferred, for example, MPEG. Following are some Video Encryption algorithms developed for secure video exchange.

1] Naive Algorithm

Naive algorithm deals with MPEG stream like a text data [3]. This algorithm gives the security advantages to entire MPEG stream as each byte is scrambled, and no calculation can break like triple "DES or AES". This algorithm does not give optimal solution for large video files.

2] Pure Permutation

In this permutation method is used which simply scrambles frame of MPEG stream. In [4] permutation algorithm shown is defenceless against known plaintext attack, and thus it ought to be utilized deliberately. If ciphertext is known to assailant with frames, than permutation list can be easily found out. Once permutation list is known ciphertext can be decoded easily to get the original text.

3] Zig zag permutation algorithm

According to[5] with the use of secret key (permutation list in this case) Zig-zag permutaion maps "8x8 block" to "1x64 vector" as substitute for mapping the "8X8 block" to "1X64 vector" in "Zig-Zag" order.

4] Video encryption algorithms

In [6] [7] various algorithms are given like Algorithm I, VEA(Algorithm II), MVEA (Algorithm III) & RVEA(Algorithm IV)

5]Selective Encryption Algorithm

Selective Encryption algorithm selectively encrypts data to provide security to desired data. To increase the speed of encryption Selective Encryption method is the best solution compared to Traditional method. It saves the time required for encryption.

2. RELATED WORK Selective Encryption

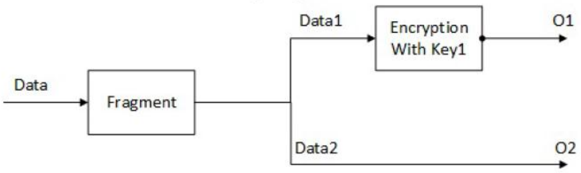

Fig 1.1 Basic Design of Selective Encryption

The general methodology is to isolate the picture content into two sections. The initial segment is planned to be open to public and unencrypted. The second part is private or secured and will be encrypted. The deal is to make the private part as little as could be and to secure the image as per the necessities of a particular situation.

In above figure data is fragmented into two parts Data1(private part) and Data2 (unencrypted part). Data1 is vital part which takes very less storage space and Data2 is unencrypted which takes most of the storage space. One important advantage of this method is that it can make vital part of the encrypted data as small as possible. In cases where transmission rate is low and bandwidth is limited traditional encryption methods fails to give required performance.

This is because in traditional method whole data is encrypted and sent on the network. Whereas in Selective Encryption method only vital part of the data is sent encrypted rest all the data is made public. Thus it is sometimes called as Partial Encryption. Computational requirements are also minimized by using this method.

1.3.2 CUDA and DCT acceleration

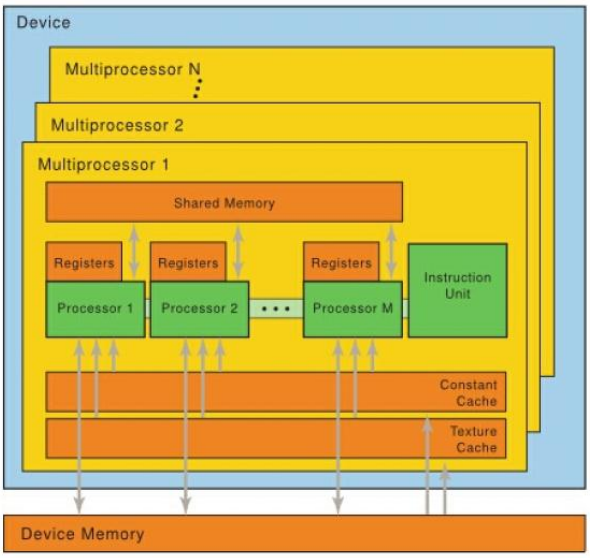

Fig 1.2 CUDA architecture

Fig.1.2 illustrates the CUDA architecture. GPU chip has different multiprocessors (MP) and every MP has M scalar processors (SP), one shared memory, and a few 32-bit registers inside. In general, the chip constitutes a various leveled SIMD (single-direction multiple data) architecture. Cutting control unit, for example, contingent branch segment from a computing unit permits computing unit density to increment. Furthermore, there is steady memory per MP that can have practically same latency as shared memory on account of reserve references to constant memory. In other word, information itself is situated in global memory, yet in the event that cache reference happens the entity is cashed into constant cache.

1.3.3 Single image scenario

In one image scenario [8], the picture will be replicated into GPU memory and divided by GPU utilizing DCT 8×8 calculation. At that point the chose coefficients which are the critical part will be yield to host memory and encrypted utilizing AES by CPU. Rest all the coefficients will be padded with zeros parallel and transformed by IDCT 8×8 algorithm.

