

# International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: [www.ijirset.com](http://www.ijirset.com)

Vol. 7, Issue 5, May 2018

## Optimize Video Encryption for Transmission

Rasika Tupe<sup>1</sup>, D.A.Phalke<sup>2</sup>, Rajshree Rathod<sup>3</sup>, Jyoti Narsale<sup>4</sup>, Priyanka Gaikwad<sup>5</sup>

U.G. Student, Department of Computer Engineering, D.Y.Patil College of Engineering Akurdi, Pune, India<sup>1</sup>

Associate Professor, Department of Computer Engineering, D.Y.Patil College of Engineering Akurdi, Pune, India<sup>2</sup>

U.G. Student, Department of Computer Engineering, D.Y.Patil College of Engineering Akurdi, Pune, India<sup>3</sup>

U.G. Student, Department of Computer Engineering, D.Y.Patil College of Engineering Akurdi, Pune, India<sup>4</sup>

U.G. Student, Department of Computer Engineering, D.Y.Patil College of Engineering Akurdi, Pune, India<sup>5</sup>

**ABSTRACT:** Now a days we have come across a lot of security related issues which result in loss of data. Now a days use of images and videos has also increased on tremendous pace. Thus this has led to develop insecurity and fear in the mind of users, as most of their data is in images and videos which either is transmitted or stored at cloud storage. Hence to improve security and to decrease in bandwidth allocation while transmission of data we are proposing one concept i.e. to decrease the size of the video and to encrypt it with the help of Blowfish encryption algorithm we are trying to get this concept work.

**KEYWORDS:** Video Encryption, Blowfish Algorithm, Encryption, Decryption, DES (Data Encryption Standard), Cryptography.

### I. INTRODUCTION

As we are trending towards technology we are getting developments within our systems in today's condition use of videos is increased along with the use transmission has also increased on greater pace, but while transmission we face some issues like videos getting hacked by hackers, transmission rate bandwidth and data allocation is also affected hence we are proposing one system which would compress as well as encrypt the data and would transmit it this would save both bandwidth and video too. A number of encryption techniques for video are proposed to encrypt the videos and used for obtaining highly secured encrypted videos. So we can use Blowfish algorithm to encrypt and decrypt video. Using Blowfish algorithm we can send encrypted video to other user then this video is decrypted using key. This key is sent to user registered mail id. After getting that key user decrypts that video and downloads video.

### Motivation

The motivation of this system is to,

1. Increasing rate of transmission.
2. Unnecessary utilization of the bandwidth
3. Chances of data getting hacked.

### Objective

Objective of this system is to:-

1. Provide security to the confidential data
2. To ensure the private multimedia messages that is traded over the remote or wired systems.

# International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: [www.ijirset.com](http://www.ijirset.com)

Vol. 7, Issue 5, May 2018

3. Video Encryption is useful in securing recordings utilized as a part of administrations such as video on interest (VOD), Video conferencing learning.
4. For ensuring medicinal recordings which might contain private data of a patient from unapproved access by vindictive clients

## II. LITERATURE SURVEY

- 1) Research of H.264 Video Transmission Encryption Technology Based on Blowfish Algorithm by Renle Huang. The experimental results show that this encryption technology can obtain a good compromise between security and encryption efficiency without reducing the security of the algorithm, so it can satisfy the demands of real-time application.
- 2) An Efficient and Secure Video Encryption Technique for Real Time Systems Pradeepkumar.M ,Kishore.O. An enhanced method for encrypt the videos is proposed by using the Huffman encryption algorithm. Instead of using the text or the images, the video encoding is taken place here.
- 3) BLOWFISH ENCRYPTION ALGORITHM FOR INFORMATION SECURITY by SaikumarManku and K. Vasanth. Blowfish is a symmetric block cipher that can be effectively used for encryption and safeguarding of data. It takes a variable-length key, from 32 bits to 448 bits, making it ideal for securing data. Blowfish was designed in 1993 by Bruce Schneier as a fast, free alternative to existing encryption algorithms.
- 4) Enhancing Blowfish File Encryption Algorithm through Parallel Computing on GPU by TejalMahajan, ShraddhaMasih. This paper demonstrates the way of implementing Blowfish cryptography algorithm on GPU for improving performance. This implementation uses GPGPU and CUDA. CUDA is used as a programming model for implementing on the GPU.
- 5) Calculation of Encryption Algorithm Combination for Video Encryption using Two Layers of AHP by Alvin Mustafa, Hendrawa. The purpose of this paper is to calculate the best combination of encryption method regarding to processing time, performance, security, dynamism of system and impact from error propagation using two layer of AHP. The first AHP is to determine encryption algorithm and the second AHP is to determine modes of operation.

