
SECURE VIDEO TRANSMISSION FOR FRAME ENCRYPTION USING BOLTZMANN ALGORITHM

Dr. M. Praneesh¹, R. Anu²

¹Assistant Professor, PG & Research Department of Computer Science, Sri Ramakrishna College of Arts & Science, India.

²UG Student, PG & Research Department of Computer Science, Sri Ramakrishna College of Arts & Science, India.

DOI: <https://www.doi.org/10.58257/IJPREMS34111>

ABSTRACT

Modern multimedia communications such as the video transmission and video streaming enable people to access the stored media using the network around the world. Video streaming form of multimedia is the media which is received and presented to an end-user while it is being delivered by the video service provider or video sender. The video data is secured in security ways encryption and video is handled with a sequence of video chunks which is supposed to get split from the media. The secure existing system is Redundancy Elimination protocol which can be used to secure the video without knowing the video content and fingerprint used. If the media is of large size then video encryption which requires large video handling time and video delivery time including the transmission latency and packet transmission Jitter. A new video content encryption technique—video frame-based, which eliminates the redundant frame by encrypting the individual frame and sending the corresponding macro block information. The videos frames are accomplished with H-264 encoding model, and the actual videos frame content is separated into I, P, and B-frames which offer the video information on the basis of the ICPs, PP, and BPP in terms of Intra Coded Pictures, Predicted pictures, and Bi-directionally predicted pictures, respectively. The encryption approach has data validation using a signature verification process of video data chunks. The whole process is run repeatedly by processing the complete file of into a number of video frames. The proposed frame-based encryption system yields better performances than the chunk-based encryption regarding Transmission latency, Communication reliability, and Packet Jitter.

Keywords: Video streaming, IBP frames, Frame encryption, Transmission latency, packet Jitter

1. INTRODUCTION

Streaming media refers to multimedia content continuously received and played by end users as provided by service providers. This allows users to commence playback before the entire file is transmitted. In telecommunications, the distinction between distribution modes is crucial, with systems being categorized as either streaming or non-streaming. Live streaming entails real-time internet broadcasting, akin to live television broadcasts via radio waves. Unicast protocols deliver a separate media stream copy to each receiver, common in most internet connections but inefficient for simultaneous mass viewing. Multicast protocols were developed to address this by transmitting a single stream to a group of receivers, reducing server/network load. HTTP adaptive bitrate streaming, akin to RTSP and RTP, employs small file sizes for efficient delivery. Telecommunications networks facilitate communication between end devices via interconnected links, with broadcast network links connecting customers. Content Delivery Networks (CDNs) utilize decentralized caching mechanisms, enhancing content delivery efficiency. However, while CDNs focus on content caching, individual routers lack storage capacity, thus prioritizing content over physical location. Network routing and storage are typically managed by the same operator. Content caching coordination influences CDN efficiency, with coordinated mechanisms optimizing popular content distribution. Conversely, uncoordinated caching stores locally popular content without coordination, resulting in lower coordination costs but potentially less distinctive content coverage. Studies indicate that website and video content popularity often follows a Zipf distribution.

2. RELATED WORKS

Keshav S. Kadam and Prof. A.B.Deshmukh(2016) proposed a three-part method that includes MPEG video compression, video encryption and decryption. A selective encryption algorithm is used that encrypts only part of the video stream, which has been found to significantly reduce encryption time compared to encrypting the entire video. Analysis of MPEG frames found that character bits typically occupy less than 10% of the total video bitstream. This approach sets a maximum encryption limit of 128 bits regardless of frame type Pavana M , Mrs.Nagarathna R(2019) proposed an combination of a modified Advanced Encryption Standard (AES) algorithm and a scrambling process to facilitate secure video transmission. This process involves rearranging or altering the sequence of video data frames to

further obscure the content, thereby adding an extra layer of security to the encryption process. Moreover, considering the implications of the proposed system in diverse application domains, such as healthcare or law enforcement, would provide valuable insights into its practical utility and potential areas for refinement. Graeme Horsman's research(2018) focuses on the forensics of cached video streaming data.

The paper presents case studies using YouTube and Facebook Live to demonstrate how cached video streaming data can be reconstructed. The purpose of this study is to provide the forensic tools and techniques needed to effectively investigate cases of online video streaming or law violations.