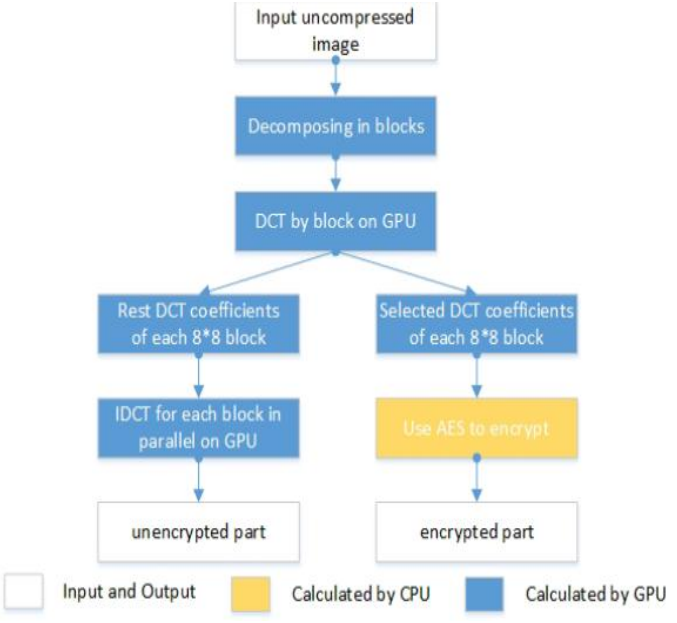

Fig 1.3 Single image processing flowchart

In this plan, the GPU will firstly compute the DCT 8×8 for a input image. After the DCT results are figured, CPU begins to encrypt the chose coefficients with AES. In the meantime, the GPU will figure the IDCT 8×8 for the rest coefficients padded with zero. For this case, the time expended relies on upon a race between CPU and GPU calculation.

3. EVALUATION

Video Encryption-Decryption

Our program works for image encryption and decryption. We evaluate two cases first case in which program runs on CPU and second where GPU is used to accelerate the process.

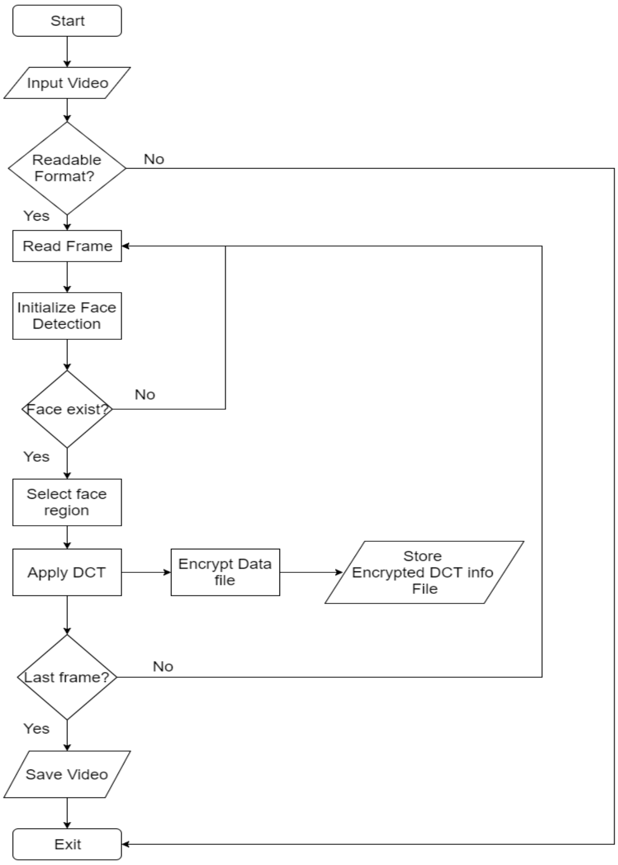

Fig 1.4 Process steps in video encryption

In first case, according to users choice encryption or decryption is carried out. Input video is taken in mpeg format through camera or any other source. Then video to be encrypted is broken down in series of video frames. Now the main task is to detect the faces to be blurred. If any frame doesn't have faces than algorithm skips that frame and moves on to next. Viola Jones face detection algorithm is used here along with Haar classifier. Then the face detected is compressed so as to lower the data rate required to send a video. Algorithm stops with the encounter of last frame. The same steps occur in reverse order for video decryption.

In second case, GPU is used to perform video encryption and video decryption so as to accelerate the rate at which video is compressed.