## III. PROPOSED SYSTEM

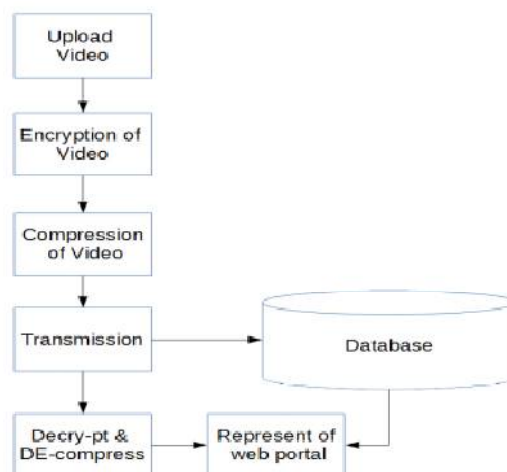


Fig-Architecture Diagram

# International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: [www.ijirset.com](http://www.ijirset.com)

Vol. 7, Issue 5, May 2018

In architecture diagram of proposed system we can upload the video on database. After that we can encrypt that uploaded video using blowfish algorithm. In this blowfish algorithm we can encrypt the video using exchanging the frames of video. i.e we can exchange right side frame with left side frame and so on. In this way we can encrypt the video. This encrypted video is compressed with the help of blowfish algorithm. In this we can compress the video. Using compression technique we can send the video easily. It can reduce the size of video. In our project we can compressed the video of any format.

After that we can transfer that video to specific user who can register on system. This video is in the encrypted format so we can first decrypt that video. So we can provide a key for decryption process. This key send to user registered mail id. After he can get the key he can enter that particular key and decrypt that video and download it. In this way we can performed the video encryption and decryption using blowfish algorithm.

## Technologies to be used

### Blowfish:

Blowfish is a symmetric block cipher that can be used as a drop-in replacement for DES or IDEA. It takes a variable-length key, from 32 bits to 448 bits, making it ideal for both domestic and exportable use. Blowfish was designed in 1993 by Bruce Schneier as a fast, free alternative to existing encryption algorithms.

We can used this algorithm for encryption and decryption purpose. In this system using blowfish algorithm we can send encrypted video to other user and this encrypted video is decrypted using blowfish algorithm. In the process of decryption we can used one key using that key user can decrypt that particular video.

### Compression:

Compression is useful because it reduces resources required to store and transmit data. Computational resources are consumed in the compression process and, usually, in the reversal of the process (decompression). Data compression is subject to a space-time complexity trade-off. For instance, a compression stream for video may require expensive hardware for the video to be decompressed fast enough to be viewed as it is being decompressed, and the option to decompress the video in full before watching it may be inconvenient or require additional storage.

We can compressed the video for reducing the size of video so that we can easily send the video with low space and bandwidth. In compression we can compress the large video. We can compress the video up to 40 MB. In specified folder zip and unzip folder is created. In that folder compressed video are saved in zip folder.