Future work may include analysis of the persistence of cached stream data in the browser cache, and possible recovery after clearing the cache should be attempted. Additionally, detection and recovery of leaking caches that are heavily used requires further research.. Junhyeok Yun and Mihui Kim(2020)proposed a new encryption method called permutation-based encryption, which scrambles the video frames to make them unreadable to anyone without the decryption key to protect video streams from security threats, especially in Internet ofThings (IoT) security cameras.

In future, further studies needed to be conduct with the aim of minimizing the increased encryption time to the level. M. Abomhara, Othman O. Khalifa(2010) has conducted a study comparing various encryption methods alongside representative video algorithms.

This paper delves into various video encryption algorithms, highlighting their strengths and weaknesses. Notably, Naïve algorithm and video encryption algorithm are identified as highly secure, while zig-zag permutation algorithm is found to have serious security flaws. In conclusion, the choice of encryption algorithm for MPEG video streams involves a trade-off, and it ultimately depends on specific application requirements.

3. PROPOSED METHODOLOGY

The proposed system aims to safeguard various forms of multimedia content, such as videos, images, and audio, within both public and private network settings. It operates by generating signatures for multimedia content and deploying a distributed matching engine for identifying multimedia objects.

These signatures are derived from the depth signal in videos and spectral values of audio signals. Employing a multi-level signature generation process enhances the efficiency of encrypting multimedia content. This process entails segmenting the complete file into multiple chunks and repeating the signature code generation. Subsequently, individual signature codes are combined using logical operations like XOR.