4. RESULTS

The results are carried out on different videos in mp4 format. For comparing the result video of length 00.36 sec was taken. Results are compared with respect to a video with different resolutions and calculating frames processed per second. The results for study are evaluated using PC with Intel i5 and 4GB RAM. The methods are released using openCV and Microsoft Visual Studio 2010.

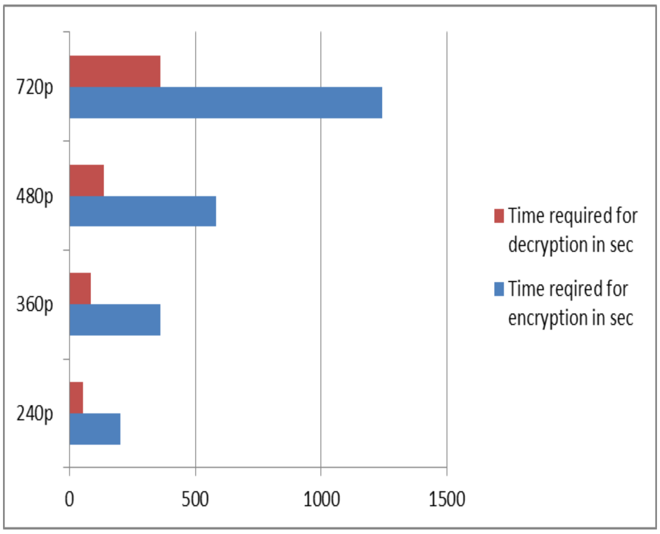

Fig 1.5 Encryption- Decryption results (CPU)

It can be clearly seen that decryption time required is less as compared to Encryption time. The analysis shows that as video quality increases the time required for Encryption as well as Decryption increases accordingly.

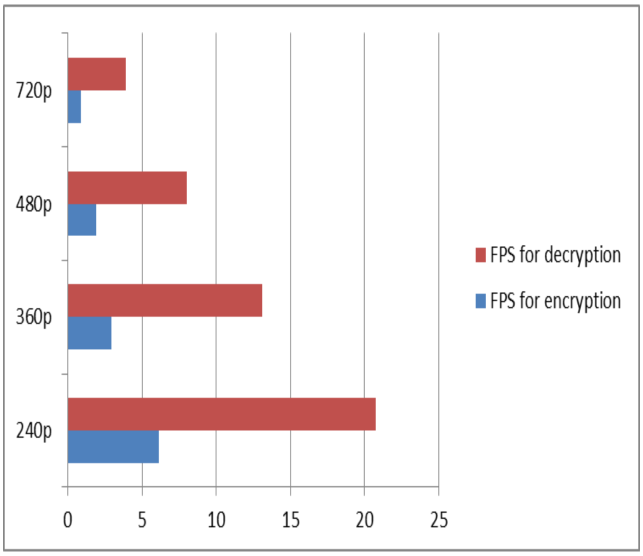

Fig 1.6 FPS (Frames per second) using CPU

It can be clearly seen that Frames processed per second goes on decreasing with higher video resolution and vice versa for decryption. This process is carried out using CPU.

Same test cases are carried out by using GPU (NVIDIA GEFORCE). The results for Encryption-Decryption time are

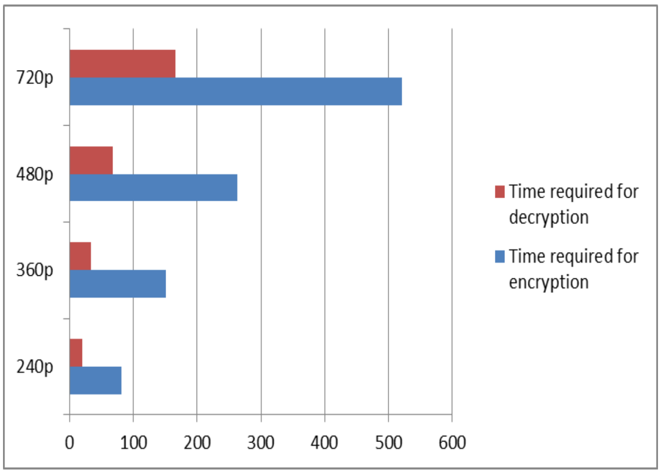

Fig 1.7 Encryption- Decryption results (GPU)

By comparing the results of Encryption-Decryption using CPU and GPU we found out that there is almost above 50% acceleration in processing on GPU.