### Algorithm

```
void encrypt(uint32_t & L, uint32_t & R) {
for(int i=0 ; i<16 ; i += 2) {
L ^= P[i];
R ^= f(L);
R ^= P[i+1];
L ^= f(R);
}
L ^= P[16];
R ^= P[17];
swap (L, R);
}
void decrypt(uint32_t & L, uint32_t & R) {
for(int i=16 ; i > 0 ; i -= 2) {
L ^= P[i+1];
R ^= f(L);
R ^= P[i];
}
```

# International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: [www.ijirset.com](http://www.ijirset.com)

Vol. 7, Issue 5, May 2018

```
L ^= f(R);  
}  
L ^= P[1];  
R ^= P[0];  
swap (L, R);  
}
```

## IV. OVERALL DESCRIPTION

### PRODUCT PERSPECTIVE:

The perspective of the proposed system is, keeping information secure structure unapproved aggressors. In this manner information is scrambled through procedure of Encryption. Various encryption algorithm has long been developed. So using blowfish algorithm we perform all this process.

### PRODUCT FUNCTION

User-

- 1) User Registration on web.
- 2) Then user Login on web.
- 3) User should be upload video.
- 4) User would Send these video to another user.
- 5) User would receive video by another user.

Web application:

- 1) Convert video in encryption and decryption.
- 2) Apply blowfish algorithm to video.
- 3) Compress these video using compression algorithm.

## V. CONCLUSION

Hence here we conclude that, through this concept we can successfully encrypt and transmit videos. Selective encryption is computationally efficient and robust way of video encryption. Encryption improves transmission confidentiality of the video data.

## VI. FUTURE SCOPE

The future work includes implementation of encryption scheme. In future we compress the large video and encrypt that video using different encryption schemes. Using compression techniques we can reduce the size of video. So easily transmit video. We can encrypt frames using different algorithms.

## REFERENCES

- [1] HaojieShen, Li Zhuo, Yingdi Zhao, An efficient motion reference structure based selective encryption algorithm for H.264 videos| Published in IET Information Security,2013, pp. - 1,2
- [2] Qihua Wang, XingjunWang,A New Selective VideoEncryption Algorithm for the H.264 Standard| IEEE 2014, pp-1,3.
- [3] HaojieShen, Li Zhuo, Yingdi Zhao, An efficient motion reference structure based selective encryption algorithm for H.264 videos| Published in IET Information Security,2013, pp. - 1,2
- [4] Qihua Wang, XingjunWang,A New Selective VideoEncryption Algorithm for the H.264 Standard| IEEE 2014, pp-1,3.
- [5] Hwa Young Um, Selective video encryption of distributed video coded bitstreams and multicast security over wireless networks|, A Thesis Submitted to the Faculty of Purdue University, Aug2006,p.48,55,62



ISSN(Online): 2319-8753  
ISSN (Print): 2347-6710

## International Journal of Innovative Research in Science, Engineering and Technology

*(A High Impact Factor, Monthly, Peer Reviewed Journal)*

Visit: [www.ijirset.com](http://www.ijirset.com)

**Vol. 7, Issue 5, May 2018**

- [6] Dinesh Goyal, Naveen Hemrajani , Suresh GyanVihar Novel Selective Video Encryption for H.264 Videol, international journal of information security science p.5-6
- [7] M. Abomhara, Omar Zakaria, Othman O. Khalifa, A.A Zaidan, B.B Zaidan. Enhancing Selective Encryption for H.264/AVC Using Advanced Encryption Standardl, International Journal of Computer Theory and Engineering,p.4-5
- [8] Mohammed A. Saleh, Nooritawati Md. Tahir, EzrilHisham&HabibahHashim, An Analysis and Comparison for Popular Video Encryption Algorithmsl,pp-2-4.
- [9]Enhancing Blowfish File Encryption Algorithm through Parallel Computing on GPUl by TejalMahajan, ShraddhaMasih.
- [10]Blowfish encryption algorithm for information securityl by SaikumarManku and K. Vasanth.