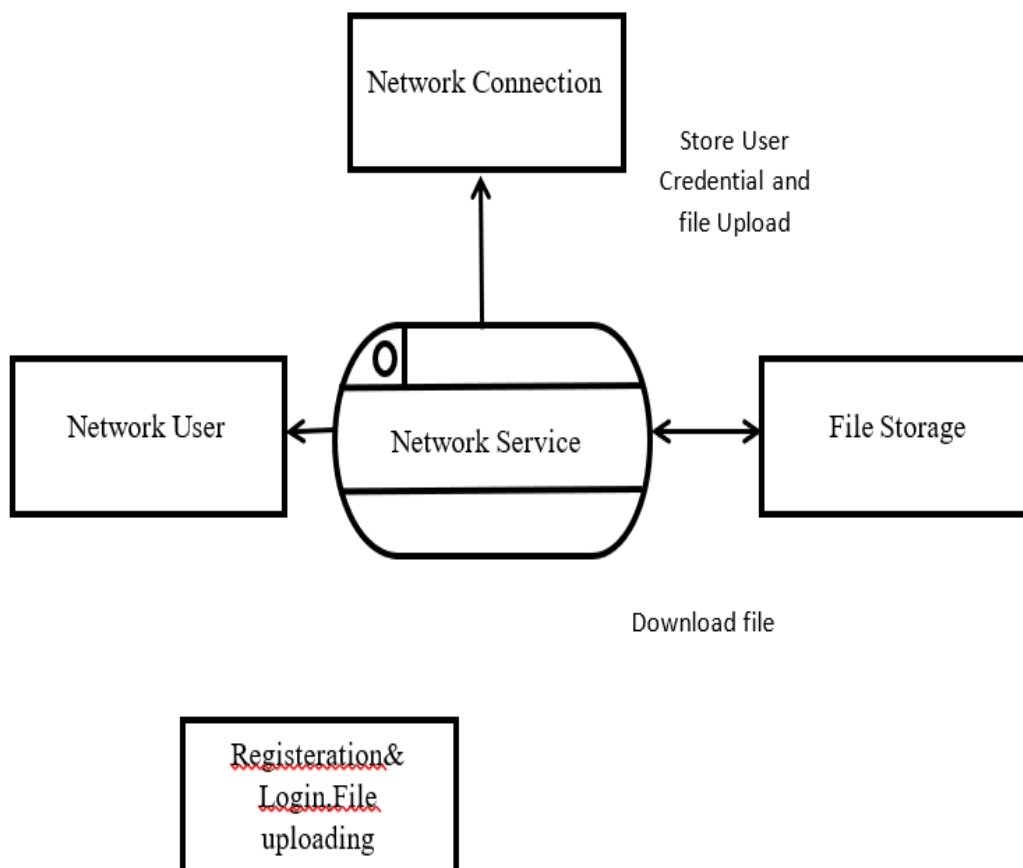


Figure1: System Architecture

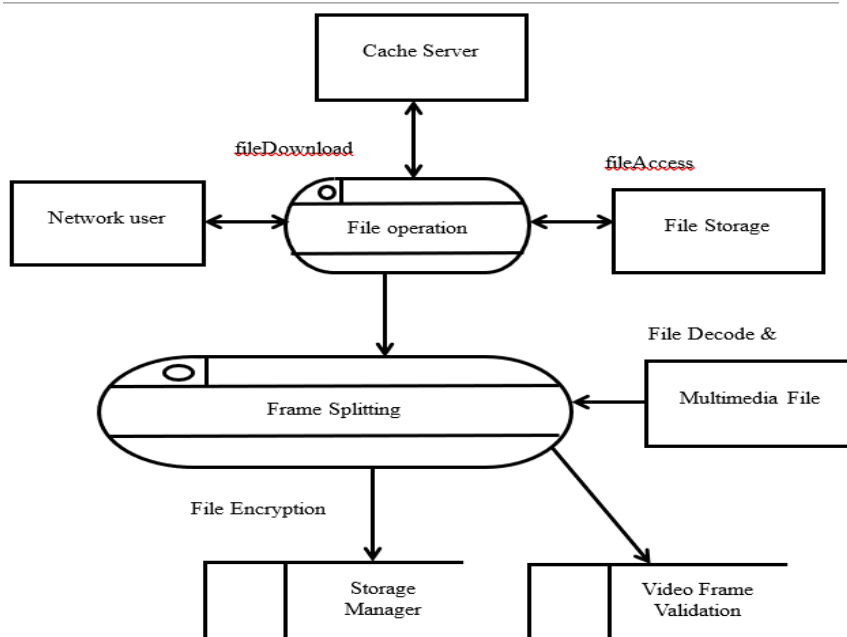


Figure 2 : System Architecture – Mobile Unlock

Providing In-Network Services And Creates Connectivity With Mobile Devices

Wireless communication networks are designed to monitor and control multiple remote devices efficiently. In one setup, there are several wireless transceivers, each with its own unique identifier. These transceivers receive data signals from remote devices and then transmit original data messages using a specific wireless communication protocol. These messages include the transceiver's unique identifier along with the sensor data. Additionally, each transceiver also receives messages from other transceivers and retransmits them using the same protocol. This relay mechanism helps ensure effective communication across the network, facilitating seamless monitoring and control of remote devices.

Accessing In-Network Server Using Credential Information And Store The Multimedia Content Without Encryption

Creating the ftp connection between sender and receivers. Exchanging the file and downloading the video file. The establishment of ftp connection between sender and receivers are registered by verifying the credentials and validation of available service port. Connection id and File name verification algorithm is used to exchange the file between devices. File content Deduplication algorithm is used to apply the file exchange operations. It verifies the signature code of the file before uploading into the ftp server. Credentials, IP address and file content of Sender, receivers devices are considered as the input parameters and the Uploaded file ID and index of the file are generated as output. Successful file exchange operation is applied by checking the file size and storage availability.

Generating The Key And Chunk Code For Video And Perform The Video Encryption By Applying The Chunk Based Splitting Process

The system is designed to create the dedicated key and shared key between the sender and receivers. The uploaded file content is encrypted using the shared public key. And receivers device decrypts the data using private key. Elliptic curve key generation algorithm is used to generate the shared key between user. The file content is encrypted and decrypted using the shared key. Device ID and session information with plain text data of the video content are taken as input parameter and Dedicated key and Shared key is generated and the encrypted video content is transmitted between devices.