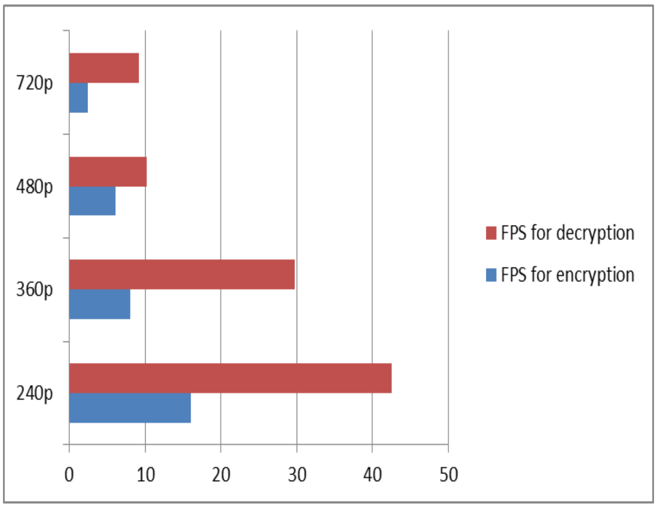

Fig 1.8 FPS (Frames per second) using GPU

In these results also we can see performance improvement compared to the results got using CPU.

5. CONCLUSIONS

The technique proposed here is of Selective Video Encryption which is faster as compared to normal CPU based technique. The technique proposed makes use of GPGPU (General Purpose Graphic Processing Unit) to accelerate the process of Selective video Encryption. Analysis is performed on videos with different resolutions and on Frames processed per second(FPS) . The analysis performed and the results we have got proves that the above method overall accelerates the performance.

In future, performance can be accelerated by using latest GPGPU available. By using adapter to auto-configure multiple CPUs and multiple GPUs much more enhanced results can be found. Different Encryption algorithms can be used to increase the performance.

REFERENCES

[1] S.Baba et al L.Krikor, "Image encryption using dct and stream cipher," *European Journal of Scientific Research*, pp. 47-57, 2009.

[2] Shiguo lian, "Multimedia Content Encryption: Algorithms and Application," *CRC Press*, 2008.

[3] Adam J. Slagell, "Known-Plaintext Attack Against a Permutation Based VideoEncryption Algorithm," *IACR internatioanl Journal*, 2013.

[4] L.Tang, "For Encrypting and Decrypting MPEG Video Data Efficiently," in *Fourth ACM International Multimedia Conference*, 1996, pp. 219-230.

[5] B. Bhargava C.Shi, "For Encrypting and Decrypting MPEG Video Data Efficiently," in *6th International Multimedia Conference*, Bristol, 1998, pp. 12-16.

[6]Pushpendra Kumar Pateriya Saurabh Sharma, "A Study on Different Approaches of Selective Encryption Technique," *International Journal of Computer Science and Communication network*, pp. 658-662.

[7] Genard MEMMI Han QIU, "Fast selective encryption method for bitmaps based on GPU acceleration," *IEEE International Symposium on Multimedia*, 2014.

[8] K.Bhagyalaxmi, M.B. Munjunath,Shashikant Chaudhari,T.R. Rammohan Jayashri Nehete, "A Real-time MPEG Video Encryption Algorithm using AES," *Central Research Laboratory Bharat Electronics Ltd.*, 2012.

[9] F. Gadegast J. Meyer, "Security Mechanisms for Multimedia Data with the Example MPEG-1 video," Berlin, 1995.

[10] T. B. Maples G.A. Spanos, "Performance Study of a Selective Encryption Scheme for the Security of Networked Real Time Video," in International Conference on Computer Communication and Network, 1995, pp. 2-10.

[11] C.J. Kuo C. P. Wu, "Fast Encryption Methods for Audiovisual Data Confidentiality," in Proceedings of SPIE, 2001, pp. 284-295.

[12] M. Severa, W. Zeng, M.H. Luttrell,W.Jin J. Wen, "A Format-Compliant Configurable Encryption Framework for Access Control of Video," in IEEE Transactions on Circuits and Systems for Video Technology, 2002, pp. 545-557.

[13] S. Lei Zeng, "Efficient Frequency Domain Selective Scrambling of Digital Video," in IEEE Transaction on Multimedia, 2003, pp. 118-129.

[14] Saurabh kulkarni, ketki Haridas,Aniket More Ajay kulkarni, "Proposed Video Encryption Algorithm v/s Other Existing Algorithms: A Comparative Study," International Journal of Computer applications, vol. 65, 2013.

[15] C.Lamy Bergot C. Bergeron, "Compliant Selective Encryption for H. 264/ AVC Video Streams," in Proceedings of 7th IEEE Workshop on Multimedia Signal Processing, 2005, pp. 1-4.