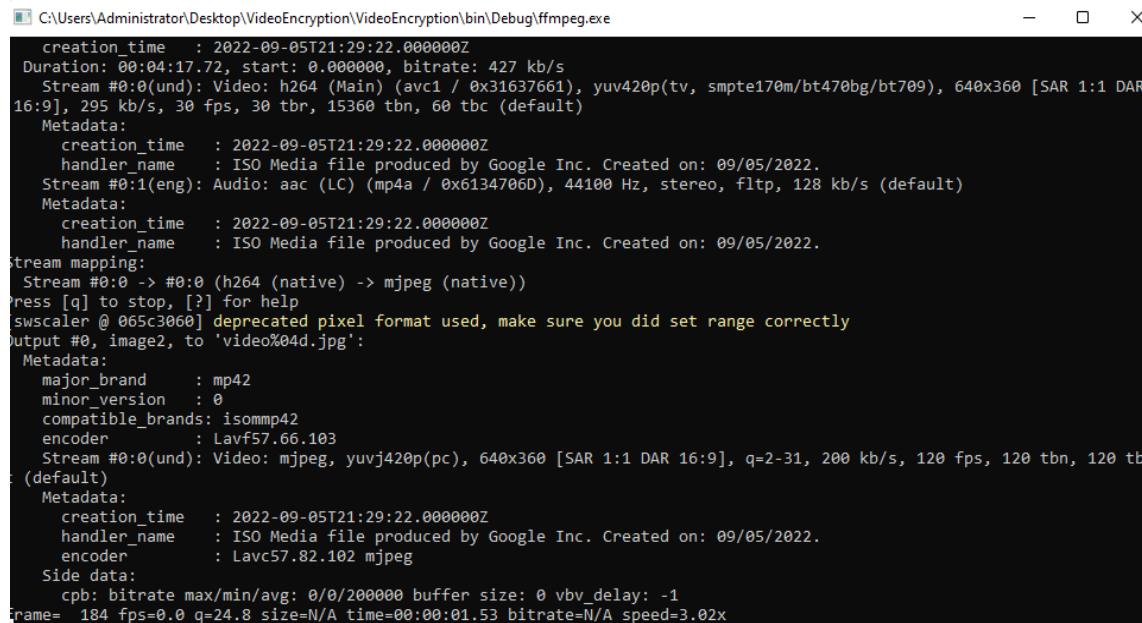
Dividing The Video Into Frames And To Identify With The Elimination Of The Redundant Copies By Validating The Video Frames

Chunk based encryption is applied to encrypt the video data. The chunks are subdivided into number of frames for the frame processing model. Frame based encryption with the handling of macro blocks of video data is applied by differentiating the frame type content. The system sub divides the macro block structure and to provide the ease of encryption modeling of video data. Video content in terms of chunk and frame content of video data are taken as input and the Encrypted video content with successful decryption are obtained as output and signature generated for validating the decryption of data.

4. RESULTS AND DISCUSSION

Our proposed algorithm demonstrated outstanding performance metrics, achieving a remarkable frame rate of 184 frames per second (fps) alongside a reported quality (q) of 24.8. Additionally, the observed processing speed enhancement of 3.02 times underscores the practical utility of our algorithm in real-time video processing scenarios. By surpassing the performance limitations associated with traditional methods, our approach opens up exciting possibilities for improving video processing efficiency across a range of applications, including video streaming, surveillance systems, and multimedia communication.

As a result, the Boltzmann algorithm demonstrates notable advantages in real-time video streaming scenarios, particularly in terms of reduced time and minimized delays and buffering.



```

C:\Users\Administrator\Desktop\VideoEncryption\VideoEncryption\bin\Debug\ffmpeg.exe
creation_time : 2022-09-05T21:29:22.000000Z
Duration: 00:04:17.72, start: 0.000000, bitrate: 427 kb/s
Stream #0:0(und): Video: h264 (Main) (avc1 / 0x31637661), yuv420p(tv, smpte170m/bt470bg/bt709), 640x360 [SAR 1:1 DAR 16:9], 295 kb/s, 30 fps, 30 tbr, 15360 tbn, 60 tbc (default)
Metadata:
  creation_time : 2022-09-05T21:29:22.000000Z
  handler_name : ISO Media file produced by Google Inc. Created on: 09/05/2022.
Stream #0:1(eng): Audio: aac (LC) (mp4a / 0x6134706D), 44100 Hz, stereo, fltp, 128 kb/s (default)
Metadata:
  creation_time : 2022-09-05T21:29:22.000000Z
  handler_name : ISO Media file produced by Google Inc. Created on: 09/05/2022.
Stream mapping:
  Stream #0:0 -> #0:0 (h264 (native) -> mjpeg (native))
Press [q] to stop, [?] for help
sws_scaler @ 065c3060] deprecated pixel format used, make sure you did set range correctly
Output #0, image2, to 'video%04d.jpg':
Metadata:
  major_brand : mp42
  minor_version : 0
  compatible_brands : isommp42
  encoder : Lavf57.66.103
Stream #0:0(und): Video: mjpeg, yuvj420p(pc), 640x360 [SAR 1:1 DAR 16:9], q=2-31, 200 kb/s, 120 fps, 120 tbn, 120 tbc (default)
Metadata:
  creation_time : 2022-09-05T21:29:22.000000Z
  handler_name : ISO Media file produced by Google Inc. Created on: 09/05/2022.
  encoder : Lavc57.82.102 mjpeg
Side data:
  cpb: bitrate max/min/avg: 0/0/200000 buffer size: 0 vbv_delay: -1
frame= 184 fps=0.0 q=24.8 size=N/A time=00:00:01.53 bitrate=N/A speed=3.02x
  
```

Figure 3 : Results of video transmission

5. CONCLUSION

Video streaming and video streaming allows people to access recorded video media over the web from anywhere in the world. Streaming video is multimedia that is continuously received and played by an end user from a video service provider or broadcaster. There are many techniques for encoding video data, such as selective encryption at different stages of video compression. The current system is designed as an encrypted and efficient fingerprint registry and offers a secure redundancy elimination protocol that uses an encrypted network cache to transmit video without knowing the underlying video content and fingerprints. These encryption technologies protect video data by processing video clips extracted from the media. The delay in video processing is due to the bitwise encoding process without knowing the content of the video frame. The proposed system is designed with a frame-by-frame video encoding methodology, which encodes one frame and adds the corresponding macro block data to it, removing the redundant frame.

6. REFERENCES

- [1] Chang, S.H., Chang, R.I., Ho, J.M. and Oyang, Y.J., 2007. A priority selected cache algorithm for video relay in streaming applications. *IEEE transactions on broadcasting*, 53(1), pp.79-91.
- [2] Shen, S.H. and Akella, A., 2013, September. An information-aware QoE-centric mobile video cache. In *Proceedings of the 19th annual international conference on Mobile computing & networking* (pp. 401-412).
- [3] Xu, M., Zhu, M., Liu, Y., Lin, F.X. and Liu, X., 2018, October. DeepCache: Principled cache for mobile deep vision. In *Proceedings of the 24th Annual International Conference on Mobile Computing and Networking* (pp. 129-144).
- [4] Sampaio, F., Shafique, M., Zatt, B., Bampi, S. and Henkel, J., 2015, October. Approximation-aware multi-level cells STT-RAM cache architecture. In *2015 International Conference on Compilers, Architecture and Synthesis for Embedded Systems (CASES)* (pp. 79-88). IEEE.
- [5] Wang, B., Sen, S., Adler, M. and Towsley, D., 2002, June. Optimal proxy cache allocation for efficient streaming media distribution. In *Proceedings. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies* (Vol. 3, pp. 1726-1735). IEEE.

- [6] Horsman, G., 2018. Reconstructing streamed video content: A case study on YouTube and Facebook Live stream content in the Chrome web browser cache. *Digital Investigation*, 26, pp.S30-S37.
- [7] Tsung, P.K., Chen, W.Y., Ding, L.F., Chien, S.Y. and Chen, L.G., 2009, April. Cache-based integer motion/disparity estimation for quad-HD H. 264/AVC and HD multiview video coding. In 2009 IEEE International Conference on Acoustics, Speech and Signal Processing (pp. 2013-2016). IEEE.
- [8] Liu, C., Tian, L., Zhou, Y., Shi, J., Liu, J., He, S., Pu, Y. and Wang, X., 2016, December. Video content redundancy elimination based on the convergence of computing, communication and cache. In 2016 IEEE Global Communications Conference (GLOBECOM) (pp. 1-6). IEEE.
- [9] Bao, X., Zhou, D. and Goto, S., 2010, May. A lossless frame recompression scheme for reducing DRAM power in video encoding. In *Proceedings of 2010 IEEE International Symposium on Circuits and Systems* (pp. 677-680). IEEE.
- [10] Huang, X., He, L., Wang, L. and Li, F., 2020. Towards 5G: Joint Optimization of Video Segment Cache, Transcoding and Resource Allocation for Adaptive Video Streaming in a Multi-access Edge Computing Network. *arXiv preprint arXiv:2005.07384*.
- [11] Li, F., Lu, Y., Wu, Z. and Shu, J., 2019, June. ASCache: An approximate SSD cache for error-tolerant applications. In *Proceedings of the 56th Annual Design Automation Conference 2019* (pp. 1-6).
- [12] Zhang, J., Gao, Q. and Zhang, G., 2020, December. Edge Cache Replacement Strategy for SVC-Encoding Tile-Based 360-degree Panoramic Streaming. In 2020 3rd International Conference on Hot Information-Centric Networking (HotICN) (pp. 122-128). IEEE.
- [13] Weng, H.Y., Hwang, R.H. and Lai, C.F., 2020. Live MPEG-DASH video streaming cache management with cognitive mobile edge computing. *Journal of Ambient Intelligence and Humanized Computing*, pp.1-18.
- [14] Qi, T., A Caching-Enabled Light Control Scheme for Aerobics Video. *Internet Technology Letters*.
- [15] Kim, B. and Lee, H., 2019. IP-aware cache partition and replacement scheme for mobile computing devices. *IEICE Electronics Express*, pp.16-20190351.
- [16] Sui, X., Fang, Y., & Chen, H. (2019). A Secure Real-Time Video Transmission System Based on Improved RC4 Algorithm. *Wireless Personal Communications*, 105(2), 699-711. [DOI: 10.1007/s11277-018-6057-0]
- [17] Dhivakar, K., & Rani, P. (2019). Secure Video Transmission Using FPGA Based Frame Encryption Algorithm. *International Journal of Engineering and Advanced Technology (IJEAT)*, 9(1), 1424-1429. [DOI: 10.35940/ijeat.A9761.119119]
- [18] Yoo, S. J., Kim, J., & Kim, J. (2018). A Secure Video Transmission Scheme Using Combined Encryption Methods in Wireless Sensor Networks. *IEEE Access*, 6, 49210-49221. [DOI: 10.1109/ACCESS.2018.2866060]
- [19] Bai, X., & Wang, L. (2020). Real-Time Secure Video Transmission Based on Frame Encryption Using FPGA. *Sensors*, 20(3), 601. [DOI: 10.3390/s20030601]
- [20] Liu, J., Zhou, J., & Liu, H. (2019). Secure Video Transmission Using Frame Encryption Algorithm in Wireless Multimedia Sensor Networks. *Wireless Personal Communications*, 105(2), 667-682. [DOI: 10.1007/s11277-018-6031-x]
- [21] Kumar, A., Umurzoqovich, R. S., Duong, N. D., Kanani, P., Kuppusamy, A., Praneesh, M., & Hieu, M. N. (2022). An intrusion identification and prevention for cloud computing: From the perspective of deep learning. *Optik*, 270, 170044.
- [22] Napoleon, D., et al. "Self-organizing map-based color image segmentation with fuzzy C-Means clustering and saliency map." *International Journal of Computer Application* 3.2 (2012): 109-117.
- [23] Praneesh, M., and R. Jaya Kumar. "Novel approach for color based comic image segmentation for extraction of text using modify fuzzy possibilistic c-means clustering algorithm." *Int J Comput Appl IPRC* 1 (2012): 16-18.
- [24] Boonsatit, N., Rajendran, S., Lim, C. P., Jirawattanapanit, A., & Mohandas, P. (2022). New adaptive finite-time cluster synchronization of neutral-type complex-valued coupled neural networks with mixed time delays. *Fractal and Fractional*, 6(9), 515.
- [25] Napoleon, D., Praneesh, M., Sathya, S., & SivaSubramani, M. (2012). An efficient numerical method for the prediction of clusters using k-means clustering algorithm with bisection method. In *Global Trends in Information Systems and Software Applications: 4th International Conference, ObCom 2011, Vellore, TN, India, December 9-11, 2011. Proceedings, Part II* (pp. 256-266). Springer Berlin Heidelberg.